information

MDPI

Article

Designing the Health-Related Internet of Things: Ethical Principles and Guidelines

Brent Mittelstadt [1,2,3]

[1] Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK; brent.mittelstadt@oii.ox.ac.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

Received: 29 March 2017; Accepted: 28 June 2017; Published: 1 July 2017

Abstract: The conjunction of wireless computing, ubiquitous Internet access, and the miniaturisation of sensors have opened the door for technological applications that can monitor health and well-being outside of formal healthcare systems. The health-related Internet of Things (H-IoT) increasingly plays a key role in health management by providing real-time tele-monitoring of patients, testing of treatments, actuation of medical devices, and fitness and well-being monitoring. Given its numerous applications and proposed benefits, adoption by medical and social care institutions and consumers may be rapid. However, a host of ethical concerns are also raised that must be addressed. The inherent sensitivity of health-related data being generated and latent risks of Internet-enabled devices pose serious challenges. Users, already in a vulnerable position as patients, face a seemingly impossible task to retain control over their data due to the scale, scope and complexity of systems that create, aggregate, and analyse personal health data. In response, the H-IoT must be designed to be technologically robust and scientifically reliable, while also remaining ethically responsible, trustworthy, and respectful of user rights and interests. To assist developers of the H-IoT, this paper describes nine principles and nine guidelines for ethical design of H-IoT devices and data protocols.

Keywords: internet of things; data ethics; health; data analytics; responsible research and innovation

1. Introduction

The conjunction of wireless computing, ubiquitous Internet access, and the miniaturisation of sensors have opened the door for technological applications that can monitor health and well-being outside of formal healthcare systems. The health-related Internet of Things (H-IoT) increasingly plays a key role in health management by providing real-time tele-monitoring of patients, testing of treatments, actuation of medical devices (e.g., medication dispensation), fitness and well-being monitoring, patient and carer alerts, among other applications [1]. Physiological parameters (e.g., heart rate, respiration, blood oxygen saturation, skin temperature, blood glucose, and blood chemistry) can be collected alongside behavioural parameters linked to health and well-being [2]. The health and behaviours of users can increasingly be digitised, recorded, stored and analysed, creating novel opportunities for clinical care and research [3,4]. H-IoT analytics protocols use this data in turn to produce information about various aspects of a user's health. Data streams from multiple sensors can be aggregated to facilitate linked-up care and health management. H-IoT can supplement clinical and preventative care and management of chronic health conditions with monitoring outside traditional medical environments. Novel connections can be found between areas of private life traditionally outside the scope of health and health care [5].

Given its numerous applications, H-IoT promises many benefits for health and healthcare. Despite its promise, H-IoT also raises a host of ethical concerns related to the inherent sensitivity of health-related data being generated and analysed, as well as latent risks of Internet-enabled devices. Users, already in a vulnerable position as a patient [6,7] face a seemingly impossible challenge to retain control over the data produced and analysed by the H-IoT, owing to the scale, scope and complexity of systems that routinely and automatically produce and analyse personal health data.

Users have traditionally received help in protecting their interests and privacy through regulation. Health data, and the devices that handle them, have traditionally faced strict legal rules that constrain collection and processing. Data protection law in Europe, for example, has traditionally treated health data as a "special category of personal data" requiring greater restrictions. Similarly, the Health Insurance Portability and Accountability Act has constrained processing and sharing of patient records in the United States. H-IoT presents new challenges for such legal frameworks by producing data that is not in many cases strictly medical data, but rather "health-related" data containing various physiological, psychological, and behavioural measures. Whether and to what extent H-IoT devices will be treated under law as "medical devices", or devices that collect and process health data for medical purposes, remains to be seen.

Europe's General Data Protection Regulation (GDPR), set to come into effect in May 2018, provides a clear example of this tension in law. An important change concerns the definition of "data concerning health," which is considered a "special category of personal data". It remains uncertain precisely which types of data "concern health". According to Article 4(15) of the GDPR, "data concerning health" is defined as "personal data related to the physical or mental health of a natural person, which reveal information about his or her health status." This definition implies that the purpose of processing, rather than the data source, determines whether data can be considered "health data" (Recital 35 GDPR). Data that do not directly describe health, but from which health-related inferences can be drawn, appear to fall within the scope, and will thus likely be subject to greater restrictions and protections as a "special category of personal data" (Article 9 GDPR).

Recognising these types of challenges, the H-IoT needs to be designed to be technologically robust and scientifically reliable, while also remaining ethically responsible, trustworthy, and respectful of user rights and interests. Design choices that affect how users interact with devices and services, or how the H-IoT works with existing healthcare practices, affect how H-IoT is perceived by users (for instance, as trustworthy or privacy enhancing or invasive). Privacy is a key concern, as the H-IoT can create granular, longitudinal personal health and activity records that can be highly invasive. Once data have been generated by a device, they must be transmitted, curated, labelled, stored, and analysed. Protocols for each of these steps can similarly be ethically sensitive in their design. A protocol that, for example, retains data indefinitely without a clearly defined purpose may be more problematic than storage with well-defined limitations, scope, and purpose.

Developers should not have to work in isolation to design an ethically acceptable H-IoT. To contribute to the ethical design of the H-IoT, this paper proposes nine ethical principles for the design of H-IoT devices and data protocols:

1. Facilitate public health actions and user engagement with research via the H-IoT;
2. Non-maleficence and beneficence;
3. Respect autonomy and avoid subtle nudging of user behaviour;
4. Respect individual privacy;
5. Respect group privacy;
6. Embed inclusiveness and diversity in design;
7. Collect the minimal data required;
8. Establish and maintain trust and confidentiality between H-IoT users and providers;
9. Ensure data processing protocols are transparent and accountable.

The principles are inspired by well-established concepts and ethical principles in disciplines related to H-IoT, including medicine and data protection law. Specifically, ethical principles for the H-IoT are derived from the principlist approach to medical ethics defined by Beauchamp and

Childress [8], the Organisation for Economic Co-operation and Development's (OECD) Privacy Framework [9], and values embedded in international data protection law. The principles proposed here can be considered a mid-level specification of these well-established high-level, abstract principles and values. Reflecting this, several high-level concepts (e.g., privacy and autonomy) apply across multiple mid-level principles.

Mid-level ethical principles provide contextualised but abstract requirements for technology design, and can thus be of limited use without further application and grounding in specific cases of technology design. To assist developers in addressing real world ethical challenges with the H-IoT, nine low-level guidelines for ethical design of H-IoT devices and data protocols are also proposed. These guidelines are intended as a starting point to embed the proposed ethical principles in the design of H-IoT, prior to adoption by users and subsequent assessment of acceptability:

1. Give users control over data collection and transmission;
2. Iteratively adhere to industry and research confidentiality standards;
3. Design devices and data sharing protocols to protect user privacy by default;
4. Use alternative consent mechanisms when sharing H-IoT data;
5. Meet professional duties of care and facilitate inclusion of medical professionals in H-IoT mediated care;
6. Include robust transparency mechanisms in H-IoT data protocols to grant users oversight over their data;
7. Report the uncertain utility of H-IoT data to users at the point of adoption;
8. Provide users with practically useful mechanisms to exercise meaningful data access rights;
9. Design devices to be unobtrusive according to the needs of specific user groups.

An ethically designed H-IoT will assist medical professionals, informal carers, and other health service providers in meeting their moral responsibilities in providing healthcare and management. Users will likewise be empowered and protected from exploitation and harm stemming from the H-IoT. Ethical design is essential to ensure user interests are afforded sufficient protection by H-IoT devices and data protocols. By adopting these guidelines, developers can demonstrate a serious commitment to meeting their legal and moral responsibilities to users, care providers and other stakeholders. Further, adoption will pre-empt many foreseeable ethical problems in the design and roll out of H-IoT devices and protocols, for which developers would be legally or morally liable. This is not, however, to suggest that the guidelines are a "one-size-fits-all" approach to ethics in design; rather, the guidelines are purposefully flexible to allow users with different interests and priorities to use their devices and protocols as they see fit, for example by choosing how and with whom to share H-IoT data.

The paper is structured as follows. In Section 2, nine ethical principles for H-IoT design are defined. The principles focus primarily on the data produced by H-IoT devices, as opposed to the devices themselves. While many principles can be proposed for the design of H-IoT devices, often these principles overlap substantially with concerns discussed in the context of device security and user acceptability, which are outside the scope of this paper. In Section 3, nine concrete guidelines are then proposed for H-IoT design based upon the ethical principles identified in Section 2. These guidelines are intended to be considered by H-IoT developers in the first instance. However, their relevance extends beyond the design process to include how H-IoT is deployed in specific contexts of care. To unpack the applicability of the guidelines to specific use cases, Section 4 considers H-IoT designed for two user groups: the elderly and children. Section 5 concludes with several open questions and future avenues of research concerning the ethical design of the H-IoT.

2. Principles for Ethical Design of the H-IoT

Recognising the challenges posed by H-IoT, ethical design of devices, and protocols is critical. To this end, nine principles are proposed for ethical design of H-IoT. These principles address the challenges of protecting and balancing interests of individuals, group, and society relating to the collection and sharing of H-IoT data for public and private purposes. Valuable interests of each stakeholder group can frequently come into conflict when considering potential collection, sharing, or re-purposing of H-IoT data. The following principles are intended to give providers a starting point for the complicated task of balancing and protecting competing interests in the design and deployment of H-IoT.

2.1. Facilitate Public Health Actions and User Engagement with Research via the H-IoT

H-IoT data can be highly valuable for medical research and public health programmes. The value of advancing medical and public health knowledge through secondary analysis of H-IoT data must be taken seriously [10]. At the same time, protecting the interests of individuals is undoubtedly important. However, their protection should not always come at the cost of preventing valid research programmes to be conducted with H-IoT data. In considering potential uses of H-IoT data for public health and research, individual, group, and societal interests can come into conflict.

As H-IoT will soon be responsible for generating substantial amounts of medically relevant data, public health interests must be seriously considered in designing data sharing protocols. Proposals for automatic or prompted sharing can be justified by moral obligations between patients and medicine as a practice: a non-binding "duty to participate" has, for example, been previously advanced in medical ethics [10–12]. Without taking a position on the validity of such a duty, respect for user autonomy suggests options should be provided for users to easily share their data with researchers according to personal preference. With that said, as part of such a protocol H-IoT providers may likewise have a duty to inform users of the potential risks of data sharing for research, or to "vet" research bodies requesting access [13].

Striking an equitable balance between individual and collective interests may not always be possible, yet arguments can be made for promoting one (e.g., societal interests in outbreak tracking) over another (e.g., individual interests in personal privacy). In balancing these interests, consideration must be given to the potential harms facing individuals and groups due to sharing of their data for public health purposes. Likewise, consideration must also be given to the opportunity costs of blocking data sharing for research and public health purposes, and thus to the costs in terms of societal interests for the sake of protecting individual or group interests.

2.2. Non-Maleficence and Beneficence

Following from need to consider potential harms to individual, group, and societal interests, non-maleficence and beneficence have long been foundational principles in medical ethics. The principles are often cited in relation to Beauchamp and Childress' principlist approach to medical ethics. Although intended to guide the actions of medical practitioners, the principles can be extended to H-IoT devices and services, and the data they generate.

As with any device, practice or research in medicine, and as demanded by the principles of non-maleficence and beneficence, H-IoT must be designed with user safety as a key concern. Ethically responsible devices will be secure and reliable; testing to prove functionality or long-term assurances related to device security prior to a device or service entering the market can, for example, be required. H-IoT devices and services should similarly not pose a serious threat to a user's health or safety. Devices should be secure and reliable, particularly for devices with actuating functions, with clear plans for longevity [8]. Poorly secured devices can pose a risk both to a patient's physical safety and informational privacy. Concerning the latter, H-IoT data can provide meaningful insight into the health and behaviours of users and, if aggregated, patient populations. Insight and recommendations for the care of individual users can be generated, alongside secondary usage for biomedical research and administrative monitoring concerning the epidemiology, public health and the performance of medical systems.

For each of these potential uses, the principle of non-maleficence requires that data not be used against the interests of the individual users and populations responsible for their creation. Users can have a range of interests concerning their fundamental rights (e.g., privacy), health, and well-being, all of which can be affected by H-IoT. At its best, H-IoT will help improve a user's health by generating data about the user's health and providing monitoring of conditions to supplement other forms of medical and social care. User's safety can, however, be placed at risk if H-IoT results in poorer quality of care, for instance if used as a replacement for human care [2]. In practice, this principle would require that H-IoT data to be used to inform the care of individual users and the advancement of medical knowledge and techniques.

H-IoT should not contribute to the denial of services to the individuals generating the data in the first instance; the same may be true regarding denial of medical services or resources to affected patient populations. Individuals use H-IoT in good faith that it will contribute to the maintenance of health and well-being. This expectation should not be undermined by uses of the resulting data solely for the promotion of third party interests unrelated to their care or the maintenance of medical and healthcare systems, such as targeted advertising.

Emergency alert functions provide an interesting case in which respect for autonomy, non-maleficence and beneficence must be balanced. Devices can intervene and alert carers or medical professionals when a measurement indicating an emergency is encountered, for instance when a user has fallen. Nudging of user behaviour in genuine emergencies is generally accepted for the sake of user safety. However, the threshold for emergencies is not necessarily self-evident, nor can the reliability of a measurement be taken for granted. False positives can harmful as well as false negatives, due to the distress caused to users and avoidable usage of valuable public health resources through unnecessary visits to the emergency room, for example [14]. This issue also raises concerns over automation and the degree to which a human medical professional should be involved in decision-making around emergency alerts. In cases of in-home care, professional involvement can be appropriate, particularly to contact the user prior to alerting emergency services (for example). In other cases, the involvement of a professional in the decision-making loop appears less appropriate, parents would be a more appropriate choice in the case of baby monitoring, for example.

As these examples suggest, definitions of benefit and harm, or "good" and "bad", will differ between users and contexts of use. These definitions are dependent upon the objectives of using H-IoT, and the value systems in place. As a result, design choices and external protections put into place to protect users from harm and ensure benefits will need to be malleable, and responsive to the subjective needs and values of users.

2.3. Respect Autonomy and Avoid Subtle Nudging of User Behaviour

Following from the context-specificity of benefits and harms of H-IoT use, similar constraints are relevant when considering the need to protect user autonomy. Respect for autonomy is a well-established principle in medical ethics [8] and international data protection law. Autonomy is a valued concept because it enables free and uninhibited decision-making [15,16]. H-IoT can undermine autonomy by "nudging" user behaviour to fit third party interests [17], and by "mummifying" one's identity over time through storage and exchange of personal data in perpetuity. This can inhibit the ability to lead a life of one's choosing [18].

User behaviour can be nudged in numerous ways. Personalised feedback on health or activity, a feature of many H-IoT devices, directly attempts to influence user behaviour to meet a preferred metric. Self-imposed constraints on behaviour are also an example of nudging. The user may alter their behaviours in response to perceived expectations of the device, or the service provider and care team involved. Aesthetic design choices and a user's emotional attachment to a device can amplify or nullify the effectiveness of nudges.

Nudging can undermine autonomy insofar as the user can be pushed to make the "institutionally preferred action rather than their own preference" [19]. As this suggests, the acceptability of nudging can be evaluated according to the interests being promoted. Nudging users towards behaviours that promote self-defined interests, or those aligned with the service agreed to by the user (e.g., feedback on exercise or activity levels), is initially unproblematic. Nudging towards behaviours or interests held by third parties, such as commercial interests, is problematic in contrast because it undermines the user's control over her behaviours. Online consumers, for example, can be nudged to fit market needs by filtering how products are displayed [20]. The acceptability of nudging can also be evaluated in terms of visibility. As the principle of transparency below suggests, invisible or subtle nudging is problematic insofar as it undermines the user's autonomy. In all cases, the acceptability of undermining a user's autonomy through nudging must be evaluated against the interests being promoted. Promotion of valuable public interests (e.g., health promotion) through subtle nudging could, for example, be considered justifiable in some cases despite the impact on individual autonomy.

The conflict between user and third party interests is evident in H-IoT designed for elderly and infirm users. Benefits to user safety are often the basis for adoption. However, safety interests can act as a constraint on autonomy, insofar as a "need" for H-IoT is perceived from the user that leads to adopting a device or service that would otherwise not be used [21,22]. Autonomy is constrained insofar as the patient experiences (both internally and externally imposed) pressure to use H-IoT.

The autonomy of users can also be undermined when H-IoT data are shared with third parties without input from the user. Historically, informed consent has been the default mechanism to protect the autonomy and related interests of participants in research. 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 [23]. This type of consent is typically infeasible when data are aggregated and routinely shared with third parties. The uncertain value of H-IoT data, and what it can reveal about the user through novel and unforeseen analysis and linkage with other datasets, therefore challenges the protection normally afforded to autonomy through single instance consent [24]. Consent cannot be "informed" at the point of data collection in the sense that data subjects cannot be told about future uses and consequences of their data, which are unknowable at the time the data are collected or aggregated. Where H-IoT data are used for research or secondary analysis, user interests in autonomy must be protected.

Finally, user control and oversight over their data are an important dimension of respecting autonomy. Users (or proxies thereof) should be granted access and portability rights to data collected by H-IoT. Data access allows users to protect their privacy interests, maintain oversight over the types of data being collected, how they are used. Data access is intended to empower individuals to control and benefit from their data. A right to "self-determination" can ground such connected data rights [25] to combat the "transparency asymmetry" that exists when consumers lack information about how data about them are "collected, analysed, and used" [25,26]. Data portability likewise grants users a choice to share their data with preferred parties, such as medical and social care providers [27], and to freely move between H-IoT device and service providers. It can also be argued that data subjects should be allowed to derive personal benefit from their data beyond the development of new products or services [28]. Portability allows individuals to pursue projects and aims with the data they produce without assistance from the originating H-IoT provider [29].

The importance of data access and portability are reflected in European data protection law. Users enjoy a right to data portability under Article 20 of the General Data Protection Regulation, which enables controlled sharing by users, for instance with healthcare services. Data subjects are also granted rights to be "kept in the loop" regarding data processing and storage [30]. In practice, data subjects must be notified when data about them are created, modified or analysed, and provided means to access and correct errors or misinterpretations in the data and knowledge derived from it These mechanisms provide data subjects with the means to be aware of when and for what purposes their data are being used, and thus to make choices reflecting their subjective values over when and how to share their data for public and private uses. Revision rights can, however, undermine the accuracy and integrity of datasets due to modifications made by data subjects [25]. This risk must be accounted for when designing and constraining access mechanisms.

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. For access rights to be meaningful, data subjects must be able to exercise them with reasonable effort. For instance, being provided with thousands of printed pages of data would require unreasonable effort on the part of the data subject when more efficient formats are available, and would therefore fail to preserve a meaningful right to access. Comprehension also poses a challenge; "Big Data" requires significant computational power and storage, and advanced scientific know-how [31,32]. As with any type of data science, analysis requires discipline-specific skills and knowledge, often only accessible through extensive training and education. Even for willing subjects, the amount of time and effort required to attain the background knowledge and skills to understand the totality of data held about oneself can easily be overwhelming.

2.4. Respect Individual Privacy

Subjectivity similarly applies to the protection of privacy through design. Protecting the informational privacy of H-IoT users is key, as privacy empowers users to control data about themselves, limiting opportunities for unwanted disturbances and exploitation [33–35]. Information enables regulation, behavioural control, and profiling by those with greater access [36]. Thus, informational privacy acts as a check on the power of organisations and data controllers [37,38].

The sensitivity of data describing health and health-related behaviours is widely recognised in international data protection and privacy law [39]. The data generated by H-IoT devices can be highly invasive due to the possibility to infer knowledge about a user's health and behaviour. Analysis of aggregated datasets can be particularly invasive, as the inferences allowed when data from multiple sources are considered are difficult to predict [40–42]. Protection of user privacy is therefore a critical concern for the design of H-IoT.

Privacy can be valued on many grounds, demonstrated at a minimum by the concept's prevalence in international law [43,44]. The OECD's Fair Information Principles, which place an emphasis on privacy, have proven particularly influential in commentary on the privacy impact of Big Data analytics used to make sense of H-IoT data [24]. In many cases, protection of privacy is equated to control of personally identifiable data. Techniques such as anonymisation and aggregation are thought to reduce the risk of re-identification, and thus to guarantee the privacy of the user [23,45–47].

Respect of privacy must be a key principle for H-IoT design due to the opportunity offered by H-IoT data to violate context-sensitive expectations of privacy [48]. Privacy norms are challenged when H-IoT data can be analysed outside of the "highly context-sensitive spaces" in which they are created. These data can be stored in perpetuity, meaning that traditional limitations of memory no longer apply; data collected today may, in theory, be equally accessible and of the same quality in the future. Extending the lifespan of data describing phenomena that would otherwise be forgotten, in this case the health and behaviours of users, increases the risk of privacy violations.

Respect for privacy should be the starting point for the design of H-IoT devices and protocols. Departures from this initial position would require negotiation or justification by appeal to vital third party interests. When the design of H-IoT is viewed as a *negotiation* in which the user's interests in privacy take priority by default, reasonable expectations can be formed by users and providers alike over the structure of their relationship. Users, for example, can reasonably expect to be consulted when a proposed usage of their data would be privacy invasive. Defining initial "terms of engagement" for H-IoT prior to its use contributes to the development of trust between users and providers, which is a key factor in meeting the many moral responsibilities described in the principles specified here.

Attention must also be paid to the protection of privacy in H-IoT data due to a potential lack of protection afforded to health-related data generated by H-IoT devices and services controlled by commercial actors. Unlike biobanks or academic medical research repositories, commercial databases may only be subject to requirements set forth in data protection law and voluntarily adopted codes of conduct. H-IoT data may therefore be routinely subject to less stringent requirements to protect user privacy [49].

2.5. Respect Group Privacy

H-IoT data can be used to support the care of individual users or to learn something about the health of the user and similar populations. Privacy must, therefore, be approached on both an individual and group level. Even when anonymisation is successful and re-identification is prevented, only the privacy of identifiable individuals is protected. Groups with valid interests in the processing and dissemination of data about themselves and their members do not benefit from techniques aimed at preventing re-identification [50]. Perfectly anonymised datasets still allow for group-level ethical harms for which the identities of members of the group or profile are irrelevant [51]. Where anonymised data subjects are grouped according to geographical, socioeconomic, ethnic or other characteristics, the anonymisation of individuals matters little if outcomes affect the groups to which they belong [23]. Discrimination and stigmatisation of affected groups is therefore a risk [52], even in anonymised datasets. Such effects impact on all members of the community, not only those who gave consent [50]. It is possible to conceive of privacy as a group-level concept and thus speak of “group privacy rights” that could restrict the flow and acceptable uses of aggregated datasets and profiling. Group privacy interests must therefore also be considered.

2.6. Embed Inclusiveness and Diversity in Design

As the need to protect group privacy suggests, H-IoT is designed for many different user groups, varying in terms of health condition, demographics and culture. Specific user groups will have different requirements for ethically sound H-IoT; devices for dementia patients, for example, may require reduced control over functionality for the sake of safety. Furthermore, user groups will vary in terms of technical capacity and resources to obtain and use H-IoT over time.

Given the sensitivity of data involved, varying capacities of users, and the subjectivity of the interests represented across the other eight principles between user groups and cultures [48], users (or proxies thereof) should be included in H-IoT design whenever possible. Following this, the nature of user involvement in the design process should be reported, including information on who was involved and in what capacity. Inclusion in design enhances the agency of users; devices can be designed that both align with the values and interests of specific user groups, while allowing individual control of privacy policies and features. Further, the accessibility of device and protocols to different groups can be enhanced. The value of inclusiveness requires that groups should not be marginalised or excluded from using H-IoT due to factors beyond their control. If H-IoT devices are produced only for highly technically competent affluent users, potential users that could benefit greatly from the technology would be marginalised [24]. Equity of access demands that development of H-IoT does not ignore user groups for the sake of commercial interests or efficiency.

2.7. Collect the Minimal Data Desired by Users

While individual and group preferences for the design of H-IoT devices and data protocols can vary significantly, certain principles can be recommended as default positions to be adopted by designers to ensure this subjectivity is respected. The proliferation of sensing devices creates unprecedented opportunities to collect data about the private lives and habits of users. Despite requirements for data minimisation in data protection law, a culture of “data hoarding”, or data collection for its own sake, has emerged in which data are pervasively collected and stored under the impression that they may have future value. However, data collection inherently presents a latent privacy risk to the users whose lives, or health and well-being, are being digitised. Data generated by H-IoT may make it more difficult to shake off a pathologically-based identity, when H-IoT usage ceases or the monitored condition is cured.

H-IoT should, therefore, collect only the minimal data desired by users. Some preferences in this context can be inferred from the nature of the user-provider relationship. Users have, for example, an obvious interest in the utility of the device or service being used, and can thus be assumed to want data to be collected required for functionality. Reflecting the primacy of user's privacy interests, an option should be available to have additional data collected for purposes not immediately related to functionality.

Collection of identifiable data should similarly be minimised in accordance with data protection law. The importance of data minimization as a design principle is echoed in the OECD's Fair Information Principles, as well as forthcoming requirements in the European Union's (EU) General Data Protection Regulation (Articles 6–7). The latter clarifies that user consent concerning the collection of data that are "excessive in relation to the purpose specified" will not be considered valid in the future [53]. Despite common ground, this principle emphasises that more restrictive limits on data collection may be ethically justified beyond legal requirements. Interpretation of "legitimate interests" of data controllers under the General Data Protection Regulation may, for example, significantly weaken user control over processing of personal data.

2.8. Establish and Maintain Trust and Confidentiality between H-IoT Users and Providers

Each of the preceding principles describes key interests of individuals, groups, and society that, if protected through design, can contribute to the trustworthiness of the H-IoT and trust between users and providers. Trust is closely linked to other values including privacy, confidentiality, safety, efficacy, and others. As a characteristic of relationships between users and H-IoT providers, trustworthiness can be valued on its own for the positive psychological and emotional benefit it grants to participants in a trusting relationship. In other words, a system can be privacy enhancing, confidential, safe and effective, but the user can still experience distress or suffer material harm if it or its providers are perceived as untrustworthy.

Confidentiality is a critical element of trusting relationships between H-IoT users and providers, given the sensitivity of the data being collected. Users of H-IoT have been shown to place significant trust in devices and service providers to handle their data responsibly and confidentially [36,54,55]. Trust is often a prerequisite for H-IoT systems to be viewed as privacy enhancing in the context of informational privacy [54,56–61]. Users place trust in devices and service providers to handle their data responsibly [36,54,55].

Trust concerns the interaction between a system processing data (including the people or institutions involved), users providing the data, and third parties accessing the data. Trustworthiness in developers concerns the developers' choices, the values they imbue in their artefacts, and their ability to foresee and prevent misuses and undesired consequences. It also involves the obligations of data processors to respect users' rights and terms of consent, insofar as the latter specifies the conditions of the trust of data subjects in data processors [62–64].

Users may trust systems and data processors to handle their data responsibly; similarly, users can trust a device or service provider to have designed a robust, safe and effective system. A lack of trust has been linked to reluctance to adopt H-IoT [15,65]. Users will not necessarily trust H-IoT by default. H-IoT should therefore be designed to demonstrate trustworthiness, for instance by operating transparently or giving users an active choice in how data are collected and shared.

2.9. Ensure Data Processing Protocols Are Transparent and Accountable

H-IoT can collect a wide range of data, and process it in complex and opaque ways. H-IoT devices encourage the flow of data among users, service providers, and third parties. Often, data are processed and exchanged with little oversight from data subjects. When problems occur, or queries arise, it is critical that information be available to data subjects to explain how data have been handled that led to the outcome in question.

The need for transparency, independent of any rights held by data subjects, increases in step with the social impact of decisions made based on the data in question [66]. Transparency is a well-established aim in mature information societies [67]. In the context of the IoT, guidelines proposed by TechUK to ensure trust in the design of the IoT highlight transparency as a key concern [27]. These guidelines suggest that data processors cannot presume that the derivation of value from IoT data is justified before involving users. Rather, to earn the right to derive value from IoT data, data processors must first demonstrate transparency, integrity and security in processing, and show the benefits of processing to the public.

Transparency empowers users to hold providers accountable for the impact of H-IoT on their medical care and quality of life. If H-IoT providers do not operate transparently proactively, the capacity of users to establish liability or question decisions reached based on H-IoT data is undermined. Impact can be assessed, at a minimum, according to the degree to which providers adhere to the preceding eight principles in designing and deploying H-IoT devices and data protocols.

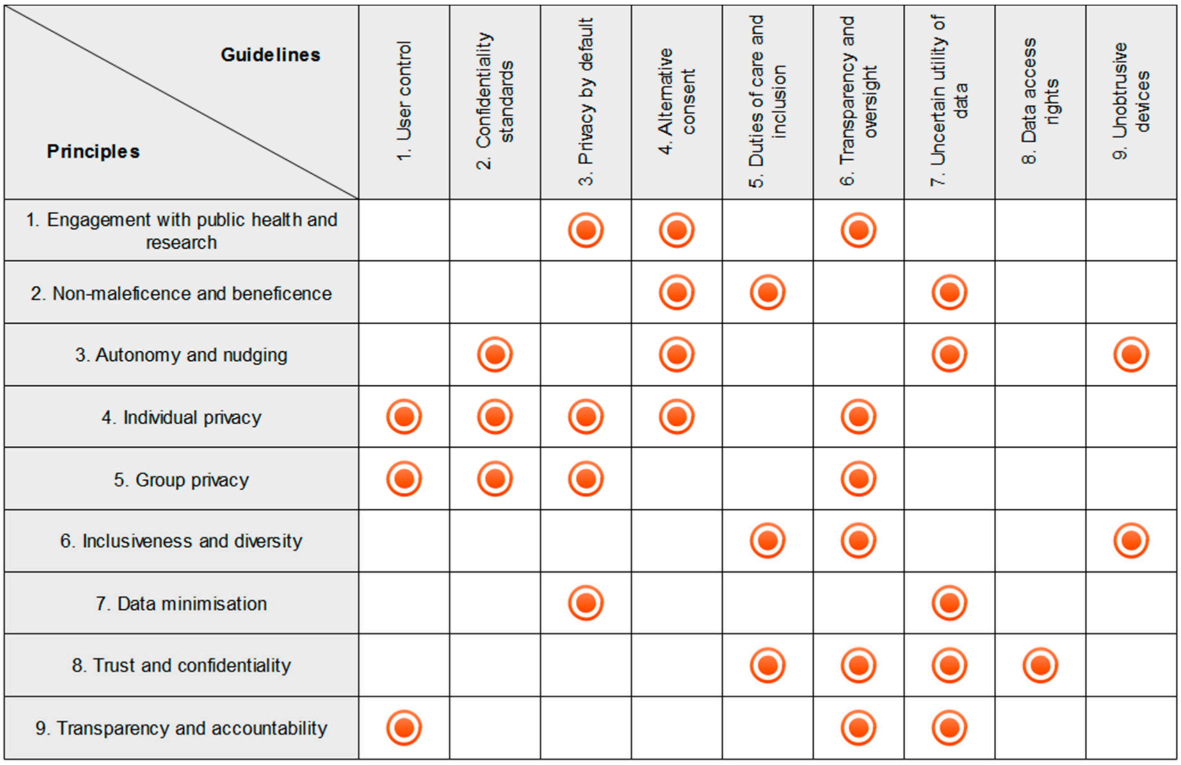
As the utility of transparency as a wide-ranging accountability mechanism suggests, the concept can be valued on many grounds. Basic respect for the autonomy of users suggests reasons and evidence should be provided for actions taken towards them. In H-IoT, transparency could require, for instance, an explanation of how the data produced by using H-IoT has influenced the user's medical care [68]. This type of explanation allows users to make informed decisions about acceptable uses of their data, and the personal impact of continuing to use H-IoT [69]. Explanations can be directed to both the user and care team, who may be better placed with technical knowledge to understand and modify the user's treatment in response. Users can only exercise control over their data in the interest of privacy if they are aware how it is handled and processed by third parties [69].

3. Guidelines for Ethical Design of the H-IoT

Inspired by these principles, several practical guidelines for the ethical design of H-IoT devices and protocols can be defined. As Figure 1 indicates, the nine principles do not map one-to-one to the nine guidelines proposed below. Rather, the quantity of principles and guidelines was incidental, and not intended to suggest a linear relationship. Following this, the guidelines proposed here do not exhaust the potential applications of the principles above, which are intended to be considered throughout the design and deployment of H-IoT. Rather, these guidelines provide initial direction to the ethical design of H-IoT.

3.1. Give Users Control over Data Collection and Transmission

Following the principles concerning user privacy interests and transparent data protocols, users should be granted meaningful levels of oversight and control of the data generated by H-IoT devices. Users' expectations of privacy can be violated when data gathered by a device is handed poorly, for instance being shared with third parties without the user's explicit knowledge or consent. Unauthorised sharing can impede a user's autonomy and sense of identity, and expose her to additional risks of identity theft, physical and virtual intrusion, and discrimination, among others. By controlling the dissemination of personal data, a person may be spared future disturbance from friends, family, caregivers, service providers, and others [37]. Caregivers can, for instance, use H-IoT to monitor whether the user is following prescribed medical care or engaging in risky behaviours that suggest frailty; both can disrespect the user's autonomy and ability to manage the identity presented to others. These activities are often hidden by elderly users wishing to control the image presented to, meaning H-IoT can erode the ability to manage identity. See [70].



Guidelines Principles	1. User control	2. Confidentiality standards	3. Privacy by default	4. Alternative consent	5. Duties of care and inclusion	6. Transparency and oversight	7. Uncertain utility of data	8. Data access rights	9. Unobtrusive devices
1. Engagement with public health and research			●	●		●			
2. Non-maleficence and beneficence				●	●		●		
3. Autonomy and nudging		●		●			●		●
4. Individual privacy	●	●	●	●		●			
5. Group privacy	●	●	●			●			
6. Inclusiveness and diversity					●	●			●
7. Data minimisation			●				●		
8. Trust and confidentiality					●	●	●	●	
9. Transparency and accountability	●					●	●		

Figure 1. Relationship between Principles and Guidelines.

It is therefore critical for H-IoT to allow users to decide how data should be shared. To enhance agency, users should be enabled to define and enforce context-specific norms of privacy [48], expressed through their choice of whom to share data with, when, and how. At a minimum, users must understand which categories of personal data are being collected by H-IoT, and some of the things different categories of data can reveal [27]. Features that provide users with control over data collection and transmission should be included in the design of H-IoT. These include simple on/off switches (or an online/offline mode), "consent sliders" to set at the time of use which data are collected and how they transmitted, and complex privacy policy management systems that allow users to select granularly what data to share, for what purposes, and with whom [37,71,72]. "Offline" privacy barriers such as physical walls can be replicated by requiring explicit action by users to upload or share data to publicly accessible locations. At best, cooperation between developers can create privacy enhancing tools that enable users to move freely between and interact with a range of H-IoT systems. These interactions would reflect the value-laden choices of users, without negotiating individual privacy agreements with each device or service provider [73–75].

There are, however, risks to full control by patients that must also be considered, particularly for infirm or vulnerable users. Necessary care may be foregone, risking the user's safety. Further, this choice may not be intentional; devices requiring manual activation would, for instance, present risks to the user's health if the user suffers an accident or is otherwise impaired. Default privacy settings can also prove harmful or beneficial. Assuming devices are set by default to allow "maximum" data collection and transmission, subsequent processing determines whether this proves harmful or beneficial. Greater data collection can, for instance, facilitate research and service improvement, but also expose the user to greater privacy risks. Recognising these risks, an appropriate balance must be struck between user control to protect her privacy and autonomy, and benefits to user safety and public interests via default settings and externally controlled collection and transmission settings. Participatory design methods can be used to help strike an appropriate balance [76,77]. Prior empirical research on balancing user and public interests in H-IoT is also available as guidance [55,78,79].

3.2. Iteratively Adhere to Public, Research, and Industry Confidentiality Standards

Following the principles of respect for privacy and autonomy interests of users, technical, organisational and legal confidentiality standards should be followed in the design of H-IoT. Guidance is provided by public and industry bodies (e.g., the Online Trust Alliance's IoT Trust Framework) [80] and regulators (e.g., the Food and Drug Administration's guidelines for cybersecurity in medical devices, the International Telecommunications Union's H.810 standards) [81–83]. At a minimum, de-identification of data when transferred to third parties should be required. However, even de-identified data can pose a residual risk of re-identification; an assessment of the genuine need for data of all types, balanced against possibilities of re-identification and other risks, should therefore accompany any sharing mechanisms.

Developers can build on work undertaken in the context of governance of medical data repositories (e.g., biobanks, patient registries) and sharing platforms [22,84]. Among such platforms in Europe, the European Medical Informatics Framework (EMIF) features one of the broadest (in terms of scale and data types) and demonstrative governance structures. EMIF's soon to be published ethical code of practice defines the responsibilities of data sources and data users (i.e. bona fide research organisations and individuals). The code is built upon both ethical principles and European data protection and privacy legal requirements. Common terms and guidance are provided for planning of feasibility studies, data sharing, collection and use of data subject consent, ethical approvals, legal requirements of data and privacy protection, and information security measures. Core values include data minimization, consent, anonymisation, and confidentiality. The code is laudable for moving beyond participant consent by defining responsibilities for third parties accessing the platform. Governance of the platform is structured requiring contributions from all stakeholders, as opposed to requirements defined solely by limitations specified in consent processes.

3.3. Design Devices and Data Sharing Protocols to Protect User Privacy by Default

Following the principles of data minimisation, protection of privacy, and public health interests, H-IoT should be designed to protect privacy "by default" [27]. Data collection and transmission should be limited by default, with collection and sharing of data exceeding minimum settings controlled by the user. Doing so allows users greater control over processing and sharing of their data, and avoids unnecessary privacy risks encouraged through the collection of data that are potentially valuable but not immediately relevant to the service provided.

Significant risks are also posed by inadvertent transfer of data if a device is loaned, sold or otherwise decommissioned from use. To protect the confidentiality of the user's data, devices should either reset by default when a change of user occurs, or offer the user an option to "reset" the device to a factory default (and in doing so, delete her personal data) [80]. Concerns over data legacy are related. Users of H-IoT may pass away, become cognitively impaired or otherwise lose the capacity to consent. When this occurs, data or control over data may need to be transferred to another party, such as the user's family, a data controller, a governmental body, or public health or medical institutions. Clear guidelines to handle the legacy of H-IoT data are required. Building a model based upon organ donation may provide a way forward to allow users to proactively specify recipients and the scope of data to be transferred. However, norms are also required to clarify when and how different third parties (e.g., relatives, family members, medical institutions) should receive the data based upon a valid interest.

Sales of data to third parties should be similarly restricted. As the Online Trust Alliance's IoT Trust Framework suggests, "identifiable consumer data" should not be sold unless the buyer has an equivalent privacy policy in place; "otherwise notice and consent must be obtained." Without such a mechanism, users can inadvertently share invasive details of their health and well-being, which can be highly valuable to third parties or data brokers.

As specified in the principle describing public health interests in the H-IoT, it must be recognised that H-IoT creates data with immense potential utility for medical and public health research and surveillance, which can come at the cost of individual interests. Privacy by default nonetheless still applies. Recognising that data can (and perhaps should) be shared for legitimate public health pursuits, user privacy must still be respected. In some cases, the need to take decisions for individuals on how best to use and share their data, and thus on the appropriate balance between individual and collective interests, can be avoided. User choice in how and with whom their data are shared should be supported above all else to ensure users can contribute to medical and public health research and administrative programmes of their choosing.

For developers, user choice and public health interests can likewise be supported by ensuring data can be easily shared with sufficient protections in place by default. Users should, for example, be provided with options to share data at different levels of identifiability with research and public health groups of their choosing. Following the need for privacy by default, H-IoT providers should ensure by default that data are sufficiently de-identified prior to sharing for secondary uses. Appropriate thresholds of identifiability will need to be determined according to the needs of particular studies or public health programmes. To meet their responsibilities relating to user privacy, providers can implement mechanisms into H-IoT to consult users and researchers in advance to ensure data are shared at an appropriate level of identifiability. In other words, H-IoT data controllers should provide users with customisable data de-identification and transmission tools for research and public health purposes.

One possible model of this approach would be a "data donation" model, comparable to organ donation, whereby users can flag segments of their health record generated by an H-IoT device or service for automatic sharing with approved medical and public health researchers in real-time. Users could alternatively be prompted to share their (anonymised) data after a set period (e.g., five years after collection).

3.4. Use Alternative Consent Mechanisms when Sharing H-IoT Data

Following the principles of respect for privacy, non-maleficence, autonomy, and public health, when informed consent is infeasible, alternative mechanisms to protect user interests normally protected by consent should be embedded in H-IoT data protocols. H-IoT providers should embed these mechanisms whenever data will be shared with third parties for secondary analyses, for both commercial and research purposes; the risks to user interests are equivalent in both cases. "Broad" and "blanket" consent mechanisms, which pre-authorise future secondary analyses, are sometimes used in place of single-instance consent in biomedical research, and should be considered [85,86]. Tiered or dynamic consent can also be used, which allow data subjects to pre-specify or active choose uses of their data—for example, to allow the data to be used in cancer research but not in genomic research [87,88]. Alternatively, data may be hosted in "safe harbours" rather than exchanged with third parties. This setup allows H-IoT providers to monitor actively and control how H-IoT data are used, minimising the risk of misuse by third parties [13]. Where these formats are used, governance mechanisms, such as review councils and committees, help distinguish *"bona fide"* and problematic requests for access to data. Equivalent bodies to represent the interests of users would need to be established by H-IoT providers.

As in the case of the governance of biobanks and medical data repositories (e.g., UK Biobank, EMIF), consent protocols are critical to protecting the user's interests. However, public heath interests must simultaneously be considered. Consent should ideally be sufficiently permissive or broad to allow for responsible secondary usage of de-identified data for research that promotes public health interests. The impact of restrictive, single-instance consent mechanisms is often to restrict future secondary uses [24]. Where legitimate public health interests can be pursued within responsible and well-designed studies, consent in the H-IoT should act as an enabler rather than restriction of secondary uses.

3.5. Meet Professional Duties of Care and Facilitate Inclusion of Medical Professionals in H-IoT Mediated Care

Following the principles of autonomy, non-maleficence, trust and inclusiveness, H-IoT should seek at a minimum to adhere to professional duties of care and include medical professionals wherever possible. While this is in part dependent upon how the H-IoT is deployed and used, steps can be taken at the design phase to facilitate meeting both requirements.

By providing devices and services that contribute to health care and management, H-IoT providers incur similar moral obligations [89] to medical professionals [90]. Whereas healthcare has traditionally centred on the doctor-patient relationship, H-IoT enables new multi-stakeholder care relationships. Existing accounts of the moral obligations of medicine may not translate well to these new types of relationships involving patients, medical professionals, and H-IoT device and service providers [39]. The values defining the traditional doctor-patient relationship extend beyond "efficiency" or "effectiveness" of interventions. Rather, medical professionals take on certain moral responsibilities in practicing medicine, and develop virtues or norms of good practice through their experiences providing care to patients [7,8,89]. Thus, these values and internal norms of "good" medical care may be undermined when care is distributed across H-IoT providers as well.

One critical duty of care, as suggested by the principle of non-maleficence, is to ensure that devices benefit the health and well-being of users in the first instance. This duty can be met through extensive testing of devices to avoid generation of false positives, unnecessary distress and material harms to users, and waste of healthcare resources.

Care relationships enabled by H-IoT also present risks for a patient's social, emotional and mental well-being. H-IoT allows greater emphasis on data representations of the patient created by the device [7,8,89]. Patients can be harmed by misinterpretation or overreliance on data representing their health status and well-being [91]. Monitoring data can complicate assessments of the patient's conditions, which otherwise rely upon physical examination and tacit knowledge [92,93]. Ignorance of the patient's social, mental, and emotional state, or "decontextualisation" of the patient by stifling the patient's "voice" in clinical care, can be the result [92–95].

To ensure duties of care are fully met, H-IoT data protocols should also allow users to share data and engage with medical professionals as desired. H-IoT is often viewed as a technological means to reduce the costs or need for professionals in medical and social care, while still providing comparable care. The user's quality of care, and physical and social well-being, are therefore at risk [65,96–99]. A combination of sensors, H-IoT service providers, healthcare professionals and informal caregivers may not provide equivalent quality of care, particularly in social and interpersonal aspects of care.

H-IoT devices should therefore meet, as far as possible, duties of care typical to healthcare. Opportunities should be created for medical and social care professionals to remain involved in management of the user's health and well-being. As already mentioned, clinical testing of devices and mechanisms for data access and portability are good starting points. Clinician involvement can include assigning responsibilities for analysing H-IoT data, providing feedback and follow-up to patients, answering questions and concerns and, as far as, possible emulating the face-to-face clinical encounter and dialogue through remote monitoring. Training for users on the operation is also desirable, particularly those with low technical competence (see Guideline 9).

3.6. Include Robust Transparency Mechanisms in H-IoT Data Protocols to Grant Users Oversight over Their Data

Following the principles of group privacy, trust, transparency, inclusiveness and public health, H-IoT providers should offer information about how the data generated through their device or service are processed and shared with third parties. This practice will ensure that users can meaningfully assert their privacy rights (including control over personal data) and make decisions regarding acceptable uses. Users should periodically be informed in clear, simple language about the scope of data collected, intended uses, and parties granted access. Users should be helped to understand the extent, format, and intended uses of the data obtained by third parties. Ideally, these disclosures will also include some explanation of the methods and algorithms used to make sense of H-IoT data [68], including profiling measures and the impact of profiling on choices available to the user. The difficulties of such explanations in lay language must be acknowledged; different levels of technical detail, vocabulary and communication media will be required [24,31,32]. User-centric design, as supported by the principle of inclusiveness, can help assess the capacities and needs of different user groups.

As users can change their preferences over time, periodic confirmation of preferences should be included in devices and protocols, in addition to disclosures by H-IoT providers. Re-consent processes can help users retain oversight over movement and secondary processing of their data. By taking on the responsibility for period re-consent, providers can effectively function as gatekeepers to the network of third parties involved in secondary processing of H-IoT data.

The gatekeeping format presents several potential benefits to users. First, it clearly establishes the party liable for further processing of the user's data, insofar as the provider is responsible for re-confirming consent as needed in accordance with the purposes for which third parties process the user's data. Second, it minimizes the number of parties the user must engage with to retain oversight and control over their data. Legal entities change over time. If providers track access to the user's data, how they are being used, and changes to these uses over time, much of the oversight burden is removed from users. Finally, third parties often have privacy policies or interests different to those of H-IoT providers; potential conflicts within user interests must be highlighted if trust is to be maintained between providers and users. As a gatekeeper, the provider would be responsible for identifying and alerting the user to potential conflicts, rather than the user herself having to remain vigilant.

Operational transparency is critical if H-IoT providers seek to maintain trust and demonstrate respect for the autonomy and privacy of users. Owing to the opacity and complexity of H-IoT and related analytics systems [32,100,101], users are in a highly vulnerable position. As suggested above in relation to group privacy, meaningful control over data collection and processing is normally infeasible for individual users. Transparent operation can reduce user vulnerability in this regard. A trusting operational relationship is key to ethical design of the H-IoT.

3.7. Report the Uncertain Utility of H-IoT Data to Users at the Point of Adoption

Following the principles of respect for autonomy, trust, non-maleficence, and transparency, and to limit possibilities of data misuse and come closer to replicating the protection offered by informed consent, information about data retention and processing aims needs to be available to users before data are collected [36]. Significant risks exist to violate user privacy expectations. Data can be generated that allow for unanticipated, invasive inferences about the user's life [24]. Physiological and activity data combined with location and time stamps provides myriad opportunities for invasive classification and interventions (e.g., real-world targeted advertising enabled by the IoT) [15,102]. Users may assume that they are protected from invasive findings by privacy policies and data protection law [59]. However, the uncertain value and inferences made possible by aggregating H-IoT data cast doubts on the level of protection offered [103,104].

For H-IoT devices to be considered trustworthy, providers should take steps to inform users about the scope of data to be collected, and what the collected data can foreseeably reveal about them. This type of notification can be embedded in informed consent mechanisms that, for instance, report at the point of sale or deployment about the scope and purpose of data collection. Notification is critical to allow users to make an informed choice about the acceptability of data collection and risks within their personal context, or according to the needs of the user if the decision to adopt H-IoT is made by a proxy (e.g., for children or people with an impaired capacity to consent).

To generate the necessary information, a risk analysis should be performed prior to data processing that assesses the uses and types of inferences that may be drawn from H-IoT data. Awareness of the uncertain value of H-IoT data should be raised both at the point of collection and further processing or secondary usage of the data. "Offline" privacy barriers such as physical walls can be replaced by raising awareness among data subjects of the uncertain but broad value and seemingly limitless lifespan of the data outside of the original context in which it was authored. Awareness may inhibit authorship or dissemination of sensitive or particularly context-sensitive data.

Users should also be made aware of the practical arrangements for data storage, processing and exchange. Meaningful explanations of steps to be taken in storing and processing data, and their anticipated uses, need to be available to users throughout a device's lifecycle [36]. Terms of Service and other end-user agreements that allow collection, aggregation, and analysis of H-IoT data without clear indications of how data will be used in the future, beyond general statements about third party access, are not sufficient. In gaining consent from users, H-IoT developers should describe the uncertain value of the data generated and the potential for aggregation and linkage by third parties for academic, commercial, civil, and other purposes.

3.8. Provide Users with Practically Useful Mechanisms to Exercise Meaningful Data Access Rights

Following the principles of trust and autonomy, mechanisms should be included in H-IoT data protocols to help users exercise their data accessibility and portability rights. For access rights to be meaningful, only reasonable effort should be required. As an example, being provided with thousands of printed pages would require unreasonable effort on the part of the data subject to compile and understand the data, and would therefore fail to preserve a meaningful right to access. H-IoT developers should grant users full access to their personal data in a practically useful format. Data should, at a minimum, be provided in a machine-readable format, along with information about the tools necessary to read it [30]. The requirement for data to be provided in a meaningful format is further supported by Article 12 of the General Data Protection Regulation.

However, accessibility and portability come with risks. Unrestricted access to raw data may be harmful if subjects lack the necessary expertise or resources to make sense of it [25,105]. Misinterpretation is a concern when data are assessed without assistance from a trained clinician, service provider or caregiver [106]. H-IoT developers should, therefore, provide not just mere access and portability, but rather meaningful access and portability. That is, additional guidance or training to assist users in understanding the scope and meaning of their data should be available.

3.9. Design Devices to be Unobtrusive According to the Needs of Specific User Groups

Following the principles of respect for autonomy and inclusiveness, the design of H-IoT should account for both the physical and informational obtrusiveness of devices and the data they produce. Sensing technologies can create a sense of obtrusiveness or feelings of "being watched" [107,108]. Likewise, they can be physically obtrusive, owing to difficulty of use, uncomfortable design, or aesthetics. Highly obtrusive H-IoT can disrupt a user's normal behaviour and autonomy. Smart homes have, for example, been shown to exhibit passive control over users, including the alteration of daily routines based on the presence of monitoring [109]. Obtrusive H-IoT can also impact a user's sense of identity, including by exposing the user to stigma. 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 activity being monitored [110]. A person's identity is often affected by an illness or concern which becomes part of their identity, e.g. Alice is a schizophrenic or Bob is a bad sleeper. H-IoT can inadvertently be a catalyst for these concerns.

Design should, therefore, minimize obtrusiveness to protect a user's decision-making autonomy and sense of identity, according to the requirements of specific user groups. 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 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 [74]. However, a balance must be struck; the inclusion of such a feature on devices designed for cognitively impaired users will pose a significant risk to patient safety. H-IoT should also remain visible to some degree to prevent covert monitoring that would raise questions about the validity of consent over time [5,111], particularly among cognitively impaired users in institutional care environments. H-IoT embedded in a home or institutional care environment can be forgotten following extended use [112,113]. Devices should thus be "self-disclosive," meaning their existence, intended uses, and capabilities should be proactively and periodically disclosed to users and unintentionally monitored third parties [74].

4. Two Examples

To unpack how these guidelines can impact H-IoT design in practice, two cases of H-IoT intended for specific user groups will be considered: elderly users and children. The application of the guidelines here is intended as provisional and instructive, and aims to demonstrate how the guidelines can mitigate ethical concerns via design choices.

4.1. H-IoT for Elderly Users

Many H-IoT devices and services are designed to support elderly and infirm users, or to target health conditions that primarily affect the elderly. Wearable, embedded and implantable sensors can be used to monitor a variety of physiological parameters and behaviours. Semi-permanent sensors can also be woven into clothes or wristbands for physiological measurements, including detection of specific molecules in perspiration [114,115] or motion metrics to monitor Parkinson's disease [116]. Software updates and applications can also turn existing devices into wearable monitors, as shown with health monitoring smart phones application that can track exercise or movement and share data with health professionals and other third parties [117,118]. Embedded environmental sensors can unobtrusively provide information about a patient's private space, including "smart home" systems for "ageing at home" or gerontechnologies to support frail patients (e.g., Marubeni's HRS-I, smart pillboxes and furniture, and fall detectors). Implantable, dissolvable wireless sensors can be ingested, injected or attached to the skin to measure pressure, temperature, pH, motion, flow and detect specific biomolecules [119]. Examples include in vivo glucose monitoring chips [120] and implantable stents for blood quality monitoring [78,121].

H-IoT for the elderly often aims to support "ageing-at-home". The health and behaviours of at-risk elderly users can be monitored in their homes by a care team. Devices can alert third parties to emergencies, or enable communication between the users and care teams during emergencies or daily usage. Such applications aim to enhance both the safety and autonomy of users, by allowing for care to be carried out in the home rather than community or professional care settings.

The emphasis on patient safety often seen with H-IoT applications for the elderly can prove ethically problematic. A risk of coercion exists, insofar as elderly users may be left with little choice to use a device suggested by their family or care team. While "ageing-at-home" can support independent living, there is also a risk of social isolation if H-IoT is treated as a replacement for human care, or as a "watchful safety net" that will alert carers in case of an emergency.

Following the guidelines proposed here in the design of H-IoT for elderly users can mitigate many of these concerns. Guidelines 3 and 9 calls for the design of devices and data protocols to be unobtrusive and protect user privacy by default. Following both, systems that monitor the user at home can be designed to collect the least intrusive type of data possible. Avoidance of cameras in embedded sensors is generally seen as privacy enhancing; visual sensors that detect motion, heat, or capture intentionally blurred images are generally seen as less privacy sensitive than full audio/visual capture [98,122]. A fall detection system, for instance, can be designed to detect motion only.

Guidelines 1 and 2 also address user privacy and confidentiality. Sensors that monitor user behaviour on a semi-constant basis collect potentially invasive data, including behaviours unrelated to health or the monitored parameters. "Smart beds", for example, can allow inferences to be made about the user's personal life if a second person is detected. Users should arguably have oversight and choice over the type and extent of data being transmitted to third parties, although user control can potentially undermine the accuracy and comprehensiveness of data collected by the device. Guideline 1 suggests that a balance needs to be struck between user control of data transmission to protect privacy, and the medical interest in accurate information. A device could, for instance, allow users to temporarily disable data storage and transmission, while keeping active monitoring enabled to detect emergencies.

Guideline 5 calls for design that supports the inclusion of medical professionals in H-IoT. A risk exists of using H-IoT with elderly users as a proxy for human care, or to shift care burdens from formal medical and social care institutions to the community and informal carers [2]. For the former, devices can be designed to periodically remind third party carers to visit the user in person to avoid social isolation. For the latter, data protocols can be designed to automatically share data with the user's general practitioner and professional care team. Both the user and informal carers should be able contact a relevant professional with questions or concerns [123], concerning for instance the interpretation of patterns found in the data being collected.

Guideline 8 concerning data access rights is complementary to Guideline 5. Following it, mechanisms should be included for the user to share data with professionals and informal carers as desired, with minimal effort. Doing so ensures that a user can customize and query the care mediated by H-IoT as needed. Similar mechanisms may also be required for informal carers that receive data from H-IoT devices, for instance to allow for contact with medical professionals as described above.

4.2. H-IoT for Children

An increasing number of IoT and H-IoT devices and services are designed for children. Next to the IoT, the "Internet of Toys" is an emerging phenomenon describing Internet-enabled "smart" toys that can collect and transmit data about children. Toys that monitor developmental conditions are one health-related application [124]. Health monitors for children have also proven an area of rapid development, particularly those designed to monitor physiological parameters and behaviours of infants [125].

The safety, effectiveness and impact on parents of health monitors for infants are beginning to garner public attention. Such devices are often not marketed or regulated as medical devices, and thus lack evidence of safety and efficacy normally required to bring a medical device to market [125]. This is concerning for two reasons. First, unproven devices may produce false positives that lead to over-diagnosis, which does not benefit the patient's health and unnecessarily distresses parents and infants alike. False positives also waste valuable limited healthcare resources through unnecessary hospital admissions and testing. Second, unproven devices can provide a false sense of security, insofar as devices promise to create a watchful safety net for concerned parents. Without rigorous clinical testing to prove efficacy, devices designed to improve health and well-being can unintentionally place infants at risk [125]. Parents may be less mindful of physically checking on the child if under the impression the device will provide an alert if anything goes wrong.

Other concerns can be noted that apply to IoT designed for children in general, not only those designed to benefit health and well-being. Internet-enabled toys have recently proven the target of concerns over privacy, confidentiality and security. Toys that record and transmit children's behaviour and conversations, such as the Hello Barbie and Cayla doll, have been shown to lack robust data protection and security standards, placing the child user's privacy at risk [126–128]. Secondary processing by manufacturers and third parties, consented to via terms of service or user agreements, expose children's data to unclear and potentially invasive secondary uses [128,129]. Further, weak security and confidentiality standards can expose this data to access and exploitation by unauthorised third parties.

Again, following the guidelines proposed here can address many of these concerns. Guideline 1 requires users be given control over data collection and transmission. In the case of H-IoT for children, the user will not be able to grant valid consent, meaning parents or guardians will need to protect the interests of child users. Providing options to disable data transmission to the manufacturer and third parties is one plausible option to protect user privacy and safety, although it may disrupt the service provided by the device. Given that child users cannot reasonably assess the risks of the data collected by H-IoT, and thus cannot make informed decisions of what is shared with the device or when the device should be disabled to avoid invasive data collection, parents and guardians can be given interfaces to review data transmission. This does not necessarily equate to full review of collected data; parents being able to listen to all conversations collected by an IoT toy would be invasive. Rather, Guideline 1 suggests that parents should be given options to define context appropriate transmission rules to preserve the child's privacy and safety.

Guideline 2 is similarly important, insofar as any data collected from children are highly sensitive. Protecting devices from third party attacks and limiting sharing of data with third party data controllers according to legal and industry standards are crucial to ensure confidentiality, without which devices are unlikely to be adopted.

Application of Guideline 3 is not as straightforward. While the privacy of child users must be respected, providing children with an option to disable the device can cause significant distress for parents and guardians, and pose a safety risk if the device is relied upon as a means of health or safety monitoring. Allowing the child to disable a GPS tracking device, for instance, can pose a serious safety risk. Application of Guideline 3 is therefore highly context- and device-dependent. However, as suggested above, parents and guardians at a minimum should be provided mechanisms to limit transmission of data about the child user. Default settings for data collection and transmission should similarly be set to the most privacy-enhancing option, and require an intentional choice from the parent or guardian to transmit data to a third party. Terms of Service and user agreements cannot be relied upon to ensure users make an informed choice, particularly when a proxy of the user is responsible for making the decision.

Guideline 5 is particularly important for H-IoT devices targeted at monitoring the health of infants and children. Concerns have recently been raised over the marketing of health monitoring for infants that plays on the concerns over child safety felt by new parents. As suggested by Guideline 5, such exploitative marketing practices can lead to unnecessary distress for parents and guardians and waste of limited healthcare resources due to false positives. On the other hand, devices lacking robust clinical testing and evidence of efficacy can pose a safety hazard to child users if they are perceived as reliable medical devices by parent users. It is thus critical that devices are both thoroughly tested to the standards normally expected of medical devices, and designed to facilitate assessment of collected data and alerts by medical professionals. Both requirements aim to ensure that H-IoT devices for children do not create a safety hazard for users, and distress parents and guardians seeking peace of mind through their usage.

5. Conclusions

As the discussion above of the nine ethical principles and guidelines for design of the H-IoT indicates, a delicate balance must be struck between user, developer and public health interests. Future development of principles for ethical design of H-IoT will depend in large part on the potential crossover between consumer and clinical devices and datasets. The potential value of H-IoT datasets for medical research and consumer analytics exists across both types of H-IoT. Whether and how this crossover can occur in practice to allow data sharing among medical, academic, government, and commercial entities remains to be seen. Regardless of how data are shared, ethical design of the contributing H-IoT devices, and data collection protocols is essential to ensure user interests are afforded sufficient protection. Adopting these and similar guidelines are in the interests of all stakeholders in the run up to a H-IoT device or service entering the market. With proactive and meaningful self-regulation, developers demonstrate accountability and trustworthiness, while easing the need for reactive and overly restrictive regulation.

Acknowledgments: 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.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kubitschke, L.; Cullen, K.; Műller, S. *ICT & Ageing: European Study on Users, Markets and Technologies–Final Report*; European Commission: Brussels, Belgium, 2010.
2. Mittelstadt, B.; Fairweather, N.B.; Shaw, M.; McBride, N. The ethical implications of personal health monitoring. *Int. J. Tech.* **2014**, *5*, 37–60. [CrossRef]
3. Lupton, D. The commodification of patient opinion: the digital patient experience economy in the age of big data. *Sociol. Health Illn.* **2014**, *36*, 856–869. [CrossRef] [PubMed]
4. Lyon, D. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*; Routledge: London, UK, 2003.
5. Bowes, A.; Dawson, A.; Bell, D. Ethical implications of lifestyle monitoring data in ageing research. *Inf. Commun. Soc.* **2012**, *15*, 5–22. [CrossRef]
6. Edgar, A. The expert patient: Illness as practice. *Med. Health Care Philos.* **2005**, *8*, 165–171. [CrossRef] [PubMed]
7. Pellegrino, E.D.; Thomasma, D.C. *The Virtues in Medical Practice*; Oxford University Press: New York, NY, USA, 1993.
8. Beauchamp, T.L.; Childress, J.F. *Principles of Biomedical Ethics*; Oxford University Press: New York, NY, USA, 2009.
9. Woodward, R. *The OECD Privacy Framework*; Organisation for Economic Co-operation and Development; Routledge: Abingdon-on-Thames, UK, 2009. Available online: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed on 30 June 2017).
10. Schaefer, G.O.; Emanuel, E.J.; Wertheimer, A. The obligation to participate in biomedical research. *J. Am. Med. Assoc.* **2009**, *302*, 67–72. [CrossRef] [PubMed]
11. Chadwick, R.; Berg, K. Solidarity and equity: new ethical frameworks for genetic databases. *Nat. Rev. Genet.* **2001**, *2*, 318–321. [CrossRef] [PubMed]
12. Mittelstadt, B.; Benzler, J.; Engelmann, L.; Prainsack, B.; Vayena, E. Is there a duty to participate in digital epidemiology? *Life Sci. Soc. Policy* **2017**, in press.
13. Dove, E.S.; Knoppers, B.M.; Zawati, M.H. Towards an ethics safe harbor for global biomedical research. *J. Law Biosci.* **2014**, *1*, 3–51. [CrossRef] [PubMed]
14. Gao, T.; Pesto, C.; Selavo, L.; Chen, Y.; Ko, J.G.; Lim, J.H.; Terzis, A.; Watt, A.; Jeng, J.; Chen, B. Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results. In Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA, 12–13 May 2008.
15. Brey, P. Freedom and privacy in ambient intelligence. *Eth. Inf. Technol.* **2005**, *7*, 157–166. [CrossRef]
16. Remmers, H. Environments for ageing, assistive technology and self-determination: Ethical perspectives. *Inform. Health Soc. Care* **2010**, *35*, 200–210. [CrossRef] [PubMed]
17. Ananny, M. Toward an ethics of algorithms convening, observation, probability, and timeliness. *Sci. Technol. Hum. Values* **2016**, *41*, 93–117. [CrossRef]
18. Floridi, L. The informational nature of personal identity. *Minds Mach.* **2011**, *21*, 549–566. [CrossRef]
19. Johnson, J.A. *Ethics of Data Mining and Predictive Analytics in Higher Education*; Social Science Research Network: Rochester, NY, USA, 2013.
20. Coll, S. Consumption as biopower: Governing bodies with loyalty cards. *J. Consum. Cult.* **2013**, *13*, 201–220. [CrossRef]
21. Landau, R.; Werner, S.; Auslander, G.K.; Shoval, N.; Heinik, J. What do cognitively intact older people think about the use of electronic tracking devices for people with dementia? A preliminary analysis. *Int. Psychogeriatr.* **2010**, *22*, 1301–1309. [CrossRef] [PubMed]
22. Topo, P. Technology studies to meet the needs of people with dementia and their caregivers a literature review. *J. Appl. Gerontol.* **2009**, *28*, 5–37. [CrossRef]
23. Choudhury, S.; Fishman, J.R.; McGowan, M.L.; Juengst, E.T. Big data, open science and the brain: Lessons learned from genomics. *Front. Hum. Neurosci.* **2014**, *8*, 239. [CrossRef] [PubMed]
24. Mittelstadt, B.; Floridi, L. The ethics of big data: Current and foreseeable issues in biomedical contexts. *Sci. Eng. Eth.* **2016**, *22*, 303–341. [CrossRef] [PubMed]
25. Coll, S. Power, knowledge, and the subjects of privacy: Understanding privacy as the ally of surveillance. *Inf. Commun. Soc.* **2014**, *17*, 1250–1263. [CrossRef]
26. Richards, N.M.; King, J.H. Three paradoxes of big data. *Stanf. Law Rev. Online* **2013**, *66*, 41.

27. TechUK. *Trust in an Internet of Things World*; TechUK: London, UK, 2017. Available online: https://www.techuk.org/component/techuksecurity/security/download/10031?file=IoT_Trust.pdf&Itemid=177&return=aHR0cHM6Ly93d3cudGVjaHVrLm9yZy9pbnNpZ2h0cy9uZXdzL2l0ZW0vMTAwMzEtaW90LXRydXN0LXByaW5jaXBsZXM= (accessed on 30 June 2017).
28. Kitchin, R. *The Data Revolution: Big data, Open Data, Data Infrastructures and Their Consequences*; CPI Group: Croydon, UK, 2014.
29. Pasquale, F.; Ragone, T.A. Protecting health privacy in an era of big data processing and cloud computing. *Stan. Tech. L. Rev.* **2013**, *17*, 595–654.
30. Tene, O.; Polonetsky, J. Big data for all: Privacy and user control in the age of analytics. *Northwest. J. Technol. Intellect. Prop.* **2013**, *11*, 239–273.
31. Mittelstadt, B.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L. The ethics of algorithms: Mapping the debate. *Big Data Soc.* **2016**, *3*, 2053951716679679. [CrossRef]
32. Burrell, J. How the machine "thinks:" understanding opacity in machine learning algorithms. *Big Data Soc.* **2016**, *3*, 2053951715622512. [CrossRef]
33. Wel, L.; Royakkers, L. Ethical issues in web data mining. *Ethics Inf. Technol.* **2004**, *6*, 129–140.
34. Schermer, B.W. The limits of privacy in automated profiling and data mining. *Comput. Law Secur. Rev.* **2011**, *27*, 45–52. [CrossRef]
35. Floridi, L. The ontological interpretation of informational privacy. *Eth. Inf. Technol.* **2005**, *7*, 185–200. [CrossRef]
36. Kosta, E.; Pitkänen, O.; Niemelä, M.; Kaasinen, E. Mobile-centric ambient intelligence in Health- and Homecare-anticipating ethical and legal challenges. *Sci. Eng. Eth.* **2010**, *16*, 303–323. [CrossRef] [PubMed]
37. Friedewald, M.; Vildjiounaite, E.; Punie, Y.; Wright, D. Privacy, identity and security in ambient intelligence: A scenario analysis. *Telemat. Inform.* **2007**, *24*, 15–29. [CrossRef]
38. Moncrieff, S.; Venkatesh, S.; West, G. A framework for the design of privacy preserving pervasive healthcare. In Proceedings of the 2009 IEEE International Conference on Multimedia and Expo, New York, NY, USA, 28 June–2 July 2009.
39. Terry, N. Health privacy is difficult but not impossible in a post-hipaa data-driven world. *Chest* **2014**, *146*, 835–840. [CrossRef] [PubMed]
40. Moore, P.; Xhafa, F.; Barolli, L.; Thomas, A. Monitoring and Detection of Agitation in Dementia: Towards Real-Time and Big-Data Solutions. In Proceedings of the 2013 Eighth International Conference on P2P Parallel Grid Cloud Internet Computing (3PGCIC), Compiegne, France, 28–30 October 2013.
41. Shilton, K. Participatory personal data: An emerging research challenge for the information sciences. *J. Am. Soc. Inf. Sci. Technol.* **2012**, *63*, 1905–1915. [CrossRef]
42. Markowetz, A.; Błaszkiewicz, K.; Montag, C.; Switala, C.; Schlaepfer, T.E. Psycho-informatics: Big data shaping modern psychometrics. *Med. Hypotheses* **2014**, *82*, 405–411. [CrossRef] [PubMed]
43. Schadt, E.E. The changing privacy landscape in the era of big data. *Mol. Syst. Biol.* **2012**, *8*, 612. [CrossRef] [PubMed]
44. Goodman, E. Design and ethics in the era of big data. *Interactions* **2014**, *21*, 22–24. [CrossRef]
45. Hayden, E.C. A Broken Contract. *Nature* **2012**, *486*, 312–314. [CrossRef] [PubMed]
46. Joly, Y.; Dove, E.S.; Knoppers, B.M.; Bobrow, M.; Chalmers, D. Data sharing in the post-genomic world: The experience of the International Cancer Genome Consortium (ICGC) Data Access Compliance Office (DACO). *PLoS Comput. Biol.* **2012**, *8*, e1002549. [CrossRef] [PubMed]
47. McGuire, A.L.; Achenbaum, L.S.; Whitney, S.N.; Slashinski, M.J.; Versalovic, J.; Keitel, W.A.; McCurdy, S.A. Perspectives on human microbiome research ethics. *J. Empir. Res. Hum. Res. Eth. Int. J.* **2012**, *7*, 1–14.
48. Nissenbaum, H. *Privacy as Contextual Integrity*; Social Science Research Network: Rochester, NY, USA, 2004.
49. Liyanage, H.; de Lusignan, S.; Liaw, S.T.; Kuziemsky, C.E.; Mold, F.; Krause, P.; Fleming, D.; Jones, S. Big data usage patterns in the health care domain: A use case driven approach applied to the assessment of vaccination benefits and risks. *Yearb. Med. Inform.* **2014**, *9*, 27–35. [CrossRef] [PubMed]
50. Fairfield, J.; Shtein, H. Big data, big problems: Emerging issues in the ethics of data science and journalism. *J. Mass Media Eth.* **2014**, *29*, 38–51. [CrossRef]
51. Sloot, B. Privacy in the Post-NSA era: Time for a fundamental revision? *JIPITEC* **2014**, *1*, 1–11.
52. Docherty, A. Big data-ethical perspectives. *Anaesthesia* **2014**, *69*, 390–391. [CrossRef] [PubMed]

53. Article 29 Data Protection Working Party Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC. 2014. Available online: http://www.dataprotection.ro/servlet/ViewDocument?id=1086 (accessed on 30 June 2017).
54. Bagüés, S.A.; Zeidler, A.; Klein, C.; Valdivielso, F.; Matias, R. Enabling personal privacy for pervasive computing environments. *J. Univers. Comput. Sci.* **2010**, *16*, 341–371.
55. Little, L.; Briggs, P. Pervasive healthcare: The elderly perspective. In Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments, Corfu, Greece, 9–13 June 2009.
56. Chakraborty, S.; Choi, H.; Srivastava, M.B. Demystifying Privacy in Sensory Data: A QoI Based Approach. In Proceedings of the 2011 9th IEEE International Conference on Pervasive Computing and Communications Workshops, Seattle, WA, USA, 21–25 March 2011.
57. Coughlin, J.F.; Lau, J.; D'Ambrosio, L.A.; Reimer, B. Adult Children's Perceptions of Intelligent Home Systems in the Care of Elderly Parents. In Proceedings of the 3rd International Convention on Rehabilitation Engineering and Assistive Technology, Singapore, 22–26 April 2009.
58. Dhukaram, A.V.; Baber, C.; Elloumi, L.; Van Beijnum, B.J.; De Stefanis, P. End-User Perception Towards Pervasive Cardiac Healthcare Services: Benefits, Acceptance, Adoption, Risks, Security, Privacy and Trust. In Proceedings of the 2011 5th International Conference on Pervasive Computing Technologies for Healthcare and Workshops, Dublin, Ireland, 23–26 May 2011.
59. Rashid, U.; Schmidtke, H.; Woo, N. *Managing Disclosure of Personal Health Information in Smart Home Healthcare*; Springer: New York, NY, USA, 2007; pp. 188–197.
60. Wang, K.; Sui, Y.; Zou, X.; Durresi, A.; Fang, S. Pervasive and Trustworthy Healthcare. In Proceedings of the 22nd International Conference on Advanced Information Networking and Applications-Workshops, AINAW 2008, Gino-wan, Okinawa, Japan, 25–28 March 2008.
61. Yuan, W.; Guan, D.; Lee, S.; Lee, Y.K. The Role of Trust in Ubiquitous Healthcare. In Proceedings of the 9th International Conference on e-Health Networkin, Application and Services, Taipei, Taiwan, 19–22 June 2007.
62. Turilli, M.; Vaccaro, A.; Taddeo, M. The case of online trust. *Knowl. Technol. Policy* **2010**, *23*, 333–345. [CrossRef]
63. Taddeo, M. Trust in technology: A distinctive and a problematic relation. *Knowl. Technol. Policy* **2010**, *23*, 283–286. [CrossRef]
64. Taddeo, M.; Floridi, L. The case for e-trust. *Eth. Inf. Technol.* **2011**, *13*, 1–3. [CrossRef]
65. McLean, A. Ethical frontiers of ICT and older users: Cultural, pragmatic and ethical issues. *Eth. Inf. Technol.* **2011**, *13*, 313–326. [CrossRef]
66. Hildebrandt, M.; Koops, B.J. The challenges of ambient law and legal protection in the profiling era. *Mod. Law Rev.* **2010**, *73*, 428–460. [CrossRef]
67. Floridi, L. Mature information societies—A matter of expectations. *Philos. Technol.* **2016**, *29*, 1–4. [CrossRef]
68. Wachter, S.; Mittelstadt, B.; Floridi, L. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *Int. Data Priv. Law* **2017**, *7*, 76–99. [CrossRef]
69. Giannotti, F.; Saygin, Y. *Privacy and Security in Ubiquitous Knowledge Discovery*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 75–89.
70. Percival, J.; Hanson, J. Big brother or brave new world? Telecare and its implications for older people's independence and social inclusion. *Crit. Soc. Policy* **2006**, *26*, 888–909. [CrossRef]
71. Garcia-Morchon, O.; Falck, T.; Wehrle, K. Sensor network security for pervasive e-health. *Secur. Commun. Netw.* **2011**, *4*, 1257–1273. [CrossRef]
72. Massacci, F.; Nguyen, V.H.; Saidane, A. No purpose, No Data: Goal-Oriented Access Control Forambient Assisted Living. In Proceedings of the 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, IL, USA, 13 November 2009.
73. Bagüés, S.A.; Zeidler, A.; Valdivielso, F.; Matias, R. Disappearing for a while—Using white lies in pervasive computing. In Proceedings of the 2007 ACM workshop on Privacy in electronic society, Alexandria, VA, USA, 29 October 2007.
74. Greenfield, A. Some guidelines for the ethical development of ubiquitous computing. *Philos. Trans. R. Soc. Math. Phys. Eng. Sci.* **2008**, *366*, 3823–3831. [CrossRef] [PubMed]
75. Roman, R.; Najera, P.; Lopez, J. Securing the internet of things. *Computer* **2011**, *44*, 51–58. [CrossRef]

76. Genus, A.; Coles, A. On constructive technology assessment and limitations on public participation in technology assessment. *Technol. Anal. Strateg. Manag.* **2005**, *17*, 433–443. [CrossRef]
77. Joss, S.; Bellucci, S. *Participatory Technology Assessment: European Perspectives*; Centre for the Study of Democracy, University of Westminster: London, UK, 2002.
78. Gaul, S.; Ziefle, M. *Smart Home Technologies: Insights into Generation-Specific Acceptance Motives*; Springer: Berlin, Germany, 2009; pp. 312–332.
79. Ziefle, M.; Röcker, C.; Holzinger, A. Medical technology in smart homes: Exploring the user's perspective on privacy, intimacy and trust. In Proceedings of the 35th Annual Computer Software and applications Conference Workshops (COMPSACW), Munich, Germany, 18–22 July 2011.
80. OTA Releases IoT Trust Framework. 2016. Available online: https://otalliance.org/news-events/press-releases/ota-releases-iot-trust-framework (accessed on 29 June 2017).
81. International Telecommunications Union H.810: Interoperability Design Guidelines for Personal Health Systems 2016. Available online: https://www.itu.int/rec/T-REC-H.810 (accessed on 29 June 2017).
82. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. 2014. Available online: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm419118.htm (accessed on 29 June 2017).
83. Postmarket Management of Cybersecurity in Medical Devices. 2016. Available online: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (accessed on 29 June 2017).
84. Knoppers, B.M.; Harris, J.R.; Tassé, A.M.; Budin-Ljøsne, I.; Kaye, J.; Deschênes, M.; Zawati, M.H. Towards a data sharing code of conduct for international genomic research. *Genome Med.* **2011**, *3*, 46. [CrossRef] [PubMed]
85. Clayton, E.W. Informed consent and biobanks. *J. Law. Med. Eth.* **2005**, *33*, 15–21. [CrossRef]
86. Ioannidis, J.P.A. Informed consent, big data, and the oxymoron of research that is not research. *Am. J. Bioeth.* **2013**, *13*, 40–42. [CrossRef] [PubMed]
87. Majumder, M.A. Cyberbanks and other virtual research repositories. *J. Law. Med. Eth.* **2005**, *33*, 31–39. [CrossRef]
88. Kaye, J.; Whitley, E.A.; Lund, D.; Morrison, M.; Teare, H.; Melham, K. Dynamic consent: A patient interface for twenty-first century research networks. *Eur. J. Hum. Genet.* **2015**, *23*, 141–146. [CrossRef] [PubMed]
89. MacIntyre, A. *After Virtue: A Study in Moral Theory*, 3rd ed.; Gerald Duckworth: New York, NY, USA, 2007.
90. Terry, N. Protecting patient privacy in the age of big data. *UMKC Rev.* **2012**, *81*, 385. [CrossRef]
91. Barry, C.A.; Stevenson, F.A.; Britten, N.; Barber, N.; Bradley, C.P. Giving voice to the lifeworld. More humane, more effective medical care? A qualitative study of doctor-patient communication in general practice. *Soc. Sci. Med.* **2001**, *53*, 487–505. [CrossRef]
92. Lupton, D. The digitally engaged patient: self-monitoring and self-care in the digital health era. *Soc. Theory Health* **2013**, *11*, 256–270. [CrossRef]
93. Coeckelbergh, M. E-care as craftsmanship: virtuous work, skilled engagement, and information technology in health care. *Med. Health Care Philos.* **2013**, *16*, 807–816. [CrossRef] [PubMed]
94. Morris, D.B. About suffering: Voice, genre, and moral community. *Daedalus* **1996**, *125*, 25–45.
95. Stutzki, R.; Weber, M.; Reiter-Theil, S. Finding their voices again: a media project offers a floor for vulnerable patients, clients and the socially deprived. *Med. Health Care Philos.* **2013**, *16*, 739–750. [CrossRef] [PubMed]
96. Chan, M.; Estève, D.; Escriba, C.; Campo, E. A review of smart homes—Present state and future challenges. *Comput. Methods Programs Biomed.* **2008**, *91*, 55–81. [CrossRef] [PubMed]
97. Palm, E. Who cares? Moral obligations in formal and informal care provision in the light of ICT-based home care. *Health Care Anal.* **2013**, *21*, 171–188. [CrossRef] [PubMed]
98. Zwijsen, S.A.; Niemeijer, A.R.; Hertogh, C.M.P.M. Ethics of using assistive technology in the care for community-dwelling elderly people: An overview of the literature. *Aging Ment. Health* **2011**, *15*, 419–427. [CrossRef] [PubMed]
99. Wu, Y.-H.; Fassert, C.; Rigaud, A.S. Designing robots for the elderly: Appearance issue and beyond. *Arch. Gerontol. Geriatr.* **2012**, *54*, 121–126. [CrossRef] [PubMed]
100. Mittelstadt, B. Auditing for Transparency in Content Personalization Systems. *Int. J. Commun.* **2016**, *10*, 12.
101. Cath, C.J.N.; Wachter, S.; Mittelstadt, B.; Taddeo, M.; Floridi, L. *Artificial Intelligence and the "Good Society": The US, EU, and UK Approach*; Social Science Research Network: Rochester, NY, USA, 2016.

102. Howard, P.N. *Pax. Technica.: How the Internet of Things May Set Us Free or Lock Us Up*; Yale University Press: New Haven, London, UK, 2015.
103. Mittelstadt, B. From individual to group privacy in big data analytics. *Philos. Technol.* **2017**, 1–20. [CrossRef]
104. Taylor, L.; Floridi, L.; van der Sloot, B. *Group Privacy: New Challenges of Data Technologies*; Springer: New York, NY, USA, 2017.
105. Boyd, D.; Crawford, K. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Inf. Commun. Soc.* **2012**, *15*, 662–679.
106. Watson, R.W.G.; Kay, E.W.; Smith, D. Integrating biobanks: Addressing the practical and ethical issues to deliver a valuable tool for cancer research. *Nat. Rev. Cancer* **2010**, *10*, 646–651. [CrossRef] [PubMed]
107. Hensel, B.K.; Demiris, G.; Courtney, K.L. Defining obtrusiveness in home telehealth technologies: A conceptual framework. *J. Am. Med. Inform. Assoc.* **2006**, *13*, 428–431. [CrossRef] [PubMed]
108. Nefti, S.; Manzoor, U.; Manzoor, S. Cognitive agent based intelligent warning system to monitor patients suffering from dementia using ambient assisted living. In Proceedings of the 2010 International Conference on the Information Society (i-Society), London, UK, 28–30 June 2010.
109. Tiwari, P.; Warren, J.; Day, K.J.; McDonald, B. Some non-technology implications for wider application of robots assisting older people. *Health Care Inform. Rev. Online* **2010**, *14*, 2–11.
110. Courtney, K.L. Privacy and senior willingness to adopt smart home information technology in residential care facilities. *Method. Inf. Med.* **2008**, *47*, 76–81. [CrossRef]
111. Kenner, A.M. Securing the elderly body: Dementia, surveillance, and the politics of "aging in place". *Surveill. Soc.* **2008**, *5*, 252–269.
112. Essén, A. The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices. *Soc. Sci. Med.* **2008**, *67*, 128–136. [CrossRef] [PubMed]
113. van Hoof, J.; Kort, H.S.M.; Rutten, P.G.S.; Duijnstee, M.S.H. Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users. *Int. J. Med. Inf.* **2011**, *80*, 310–331. [CrossRef] [PubMed]
114. Gao, W.; Emaminejad, S.; Nyein, H.Y.Y.; Challa, S.; Chen, K.; Peck, A.; Fahad, H.M.; Ota, H.; Shiraki, H.; Kiriya, D.; et al. Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis. *Nature* **2016**, *529*, 509–514. [CrossRef] [PubMed]
115. Lee, H.; Choi, T.K.; Lee, Y.B.; Cho, H.R.; Ghaffari, R.; Wang, L.; Choi, H.J.; Chung, T.D.; Lu, N.; Hyeon, T.; et al. A graphene-based electrochemical device with thermoresponsive microneedles for diabetes monitoring and therapy. *Nat. Nanotechnol.* **2016**, *11*, 566–572. [CrossRef] [PubMed]
116. Pasluosta, C.F.; Gassner, H.; Winkler, J.; Klucken, J.; Eskofier, B.M. An emerging era in the management of Parkinson's Disease: Wearable technologies and the Internet of things. *IEEE J. Biomed. Health Inform.* **2015**, *19*, 1873–1881. [CrossRef] [PubMed]
117. Boulos, M.N.K.; Wheeler, S.; Tavares, C.; Jones, R. How smartphones are changing the face of mobile and participatory healthcare: An overview, with example from eCAALYX. *Biomed. Eng. Online* **2011**, *10*. [CrossRef] [PubMed]
118. Pentland, A.; Lazer, D.; Brewer, D.; Heibeck, T. Using reality mining to improve public health and medicine. *Stud. Health Technol. Inf.* **2009**, *149*, 93–102.
119. Kang, S.K.; Murphy, R.K.J.; Hwang, S.W.; Lee, S.M.; Harburg, D.V.; Krueger, N.A.; Shin, J.; Gamble, P.; Cheng, H.; Yu, S.; et al. Bioresorbable silicon electronic sensors for the brain. *Nature* **2016**, *530*, 71–76. [CrossRef] [PubMed]
120. PositiveID PositiveID Corporation^{TM} –GlucoChip. Available online: http://www.positiveidcorp.com/products_glucochip.html (accessed on 12 April 2013).
121. Pousaz, L. Under the Skin, a Tiny Laboratory. Available online: http://actu.epfl.ch/news/under-the-skin-a-tiny-laboratory/ (accessed on 12 April 2013).
122. Courtney, K.L.; Demiris, G.; Hensel, B.K. Obtrusiveness of information-based assistive technologies as perceived by older adults in residential care facilities: A secondary analysis. *Med. Inform. Internet Med.* **2007**, *32*, 241–249. [CrossRef] [PubMed]
123. Ure, J.; Pinnock, H.; Hanley, J.; Kidd, G.; McCall Smith, E.; Tarling, A.; Pagliari, C.; Sheikh, A.; MacNee, W.; McKinstry, B. Piloting tele-monitoring in COPD: A mixed methods exploration of issues in design and implementation. *Prim. Care Respir. J.* **2012**, *21*, 57–64. [CrossRef] [PubMed]

124. Martin-Ruiz, M.L.; Valero, M.A.; Lindén, M.; Nunez-Nagy, S.; Garcia, A.G. Foundations of a smart toy development for the early detection of motoric impairments at childhood. *Int. J. Pediatr. Res.* **2015**, *1*, 1–5. [CrossRef]
125. Bonafide, C.P.; Jamison, D.T.; Foglia, E.E. The emerging market of smartphone-integrated infant physiologic monitors. *JAMA* **2017**, *317*, 353–354. [CrossRef] [PubMed]
126. Dobbins, D.L. Analysis of Security Concerns & Privacy Risks of Children'S Smart Toys. Ph.D Thesis, Washington University, Louis, MO, USA, 2015.
127. Munro, K. Fight! Fight! Hello Barbie vs My Friend Cayla | Pen Test Partners. Available online: https://www.pentestpartners.com/blog/fight-fight-hello-barbie-vs-my-friend-cayla/ (accessed on 29 January 2017).
128. Gross, G. Privacy groups urge investigation of "internet of toys". *Computerworld*, 2016. Available online: http://www.computerworld.com/article/3147624/internet-of-things/privacy-groups-urge-investigation-of-internet-of-toys.html (accessed on 30 June 2017).
129. Mascheroni, G. The internet of toys. *Parent. Digit. Future* 2017. Available online: http://eprints.lse.ac.uk/76134/ (accessed on 29 June 2017).