European Commission

JRC TECHNICAL REPORTS

Wearable Sensors and Digital Platforms in Health: empowering citizens through trusted and trustworthy ICT technology

TRUDI
Deliverable 3.1

Monica Gemo
Davide Lunardi
Mariachiara Tallacchini

2015

Report EUR 27045 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Institute for the Protection and Security of the Citizen

Contact information
Monica Gemo
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 360, 21027 Ispra (VA), Italy
E-mail: monica.gemo@jrc.ec.europa.eu
Tel.: +39 0332 78 3081
Fax: +39 0332 78 5145

JRC Science Hub
https://ec.europa.eu/jrc

This publication is a Technical Report by the Joint Research Centre of the European Commission.

JRC93275

EUR 27045 EN

ISBN 978-92-79-44733-4

ISSN 1831-9424

doi:10.2788/788525

Luxembourg: Publications Office of the European Union, 2015

Contents

Executive Summary 5
1. Introduction 7
2. Some ethical and legal reflections: By-Design and In-Design forms of protection in ICT 9
2.1. Privacy-by-Design 9
2.1.1. The 'information society' 9
2.1.2. The concept of Privacy by Design 10
2.1.3. Practical applications of Privacy-by-Design principles 14
2.1.4. Strategies for the implementation of Privacy-by-Design 15
2.2. Rights-in-Design: citizen rights in digital architectures 17
2.2.1. A matter of architecture: the normativity of digital artifacts 17
2.2.2. Towards individual legal entitlements in the design 20
2.2.3. Rights-in-design as enhanced agency in ICT 21
3. Emerging wearable sensors for health activities 25
3.1. Definition(s) and classification(s) of wearable sensors 25
3.2. Scope of the analysis for health activities 28
3.3. Sensing Technology of Interest 29
3.3.1. Environmental gas sensors 30
3.3.2. Electromechanical sensors 31
3.3.3. Electrical sensors 32
3.3.4. Optical sensors 33
3.4. Capabilities of wearable sensors 35
3.4.1. Functionalities 35
3.4.2. Usability criteria 38
3.4.3. By design normativity 38
3.4.4. In-design customisations 39
3.4.5. Openness 39
3.4.6. Interoperability 40
3.5. Empirical testing of sample devices 41
3.5.1. Functionalities 42
3.5.2. Usability criteria 43
3.5.3. By-design normativity and in-design customisation 43
3.5.4. Openness 46
3.5.5. Interoperability 47
4. Digital platforms for health activities 49
4.1. Definition(s) and classification(s) of digital health platforms 49
4.2. Scope of the analysis for health activities 51
4.3. Capabilities of quantified self tracking systems 53
4.3.1. Functionalities 54
4.3.2. Usability criteria 55
4.3.3. By design normativity 55
4.3.4. In-design customisations 56
4.3.4. Openness 56
4.3.5. Interoperability 57

4.4. Empirical testing of sample platforms 58
4.4.1. Functionalities 58
4.4.2. Usability criteria 61
4.4.3. By-design normativity and in-design customization 61
4.4.4. Openness 61
4.4.5. Interoperability 62
5. Conclusions 65
References 69
References on ethical and legal reflections 69
References on Privacy-by-Design 69
References on Rights-in-Design 71
References on wearable sensors and health platforms 72
Annexes 81
Annex 1. Results of empirical testing of wearable sensors 83
Annex 2. Results of empirical testing of digital health platforms 95

WEARABLE SENSORS AND DIGITAL PLATFORMS IN HEALTH: empowering citizens through trusted and trustworthy ICT technology

Executive Summary

The JRC project on Trust in Digital Interactions (TRUDI) deals with the construction and renewal of confident and trusted relationships among institutions, corporations and citizens, addressed as a major and urgent issue to be solved. The present report examines relationships for nurturing trust between corporations and citizens. In this context the JRC investigated wearable sensors and digital platforms in health as an empirical case study of citizens' involvement in designing the values embedded in information systems and services as well as their implementation and management.

Personal wearable sensors could become the most powerful individual self-surveillance technology available to citizens. These ubiquitous, networked devices currently offer a breadth of capabilities to sense, digitally enhance and upload data of fine granularity such as body and health physiological functions, images, locations, sounds and motion. However, for wider adoption, it is crucial for citizens/end-users to rely on trusted and trustworthy implementations of wearable sensing technologies. Trusted systems are defined as systems functioning normally and delivering what it is promised and what the user expects, whereas trustworthiness is mostly objectively defined according to specific criteria and can be considered a metric for how much a system deserve the trust of its users (Kounelis et al. 2014). Therefore, in order to establish criteria for trust and trustworthiness, the present report aims to screen and analyse emerging solutions and architectures for verifying how these systems actually work; particularly, for checking whether functionalities, motivations and values embedded in their design hold the potential for user empowerment, equitable use and meaningful community participation in digital health platforms.

As a whole, the report provides a characterization of emerging wearable sensors and digital platforms for health activities according to identified criteria for trust and trustworthiness. These criteria specifically encompass certain normative features, embedded in the systems and aimed at providing citizens/users with powers of control and choice over the devices. Beside increasing citizens/users' trust, these normative measures—specifically by-design and in design forms of rights protection) also allow to improve agency, namely citizens/users' ability to autonomously control the system (Chapter 2). Chapters 3 and 4 review in detail some specific wearable devices and platforms chosen amongst the most popular ones, with attention to provide an overview of different technologies and technological approaches.

The report ends (Chapter 5) with a summary of the main considerations on trust and trustworthiness in current wearable sensors and digital platforms and offers emerging perspectives towards truly citizen centric developments of personal and community health technology. Some recommendations are presented and proposed for enhancing trust and trustworthiness in future personal and community health solutions.

1. Introduction

Personal wearable sensors could become the most powerful individual self-surveillance technology available to citizens. The market of wearable technology is on the rise with a sale increase of more 200% during the present year (Forlani 2014). These ubiquitous, networked devices currently offer a breadth of capabilities to sense, digitally enhance and upload data of fine granularity such as body and health measurements, images, location, sound and motion.

However, for wider adoption, it is crucial for end-users to rely on trusted and trustworthy implementations of wearable sensing technologies. Trusted systems are defined as systems functioning normally and delivering what it is promised and what the user expects, whereas trustworthiness is mostly objectively defined according to specific criteria and can be considered a metric for how much a system deserve the trust of its users (Kounelis et al. 2014). Therefore, in order to establish criteria for trust and trustworthiness, the present report aims to screen and analyse emerging solutions and architectures for verifying how these systems actually work; particularly, for checking whether functionalities, motivations and values embedded in their design hold the potential for user empowerment, equitable use and meaningful community participation in digital health platforms. As a whole, the report provides a characterization of emerging wearable sensors and digital platforms for health activities according to identified criteria for trust and trustworthiness. These criteria specifically encompass certain normative features, embedded in the systems and aimed at providing citizens/users with powers of control and choice over the devices. Beside increasing citizens/users' trust, these normative measures—specifically by-design and in design forms of rights protection) also allow to improve agency, namely citizens/users' ability to autonomously control the system (Chapter 2).

Using empirical data gathered from knowledge assessment and software testing, wearable technology will be reviewed in order to qualify key features and best practices as suitable to respond to trusted and trustworthy self-documentation in participatory

health platforms. The review will cover core functional and ethical dimensions of wearable sensing devices and platforms, as follows:

- **Functionalities** enabling data collection, sophisticated mash-up processing and data interpretation. The aim of the analysis is to highlight transparency of processing steps, actions and decisions incorporated in technology designs;
- **Usability criteria.** Aspects of concern include the ease of use of the devices evaluating their functionality and compatibility with user expectations especially important in age-friendly environments.
- **By-design normative protections**, such as implemented safety, security and privacy default measures in individual and collective tools;
- **In design customizations** integrated into the solutions under analysis. The aim is to assess the apparent and transparent value-based architectural and structural decisions that can be configured and chosen by citizens.
- **Openness** expressed as the ability to provide, extract and reuse available information from individual tools and leading to numerous questions about the quality, credibility and integrity of collected data;
- **Interoperability** for information exchange and plug-and-play interaction among various devices and systems contrasting siloed proprietary sensor data formats;

The analysis described in the present report examines case studies from emerging wearable solutions used for monitoring lifestyles in the domain of personal health and wellbeing, and their adoption in knowledge production oriented for the simultaneous benefit of individuals and communities. A wide range of low-cost sensing technologies are nowadays used to collect body and health measurements as diverse and comprehensive as motion-based activities, vital signs, and environmental quality. Data are logged in online information spaces, where citizens can also share knowledge with others and coordinate activities through social networks and community forums. Chapters 3 and 4 review in detail some specific wearable devices and platforms chosen amongst the most popular ones, with attention to provide an overview of different technologies and technological approaches. Concluding remarks and recommendations enhancing trust and trustworthiness in future personal and community health solutions are drawn in chapter 5.

2. Some ethical and legal reflections: By-Design and In-Design forms of protection in ICT

2.1. Privacy-by-Design

2.1.1. The 'information society'

The contemporary concept of privacy has changed and has expanded quite far from the original idea developed at the end of the 19th century by Warren and Brandeis [Warren and Brandeis 1890]. Indeed, it cannot be only defined as the freedom from interference in someone's personal choices plans and decision (Tavani 2010). Today, as privacy is increasingly connected with the widespread use of invasive technologies that store and share personal information, the notion of 'digital privacy' has been progressively combined with the ability to restrict the access to the digital flow of personal information.

The diffusion of new ICT (Information and Communication Technologies), namely the fact that the number of individuals around the world who have access to an ICT device and an Internet connection is constantly growing, requires an adequate regulation for this sector. Traditionally, law and government regulation have established some default rules for information policy, including constitutional norms on freedom of expression and statutory rights of ownership of information (Boyle 1996). However, in the so-called 'information society', an intervention from the legislative power does not seem to be effective anymore, and a different form of regulatory instrument is now complementing traditional normativity: technology.

Considering technology as a regulatory instrument implies that the mechanisms settled to protect privacy have to be designed and inscribed within digital architectures. According to Reidenberg, "law and government regulation are not the only source of rulemaking. Technological capabilities and system design choices impose rules on participants" (Reidenberg 1998).

With technological regulation, norms are not imposed from outside, waiting for human agency to be implemented and enforced, but they come together with technological tools: the architecture of the system itself is framed to protect rights (Reidenberg 1998).

As Reidenberg has pointed out, “The regulated-behavior approach provides an indirect but significant stimulus to Lex Informatica norm-construction. Here the government can require or prohibit particular activities […]. Behavior regulation leads to a search for the means to assure conforming practices. Technical rules can become a cornerstone of that assurance” (Reidenberg 1998, 582).

Through a technology that is already “conformed” to the principles of *Lex Informatica,* a higher degree of prevention can be reached against offences, which can be preventatively blocked at the operational level. If the constraint is embedded into, and belongs to the technological device, the perspective is completely changed: privacy is not protected through an external mechanism for protection and enforcement, but it is the tool itself that is preventing the infringement from happening: “Policy choices are available either through technology itself, through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions.' Specific information policy technologies that set information flow rules show the significance of Lex Informatica as a parallel rule system” (Reidenberg 1998, 569).

2.1.2. The concept of Privacy by Design

In 1969 Herbert A. Simon’s book *The Science of Artificial* highlighted the absence of satisfactory consideration for the "the science of design." A specific chapter on “The Science of Design: Creating the Artificial” improved the awareness about the issue, thus encouraging the inclusion of an additional chapter on design in the second edition: “Social Planning: Designing the Evolving Artifact.” In 1996, a further chapter was presented in the third edition of the book, “Alternative Views of Complexity,” investigating the implications of artificiality and hierarchical structures for complexity. Simon affirms that “in terms of the prevailing norms, academic respectability calls for subject matter that is intellectually tough, analytic, formalizable, and teachable. In the past much, if not most, of what we knew about design and about the artificial sciences was intellectually soft, intuitive, informal, and cook-booky” (Simon 1996, 112).

Code, by Lawrence Lessig, in 1999 emphasised the already essential interest on the influence of design over human behaviour: the way a digital architecture has been built has, by design, an impact on the possible utilizations of it (Lessig 2006).

The effect of design on people's lives was soon brought to the attention of the regulatory environment in the sector of data protection. Indeed, regulators saw that it is possible to take advantage of the use of design in the area of data protection and information technology: design can be presented as a defence of personal information, or privacy can be proposed within the design (Pagallo 2009). With Simon's words, "design theory is aimed at broadening the capabilities of computers to aid design, drawing upon the tools of artificial intelligence and operations research. Hence, research on many aspects of computer-aided design is being pursued with growing intensity in computer science, engineering and architecture departments, and in operations research groups in business schools. The need to make design theory explicit and precise in order to introduce computers into the process has been the key to establishing its academic acceptability its appropriateness for a university" (Simon 1996, 114).

Attention for design as a legal concept started in the 1990s and, little by little, has been gaining increasing consideration. The legal concept of design appeared for the first time in Recital 46,[1] and indirectly in Article 17,[2] of Directive 95/46/EC (CEC1995), highlighting a sort of moderate incorporation of the notion in the legislation. In order to maintain security and to prevent unauthorized processing, the Recital 46 states, it is necessary to take appropriate technical and organizational measures, both when the processing system is designed and during the processing of data itself. Several other Directive provisions call for data controllers to implement technology safeguards in the design and operation of ICT.[3] Thus, the idea of "Privacy by Design" (PbD) has been progressively developed by data protection policy makers: the first and most famous one being the Ontario Information & Privacy Commissioner Ann Cavoukian in the late 1990s.

According to Cavoukian, when considering the implications of the evolution of technology, it is not possible to simply comply with the regulatory framework requirements, but it is necessary "an organization's default mode of operation"

[1] Recital 46 requires that the "appropriate technical and organizational measures to protect personal data" of Article 17 need to be taken, both at the time of the design of the processing system and at the time of the processing itself.

[2] Article 17 lays down the data controllers' obligation to implement appropriate technical and organizational measures.

[3] Article 29 Data Protection Working Party (2009). *The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, Adopted on 01 December 2009, 02356/09/EN WP 168, p. 13.

(Cavoukian 2011). The idea is to embed privacy, and therefore privacy protection, into the design specifications of the technology developed.
The principles of PbD were formulated in order to be applicable in what has been called the "trilogy of applications:"

1. IT systems;
2. accountable business practices;
3. physical design and networked infrastructure.

In 1999 Cavoukian developed an approach based on Seven Foundational Principles. The purpose of embedding the principles of PbD into the digital architecture is to allow individuals to succeed in supervising the treatment of their personal data; every person must be able to understand the reasons why their data is collected. The development in 2009 of the Seven Foundational Principles during the "Privacy by Design: The Definitive Workshop," coordinated by the Canadian Commissioner in Madrid, represented a good starting point for the actual application of PbD. At that time, the concept of "privacy enhancing technologies" (PET), [4] despite having been proposed in the mid-1990s, was still far from been fully recognised. The idea was mostly perceived as a strategy for selling products, and there have been different attempts to take undue advantage of its reputation as well as to promote other technologies, that are not necessarily "privacy enhancing", but "privacy enforcing" or "privacy enabling" [Hustinx 2009]. The concept of PETs was at the roots of the principle of "data minimization," now widely used. PETs gradually developed into the principle of PbD, and are currently not only relevant for information technology systems, but also for organizations and methods in general, and thus also for "more effective" data protection by authorities. A good definition of PETs is a coherent system of ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system (CEC 2007).

[4] The concept of privacy enhancing technologies is very close to PbD and was developed for the first time in "Privacy-enhancing technologies: the path to anonymity," a report published in 1995 (Office of the Information & Privacy Commissioner of Ontario and Registratiekamer 1995).

In 2010, all these principles have been definitely received by the *Resolution on 'Privacy by Design'* (International Data Protection and Privacy Commissioners 2010). The principles are the following:

1. Proactive not Reactive; Preventative not Remedial: PbD is characterised by a proactive nature, in place of a reactive one. The prevention of the potentially privacy invasion event before it happens is the purpose. In short, "PbD comes before-the-fact, and not after."
2. Privacy as the Default Setting: the "default rule" aims to automatically guarantee privacy in any IT system or business practice to realise the "maximum degree of privacy."
3. Privacy Embedded into Design: PbD is directly inserted into the design and architecture of IT systems and business practices.
4. Full Functionality — Positive-Sum, not Zero-Sum: inserting privacy into the design system allows protecting both privacy and security, avoiding any compromise. Both, data protection and data security must be considered during the system design.
5. End-to-End Security — Full Lifecycle Protection: the entire lifecycle of the data is taken into consideration and not only some parts of it. The data must be safely preserved and completely deleted at the end of the practice. It is the so-called 'secure lifecycle management of information.'
6. Visibility and Transparency — Keep it Open: According to PbD principles, the design project should be let open, and mechanisms should be visible and transparent to everybody.
7. Respect for User Privacy — Keep it User-Centric: PbD "requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options."

The Seven Foundational Principles, "when applied to privacy-invasive technologies, (…) can be transformative in nature" (Cavoukian 2011), as they can protect users' safety and grant legitimate data collection. The goal is to raise consciousness amongst the citizens about the value of managing their data as required by the right to privacy as a fundamental right.

2.1.3. Practical applications of Privacy-by-Design principles

Several objections have been raised against the practical applications of PbD principles. One critique relates to the ambiguity of PbD definition: "Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality" (Cavoukian 2011).

The circularity of this formulation does not offer any concrete instruction regarding what to do in order to safeguard privacy into the design of the system as it does not make clear what needs to be done (Gürses, Troncoso and Diaz 2011). The idea is to build up systems capable of self-defence and to implement the State structural responsibility for technological development. As Pocs has argued, "(t)he approach of legal technology design offers several

advantages. It helps the state to bear its "structural responsibility" (…) and gives individuals technological aids for "self-protection" (…). It helps legislators to fulfil their duty to observe technological development and to prepare the political process by showing equally effective but less intrusive alternatives" (Pocs 2012, 642). The link between legal instruments and technological tools is deemed to get closer and closer: lawyers and engineers will soon be obliged to collaborate. According to Nigel Gilbert, on these terms not only do technologies need new regulation, but new technologies should be developed in order to minimize the impact on privacy (Gilbert 2007).

PbD can be summarised as a new approach to the management of personal information embedding privacy principles into every part of every system in every organisation. The consensus of all the operators is a mandatory precondition: all the participants should take care of the effectiveness of the system. Not only a part of the system has to be taken in to account, but the full lifecycle of any system or process, from the earliest stages of the system business case, through requirements gathering and design, to delivery, testing, operations, and out to the final decommissioning of the system (United Kingdom Information Commissioner's Office 2008).

The application of the 'lifetime approach' will ensure better effectiveness of controls as well as easier and less expensive implementation. It will be harder to elude an architecture initially designed to implement privacy-friendly measures: the process is created to reach privacy goals from the conception of a new IT system up to its realization. Software development will be more affordable if the protection of privacy is considered at the start of the project and the costs get higher if the same tool is applied only during actual implementation.

2.1.4. Strategies for the implementation of Privacy-by-Design

Some strategies can be settled down in order to implement the legal principles of PbD. The first step is to identify, at the most general level, two different approaches:

a. The privacy-by-architecture approach
b. The privacy-by-policy approach.

These strategies can be considered as mutually exclusive: "if companies do not opt for a privacy-by-architecture approach, then a privacy-by-policy approach must be taken where notice and choice will be essential mechanisms for ensuring adequate privacy protection" (Spiekermann and Cranor 2009, 77).

Different strategies can be considered, but a definition of 'design strategies' must be assumed as "a fundamental approach to achieve a certain design goal. It has certain properties that allow it to be distinguished from other (fundamental) approaches that achieve the same goal" (Hoepman 2012, 3). Assuming this design strategy, as defined, aims to achieve some levels of protection.

The division between the privacy-by-architecture and the privacy-by-policy approach can be seen also as a separation between a "data-oriented" and a "process-oriented" strategy (Spiekermann and Cranor 2009).

In 2014, an article by Hoepman (Hoepman 2014) analysed and classified the major existing strategies for implementing PbD.

These can be here summarised as follows.

1. Data oriented strategies

   - Minimise: *The amount of personal data that is processed should be restricted to the minimal amount possible.*

- Hide: *Any personal data, and their interrelationships, should be hidden from plain view.*
- Separate: *Personal data should be processed in a distributed fashion, in separate compartments whenever possible.*
- Aggregate: *Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.*

2. Process oriented strategies
   - Inform: *Data subjects should be adequately informed whenever personal data is processed.*
   - Control: *Data subjects should be provided agency over the processing of their personal data.*
   - Enforce: *A privacy policy compatible with legal requirements should be in place and should be enforced.*
   - Demonstrate: *Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.*

The following table, reproduced from Hoepman's research (Hoepman 2012, 11) shows how the legal principles that are part of the European legal framework can (or cannot) be covered by the different design strategies summarised above.

	Purpose limitation	Data minimisation	Data quality	Transparency	Data subject rights	The right to be forgotten	Adequate protection	Data portability	Data breach notification	(Provable) Compliance
MINIMISE	o	+								
HIDE		+					o			
SEPARATE	o						o			
AGGREGATE	o	+								
INFORM				+	+				+	
CONTROL			o		+			+		
ENFORCE	+		+			+	+			o
DEMONSTRATE										+

Legend: +: covers principle to a large extent. o: covers principle to some extent.

Table 1. Mapping of strategies onto legal principles.

Table reproduced from Hoepman 2012, 11.

According to Hoepman, there is no strategy autonomously covering all the principles, and not all legal data protection principles can be adequately covered through a PbD strategy, simply because the design of the system has no impact on that principle (Hoepman 2014).

2.2. Rights-in-Design: citizen rights in digital architectures

2.2.1. A matter of architecture: the normativity of digital artifacts

In 2011, while listing the essentials for an "Internet compact," Commissioner Kroes recalled that "architecture matters," referring to how the Internet structures do not only have ethical and policy impacts, but are based on certain values and choices. Therefore, she added, in discussing the "future Internet" there is the need "to have a broad,

structured and coherent debate, with the Internet policy and research communities, on the impact of architectural change" (Kroes 2011).

Architectures, however, matter in all ICT devices. As seen in the previous section of this report, a variety of technological measures have been proposed and/or already implemented to automatically protect individual rights and security, with the aim of doing so more effectively. These measures broadly consist of mechanisms "embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal" (EDPS 2010).

The European Data Protection Supervisor (EDPS) has analysed and strongly supported the by-design approach mostly in relation to privacy protection, referring to Privacy-by-Design (PbD) in technical as well as normative terms. Indeed, PbD has been defined as a "general, binding principle" that has to be included into the data protection legal framework; and also as a technical architecture and design incorporated in particular ICT areas. As stated by EDPS, in order to compel compliance with this principle, the need exists "to provide for the principle of "privacy by design" into the data protection legal framework in at least two different ways. First, by incorporating it as a general, binding principle and, second, by incorporating it in particular ICT areas, presenting specific data protection/privacy risks which may be mitigated through adequate technical architecture and design" (EDPS 2010, 2).

Therefore, the "by-design" approach can be understood not just as a set of technical solutions, but as a specific normative orientation and regulatory principle: namely, the principle of providing default protection to ICT users/citizens by embedding these measures directly in digital architectures. Moreover, though primarily looking at surveillance technologies, the Article 29 Working Party asked for Privacy by Design to be made compulsory, "where public authorities are the main actors and where measures increasing surveillance directly impact on the fundamental rights to privacy and data protection" (Art.29 WP 2009).

Although technical normativity has accompanied the history of the law and the philosophical reflection about the law, still the tendency exists to think of ethical and legal norms as intentional and free decisions about how to act. ICT have massively increased this kind of ruling as they embody rules and decisions in their own designs and structures. Such "by-design" measures of legal protection represent forms of what

can be called “factual normativity,” as technical, engineered artifacts are factually altering and influencing human behavior by shaping and/or limiting human agency.

Some legal scholars have described by-design normativity as the “end of the law” conceived as a principle or a rule that should be implemented through a human agent (or a process guided by a human agent) (Hildebrandt 2008; Hildebrandt and Rouvroy 2011).

The widespread modern “prejudice” about the separation between facts and values has been, amongst other things, a major intellectual obstacle to timely recognition and intervention on the values embedded in ICT. In philosophy of technology the idea that machines and programs can embody values is not new. Already in 1980, in “Do Artifacts have Politics?” Langdon Winner noticed that all machines, structures and technical systems should not only be analyzed from the perspective of their efficiency and productivity, but also “for the ways in which they can embody specific forms of power and authority” (Winner 1980, 121).

These early observations (that have led to a number of developments in ICT, e.g. to make them more “human-centered”), have raised awareness about the choices implicitly embedded, packed, and black-boxed in programs and devices. As Winner has pointed out, “By far the greatest latitude of choice exists the very first time a particular instrument, system, or technique is introduced. Because choices tend to become strongly fixed in material equipment...the same careful attention one would give to the rules, roles, and relationships of politics must also be given to such things…” (Winner 1980, 127-128).

Now, these normative decisions should be made explicit, transparent, discussed, and controllable, from designers and engineers, to institutions, and citizens. Increased knowledge and attention should be paid to how technology and normativity co-generate each other, and to how technical-normative black boxes should be opened up for transparent analysis and deliberation. If normative decisions are pervading the design of all ICT, open and thorough discussion becomes a matter of democratic legitimacy and citizens’ rights.

2.2.2. Towards individual legal entitlements in the design

Rights "in-design" need to be distinguished from "by-design" protection of rights, even though they can be seen, and they should be proposed as complementary (Pereira and Tallacchini 2014). Indeed, the concept of rights-in-design effectively allows extending, deepening, and strengthening the by-design paradigm; however, it also changes the perspective from a passive to an active role for the citizen/user, and frames the legal environment in terms of directly exercising rights rather than receiving a predefined protection.

The "by-design" approach aims to create built-in algorithms for law enforcement and rights protection without involving the rights holders, the "in-design" approach aims to raise awareness about the processes through which values and norms become embedded in technological architectures by opening up and making available those choices to individuals as a matter of legal entitlement.

If in the "by-design" protection of rights, privacy and data protection are delivered to the user as all-encompassing trusted products (i.e. the process of embedding privacy does not need to be disentangled from the product in order to become accessible); in the "in-design" approach digital architectures and their design are seen as the place where citizens/users can properly exert their rights and make their own choices.

These choices may certainly concern privacy and data. The European Group for Ethics in Science and New Technologies (EGE) to the European Commission has used the concept of "rights-in-design" from this perspective, by defining Privacy in Design (as distinct from Privacy by Design) as the process of "raising awareness about the processes through which values and norms become embedded in technological architecture. Privacy in design looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens" (EGE 2014, 32).

This approach also implies a deeper understanding of privacy as a "right" rather than a value covered by legal protection; and highlights that an active role should be recognized to the right-holder, who has to be seen as the real subject of his/her right rather than the merely passive recipient of protective tools designed and controlled elsewhere by other subjects.

However, rights-in-design may extend to domains and choices other than privacy. These rights may concern, for instance, attributing or limiting third parties' powers of access to some ICT functionality or to sharing information (Pereira and Tallacchini 2014; Kounelis et al 2014). Moreover, they may refer to rights of access to specific sets of data, such as raw data—that, according to some scholarly analysis, should be already considered as an individual moral right (Lunshof et al. 2014). Rights-in-design can be relevant in several areas, especially when institutions
and citizens interact, from how institutional information is delivered to how laws are implemented.

This situation calls for a variety of normative and educational measures to be adopted. Engineers and information systems engineers should work together with ethicists and lawyers in order to build collective transdisciplinary knowledge of the relationships between technology and normativity. Normativity that is consciously and unconsciously inscribed in, and embodied by, artefacts should be made as explicit and transparent as possible before and during the design phase, a crucial stage in development when normative decisions are taken and transformed into programs and functions. Moreover, these normative decisions should reflect and be consistent with the same fundamental values and rights informing legal systems.

2.2.3. Rights-in-design as enhanced agency in ICT

While privacy has been, and still is, a longstanding ethical and legal concern raised by ICT, recent developments in ICT such as the Internet of Things (IoT) are increasingly pointing at several different issues. Indeed, a major topic in IoT, due to the pervasive and sometime undetectable connections amongst networked objects and subjects—concerns agency, namely the individual capability to freely act and to adopt free decisions.
Agency represents a broader concept than autonomy, encompassing not only the specific cognitive and free will attitudes of an autonomous self, but the wider range of acts and activities connected to human life (Arendt 1958).

The preservation of the human capability to freely act and make choices has been shown as a major factual and normative concern amongst the different requirements for a sustainable governance of IoT. Indeed, a normative framework for a viable vision of IoT requires a renewed proactive attention—and moral commitment—towards human agency, namely towards a full concept of humanness and towards preserving the features of human action.

The preservation and cultivation of human agency complex interconnected ICT can impair the human ability to control the system while being a part of it. This implies that an integration of technical and human dimensions in ICT-mediated relations is provided.

While humans have been traditionally characterized as agents, namely non-deterministic, creative, and self-reflexive subjects, now the tendency is towards a transformation of both objects and subjects into actants, namely deterministic mechanisms.

In the IoT, for instance, this is the difference between a completely automated process using a pre-defined set of technical policies and a process guided and customized by human choice considering a set of policies for each particular use case (Kounelis et al.2014). If delegation of powers can remain an act of choice, the outcome is a continuous process where the interactions between agents and devices can be constantly redefined, renegotiated, renovated, and quantified when appropriate.

The concept of rights-in-design may help in this process can lead to more robustly trusted and effective digital relationships — together with new learning experiences and skills as well as the development of skills to live in the physical-digital world .

As Kounelis et al. have pointed out, "(s)imply described, the development of software encompasses necessarily a front end, commonly described as a user interface and the (often black) "box" that it accesses. Opening up of those "black-boxes" is a long-standing argument; even Open Source code does not translate to understanding of what the box actually does, unless examined by a software developer. (…) Black-boxing needs to be opened up through structural spaces to allow individual personal decisions to be taken" (Kounelis et al. 2014, 75).

Here the strong connection between "by-design" and "in-design" emerges and can be clarified. Human agents are enabled and empowered "by-design" to make their own choices and changes "in-design," namely to decide and modify — even case-by-case —

the conditions for providing/not providing access to third parties, for sharing/not sharing powers and controls, for authorizing or not authorizing certain actions, and to specify the obligations that should be fulfilled by the parties after access to their data is granted.

Also, through the concept on rights-in-design the user is increasingly seen as a citizen. While, from a market perspective, products enhancing and supporting citizens' rights to their free choices can attract an increasing number of consumers—as already happened in the field of ethically-oriented consumption—, the desire for more agency shows a specific human and civic dimension, as through and with ICT citizens live increasing portions of their private and public lives.

As technologies are increasingly in charge of normative functions, the creation, within digital architectures, of spaces for expressing human agency, freedom of choice, for conferring of removing powers, and for performing controls becomes the new natural place for exerting rights.

It is interesting to observe how the idea of rights-in-design is converging and merging with the general inspiration and the values of the Do-It-Yourself (DIY) movement, as they both tend to highlight individual entitlements—factual and normative—towards technological devices.

As it has been pointed out, "(c)itizen empowerment through DIY and making also relates to concrete and practical possibilities to embed values, norms and expectations in artifacts themselves, and thus more integrated in particular realities and contexts. Access to technical and communication means to design, modify and create an artifact (object, system, application, etc.) allows for a greater variety of options and choices to be made regarding the purposes, impacts and uses of the artifacts in question, regarding for instance personal health issues, pollution in your neighborhood, or information about local political decisions" (Tallacchini, Boucher, Nascimento 2014, 15).

Currently, while the value of users/citizens' empowerment through "by design" approaches has been widely recognized also as a "normative principle", "in-design" approaches protecting and promoting the active use of individual rights—definitely to privacy, but also to other rights of control on potential options within the architecture of the systems—still require reflection for potential implementations.

3. Emerging wearable sensors for health activities

Although still in their infancy, wearable sensors are announced as the next most promising market for personal consumer devices, after mobile smartphones (Forlani 2014). By empowering people to easily measure, report and compare their own personal environment, such tools transform everyday citizens into reporting agents who uncover and visualize unseen elements in their own everyday experiences and co-produce knowledge in an effort to improve both their individual lives and the ones of their communities (Tallacchini, Boucher Tallacchini, Figuereido Do Nascimento 2014). During the last months many new products have drawn attention from the public: Google's medical treatment device embedded in contact lenses (Scott 2014); arm, wrist and ring gadgets designed to measure and monitor lifestyle quality, such as activity and burnt calories rates; smart fabrics tracking our athletic performance; Nest's remote and smart thermostat sensor to monitor temperature, humidity and air quality (Finley 2014). Due to the their small size, low energy requirements, powerful data processing capabilities and low cost, sensors open up new possibilities to achieve a range of health outcomes. In order to give a general overview on the domain, typical categories of wearable sensing technology will be introduced in the next sections.

3.1. Definition(s) and classification(s) of wearable sensors

As technology matures and sensors are further miniaturized, novel applications, capabilities and form factors for lifestyle and health monitoring are being developed. The integration of wearable sensors into consumer electronics enables personal health data gathering, as well as support of preventive health measures and more specific developments for medical remote care programs. Most of present-day applications of health related wearable sensors can be classified into the following five categories:

- Health & Wellness Monitoring. Sensors can monitor environmental and physiological measurements of individual health outcomes, especially the ones with chronic conditions to report exposure, to identify risk factors and to facilitate prevention through alternative strategies. Some consumer health and

fitness sensors are widely used by individuals to gather quantified data about their health.

- Early Detection of Disorders. By combining physiological sensors with activity monitors and consumer electronics devices, some disease symptoms and adverse changes in an individual's health status can be the focus of early detection thus facilitating timely intervention.
- Safety Monitoring. Many wearable sensors were developed to detect falls, epileptic seizures and heart attacks in older people and susceptible individuals, and then send alarm signals to caregivers or emergency response teams.
- Treatment Efficacy Assessment. Using wearable sensors, efficacy of treatment and clinical trials can be better assessed. They help to track physiological changes in chronic conditions and lengthy treatments on a continuous basis. Sensors are also used to monitor, assess and improve adverse reactions.
- Home Rehabilitation. Sensing technology, sometimes in combination with interactive gaming, Virtual Reality environments and augmented feedback systems, is being employed to facilitate home-based rehabilitation interventions for physiotherapy, patients and ageing individuals.

Wearable sensing systems (e.g. apps) are built with various smart capabilities to capture and combine information on aspects of the environment in which they operate and can also be categorized according to the degree of smartness they provide.

- Complex accessories are the first generation of sensing devices born as artifacts with embedded processing such as fitness tracking with limited storage and feedback to the end-user. They can operate partially independently of any other device and in need of being paired to mobile and web services for more comprehensive output and logging.
- Smart accessories are more recent designs evolved for improved viewability and extended processing capabilities with embedded apps, such as the Apple watch. These products are identified by their ability to run third-party applications, though they still rely on connection to smart devices for accessing Internet.

- Smart wearables are fully autonomous sensing devices that connect directly to the Internet, such as Google's Glass headset with full input and output functionalities.

Sensing devices also come in a variety of forms. Clips, wristbands, armbands and smart watches are wearable form factors ideally unobtrusive to users. Wrist-worn wearable devices are popular fitness trackers accounting for the biggest share of the market. Current leaders in this segment are commercial products with limited functionalities, such as FitBit, Nike Fuelband, Jawbone and BodyMedia (Fitbit 2014, Nike 2014, Jawbone 2014, Bodymedia 2014). Some products are being developed for very specific uses: Sproutling wearable anklet is being proposed for monitoring babies aged six months and up (Rhodes 2014). Recent armband developments explore how to extend the form factor design and sensing functionalities in multiple directions. The most relevant examples include gesture input and control functionalities to replace computer mouse with Myo biometric authentication by Thalamic labs (Thalmiclabs 2014), Nymi authentication with heartbeat (Nymi 2014), a research headband to control devices with EEG based brain computing interfaces (Nuviun 2014, August 7), open health communication protocols and sensor data stream (Angelsensor 2014, Kellion 2014, Tate 2014, Google Developers 2014), Beddit bed worn bands to track quality of sleep (Beddit 2014) and non invasive measurement of glucose through biometric sensing (Meyer 2014). Vitaljacket smart t-shirts can embed removable sensors and microsensors woven into the textile to monitor breathing and heart-rate (VitalJacket 2014). Zephyr removable sensors from chestband can also be packaged into patches to monitor specific body areas (Zephyr 2014).

Other form factors are being augmented with wearable sensors. Already around for quite some time now, headsets are recently being extended with fitness sensing capabilities. The most prominent example is "The Dash" wireless in-ear headphones that also offer health performance tracking via in-built body sensors (Bragi 2014). Novel researches at Cornell University are experimenting with techniques to capture sound waves transmitted through the skull to detect subtle activity clues, such as food consumption, coughing and respiratory problems, or emotional states of the person wearing it (Nuviun 2014, June 26). Closely related to biosensors are health sensing devices for indoor and outdoor monitoring of temperature, humidity, pollution and air

quality packaged in Air Eggs and portable Smart Citizen kits (AirQualityEgg 2014, SmartCitizen 2014). Multiple biosensing and monitoring techniques can also be integrated together into the Withings smart scale that combines air quality and weight monitoring (Withings 2014) and in Samsung Simband innovative armband tracking vital parameters and pollution (Samsung 2014). In addition to commercial products, open source and do-it-yourself (DIY) low cost toolkits are becoming available as alternative and flexible solutions for fast prototyping and learning. BITalino DIY kit for body signals is an illustrative example (Bitalino 2014).

The brief overview on the trends and developments in wearable sensors shows that the domain is rapidly evolving and presents a multiplicity of features and characteristics that will need to be taken into account during the analysis.

3.2. Scope of the analysis for health activities

The increasing availability of wearable sensing systems carried around by millions of people has opened up diverse possibilities for information gathering by people themselves. For the purpose of the present analysis we will focus our attention on the lower end of consumer products (i.e. low-cost devices and DIY kits). The analysis will consider a range of products relevant for the promotion of health and wellbeing targeting leading risk factors for chronic degenerative diseases that may be controlled through primary prevention of lifestyles (diet factors, physical inactivity, air pollution, obesity, high blood pressure, etc.). However, it will restrict to self-tracking activities and checking of health sources of information (e.g. exposure to air pollution), addressing the application domain of health and wellness monitoring and early detection of disorders discussed in the previous section.

To keep the analysis within feasible limits, the focus will be on non / minimally invasive body worn and health sensors, whereas implantable or ingestible sensors will not be dealt with. For the same reason, medical devices for the monitoring and treatment of patient illnesses in clinical applications will also not be addressed. Similarly, individual self-assessed sources (e.g. questionnaires on lifestyle or diaries) purposively and intentionally collected by end-users are beyond the scope of interest as their mediation interactions present fewer ethical risks for the end-users with respect to automatic and automated processing. A sample of the most representative devices was selected to

comprehensively address features, form factors and set-ups from commercial products, open solutions, DIY kits and wearable devices.

The list of devices is illustrated in Table 2 and covers the extent and characteristics of consumer products and research approaches available to everyday users.

Sensor	Form factor	Product category	Sensor type	Stimulus	Use in participatory health
Beddit sleep manager	bed device	complex accessory	biomechanical (BCG)	sleep	quality of sleep monitoring
Jawbone UP activity monitor	wristband	complex accessory	biomechanical (accelerometer)	activity, sleep, calories burnt	detecting people's exercise, sleep and calory consumption patterns
BodyMedia link armband activity monitor	armband	complex accessory	bioeletrical and biomechanical (EDA, accelerometer, temperature, heat flux)	activity, sleep, calories burnt	detecting people's exercise, sleep and calory consumpation patterns
Withings blood pressure monitor	armband	complex accessory	biomechanical	blood pressure	blood pressure monitor
Withings smart scale	home device	complex accessory	bioelettrical and environmental	weight, fat mass, heart rate, air quality	indoor monitoring and weight management
Withings aura active sleep manager	bed device	complex accessory	biomechanical	body movements, sleep	quality of sleep monitoring, smart waking up
VitalJacket shirt ECG monitor	smart shirt	complex accessory	bioelectrical (ECG)	Electrical activity of the heart (ECG), movement	specific monitoring (e.g. sport training monitoring)
Zephyr bioharness	smart patch	complex accessory	bioelectrical and biomechanical (ECG and accelerometer)	breathing rate, heart rate	specific monitoring (e.g. sport training monitoring)
Smart Citizen environmental health monitor	ambient sensing kit	complex accessory	environmental and electrical	temperature, humidity, ambient light, noise, CO, NO2	indoor / outdoor air quality monitoring

Table 2. Health and lifestyle wearable sensing devices under review.

Using empirical data gathered from software testing, wearable technology will be reviewed qualifying key features and best practices to respond to trustworthy self-documentation in digital health platforms. The review will cover core functional and ethical dimensions of wearable sensing devices.

Having defined the scope of the analysis with respect to the applications and devices under analysis, as well as the elements to value, the next section will summarize the core technical aspects of sensing components embedded in wearable solutions.

3.3. Sensing Technology of Interest

Wearable technologies incorporate computationally powerful, low-cost, tiny sensors that respond to a physical input of interest with a recordable, functionally related output (Kyriacou 2010). These sensors take an analog property from the environment or body and convert it into electrical signals that can be interpreted by a digital device with a microprocessor. For any given property, there is usually more than one sensing technique that can be used to take measurement. Important properties for sensors are as follows:

- accuracy of measurements performed by certain group of end-users under certain conditions (the measurement technique provides consistent results upon repeated application)
- safety of the sensing technique that must be proven not to be harmful when the device is worn all day long
- sensitivity of input changes, which reflect into changes of the same magnitude in output specificity defined as selectivity to the input of interest and ability to operate in different conditions.

The physical input can be measured through various techniques and approaches, namely applying environmental, mechanical, electrical and optical and acoustical principles. Environmental, mechanical and electrical approaches mostly require contact with the quantity of interest and their deployment on the human body must consider aspects of comfort and biocompatility. Physical contact sensing may show very fast or slow response time (speed of the process to obtain the output result), whereas non contact sensing generally responds promptly. Each type of low cost sensor has specific characteristics and limitations, that will be briefly presented.

3.3.1. Environmental gas sensors

In environmental monitoring, low-cost gas sensors are enabling a new wave of portable air quality monitoring tools (Peters 2013). A typical gas sensor has a porous semiconductor sensing layer and a sensor base. In the presence of reducing gases, such as carbon oxide (CO) or hydrogen (H2), the resistance of the sensor decreases. Oxidizing gases such as nitrogen oxides (NOX) and ozone (O3) have opposite effects and the resistance of the sensor increases. Quantification functions need also to be applied to convert the sensor signals into concentrations. Commercially available semiconductor gas sensors can provide measurements of CO, CO2, O3, NO2, and total volatile other compounds (VOCs) (cfr. Figure 1).

Quantitative measurements of pollutant concentrations generally require techniques to be sensitive at ambient concentrations and unique to that particular compound (i.e. free from interference from other pollutants). However, gas sensors are still affected by important quality issues, such as sensitivity, cross-interference, sensor drift, and

susceptibility to temperature or humidity and only qualitative concentrations can be provided.

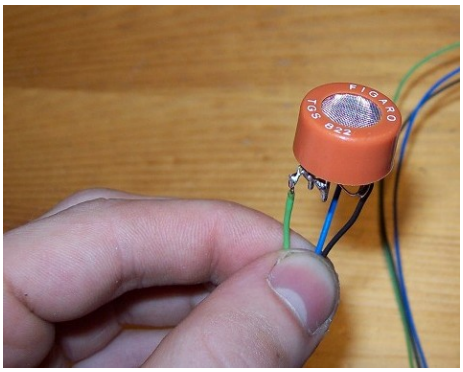

Figure 1. Figaro gas sensor detecting VOCs[5]

Their sensitivity, selectivity and stability are highly influenced by environmental conditions, particularly temperature. Environmental conditions also have a strong influence on operational lifespan, with reduced sensor's lifetime in hot and dry environments and oversaturation to the species of interest (Spinelle, Gerboles, Aleixandre 2014). To improve accuracy, new calibration models need to be developed for inter-device variance in urban large scale use. Similarly to gas sensors, semiconductor sensors can be used to measure temperature in health applications, as they exhibit strong thermal dependence. However they also suffer from limitations in accuracy and stability and slow response time.

3.3.2. Electromechanical sensors

In mechanical sensing, accelerometers are the sensor most commonly employed in a range of applications. Accelerometers can detect signals in 2 or 3 directions and consists of a micro-electro-mechanical device that measures motion. There are five modes of motion sensing: acceleration, vibration (periodic acceleration), shock (instantaneous acceleration), tilt (static acceleration) and rotation. Micro electro-mechanical accelerometers are typically piezoresistive, embedding resistive material that change its resistance according to the acceleration applied and achieving high amplitude and high

[5] The image is reproduced from Wikipedia

frequency response, but qualitative accuracy of measurements. The accelerometer includes a small mass that moves when subject to acceleration from activity, gravity and other external forces (cfr. Figure 2). When body worn, measured accelerations can be mapped to forces exerted on the body, which can in turn be mapped to energy used by the muscles of the body to generate these forces.

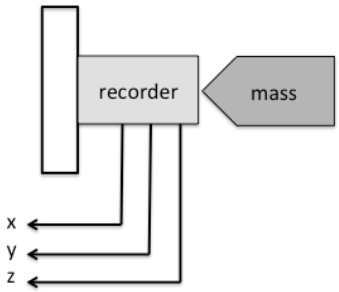

Figure 2. Accelerometer sensor

Another non invasive mechanical technique is ballistocardiography (BCG) that measures the body's reaction to the blood ejected by the heart during the cardiac cycle (Eblen-Zajjur 2003). The measurement is mostly performed in stationary setting from electromechanical film sensors or pressure sensors for non-ambulatory situations, including beds with load cells, strain gauges, and air mattress pressure sensors used to sense the BCG subjects during sleep (Beddit 2014).

3.3.3. Electrical sensors

Measurement of cardiac parameters is more precise with electrical techniques. Electrocardiography (ECG / EKG) measures electrical activity of the heart over a period of time and across a chest area during the heart contraction and relaxation process. The measurement is performed using some forms of electrodes in contact with the subject skin. Design of electrodes is also an important factor in continuous monitoring, as these electrodes should not damage the skin. During motion the electrodes could become loose, breaking the electrical contact and causing high noise spikes in the data. Wearable electromyography (EMG) measures electrical activities of a particular muscle noninvasively during muscle contraction.

During contraction microvolt level electrical signals are produced, that can be measured from skin surface (cfr. Figure 3). Some recent developments can support general placement of the sensor on the user's body, as the location of the active body area with muscle activity is automatically detected (Thalmiclabs 2014).

Electroencephalography (EEG) is another electrical process to measure brain waves of a person with electrodes or a headband placed on scalp detecting current flows through scalp tissue. EEG signal is measured between two electrodes, the position of which determines the recorded brain area.

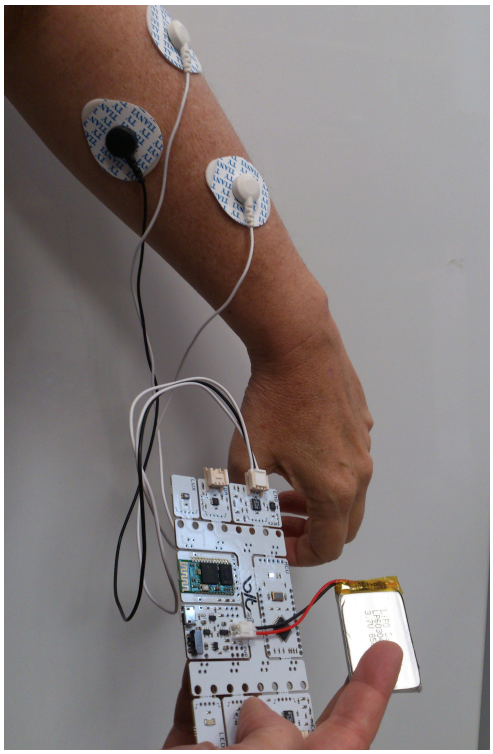

Figure 3. Bitalino EMG sensor

The electrodes detect microvolt level signals coming from brain that reflect the intensity and position of activity in the underlying neural tissue. Wearable EEG relies on wireless communication to get rid of electrode wires.

3.3.4. Optical sensors

Optical sensors apply principles for detecting waves or photons of light across the whole spectral range (i.e. visible, infrared and ultraviolet regions). Electrodermal

activity (EDA), also known as galvanic skin response (GSR) is a measurement of electrical conductance of the skin, which varies depending on the activity of the sweat gland and the skin's pore size. Skin conductivity varies with sweat from physical activity and by emotional stimuli such as pain, anger and surprise. Heat and temperature can also be measured electrically by thermistors, i.e. resistors that change their value according to temperature or very low thermally resistive materials connected to sensitive thermocouples.

Among optical techniques, recent photodetectors are replacing chest straps for heart rate monitoring and are less invasive than ECG. The measurement is a simple, reliable, low-cost process based on skin photoconductivity. The technique is based on the principles of optical detection of blood volume changes in the microvascular layers of the tissue, in the presence or absence of light. The sensor system consists of a light source and a detector, with red and infrared (IR) light-emitting diodes (LEDs) commonly used as the light source. The sensor monitors changes in the light intensity via reflection from or transmission through the tissue. The changes in light intensity are associated with small variations in blood flow within the tissue and provide information on the cardiovascular system, in particular, the pulse rate. Although the optical technique is being commercialized by several companies (e.g. Angel sensor coupled acoustical modalities measuring pulse and blood flow sounds to improve optical readings[6]), optical sensor accuracy is still affected by random noise and motion artifacts (Profis 2014).

The overview on wearable sensing technology illustrated existing limitations in the measurement process. Summarizing the previous discussion, sensor characterisation should provide information on

- calibration of offset reference values and/or models of behavior;
- range of measurable output signal including conditions of applicability;
- resolution to the smallest change it can detect in the quantity being measured;
- characterization of systematic and random errors causing deviations from ideal measurement, such as non linear sensitivity ratio between output signal and

[6]Further details on Angel sensor capabilities are illustrated in (Angelsensor 2014).

input property, hysteresis offsets, digitization error caused by approximated measurement, dynamic error caused by a rapid change of the measured property over time, noise errors showing random deviation of the signal that varies in time, drift showing slow degradation of sensor properties along time), etc.

Calibration to compensate systematic errors and adaptation to reference values, conditions and models of behaviours need to be carefully considered in specific contexts of use and applications. For this reason, it is preferable to orient towards open source solutions that can be more easily customized to changing requirements, as they promote universal access and universal redistribution of the software code, including subsequent improvements to it by anyone.

Following an overview of hardware and low level sensing characteristics, the next section will outline software facilities for collection, communication and data analysis services offered by wearable devices.

3.4. Capabilities of wearable sensors

Wearable sensors are physical objects with digital sensing, processing, and communication capabilities. They can be more or less complex depending on the range of functionalities. For example, sensing systems can detect behaviours by discriminating if the shape of the signals matches the patterns of typical conditions and activities of daily life (e.g. standing, sitting, walking, running and biking). However, functionalities do not suffice to have compelling products. Citizens also value other non-functional features, such as safety, security, privacy and usability. For this purpose, the present section will illustrate the main software capabilities and attributes of wearable sensing systems.

3.4.1. Functionalities

Wearable sensors essential functionalities consist of closely monitoring changes in end-user personal environment and providing real-time feedback to help maintain an optimal status. To accomplish these operations, wearable sensors include a core sensing architecture composed of a sensing chip to measure physical data, a microcontroller to perform local data processing such as data compression, local temporary memory,

communication facilities to optionally send the data wirelessly and the battery to provide power supply to the device. Through the optional wireless interconnection, the sensor can authenticate and interface with a private virtual space on a web platform hosting more powerful processing capabilities (e.g. to deal with more critical situations) or other wearable devices in proximity. Current development trends in wearable sensing systems evolve towards more and more complex and interconnected processing capabilities enabling collection, integration and interpretation of data.
The present analysis examines key device functionalities and limited connections with other networked sensors and online virtual spaces. Next sections will describe sensing functionalities related to the processing life cycle of acquired information.

3.4.1.1. Authentication

When interacting with wearable devices, authentication is the task for verifying the end-user identity as well as capabilities processing rights he/she is entitled to execute. To overcome challenges related to password based implementation (e.g. memorability of pin-based passwords and lack of keyboards in wearable devices), biometric processing of physiological signals is often applied for authentication purposes (Nymi 2014). However, anticipated major concerns from soft biometric based authentication are risks of disclosure of biometric health information and ethical risks related to continuous biometric information sharing and authentication, as well as loss of ownership and control on the reuse of citizen personal data (Ioannidis et al. 2012).

3.4.1.2. Data collection

Data collection from wearable sensors may involve various types of data, such as input property measurements, localisation and timestamping attributes. Data collection also encompasses various steps, namely the actual collection from sensors, data processing for further consolidation and elaboration, archival in storage and access for subsequent retrieval (e.g. by third-party).

Collection from sensors can be performed following two models. The first is manual data collection, where the end-user is conscious and actively involved in its execution (e.g. he may decide to initiate and stop the task). Conversely in opportunistic data collection, the task is programmed to execute automatically whenever specified conditions or behaviours are met (e.g. whenever the device is in a certain area). Conditions for automatic collection can be defined under the supervision of the end-

user having limited knowledge about the type of data being collected. Automatic collection is usually preferred as it is seamless and more comfortable for the end-user.

Once data are collected, data processing can be applied for further elaboration. The algorithms and the data involved (e.g. sensor measurements eventually combined with external data) depend on the application. Processing algorithms can be distinguished into recoding transformations not altering the quantity of information associated to the data themselves (e.g. non destructive compression) and interpretations that produce new findings from the data (e.g. averaging) or refined versions of the data with reduced quantity of information and potential knowledge gain (e.g. processing data with privacy preserving techniques that may protect sensitive personal information or avoiding/eliminating disturbing data points that may yield unsolicited on incidental findings) (Lunshof, Church, and Prainsack2014).

After data processing, data can be archived either locally or remotely in a private virtual space on a web platform. Local archiving ensures ownership of the data, however the amount of storage is limited. Remote archiving can be performed in a third-party virtual space on a web platform, where end users lose any track of their data, as they cannot pose restrictions on their remote collection and processing. To partially mitigate third party disclosure, user centric archives have developed trusted personal virtual spaces where end users can define personal privacy policies granting control and apply privacy enhancing techniques on the stored and owned data (Mun et al. 2014). However, these require end user engagement for extensive configuration / maintenance of the appropriate domain specific identity management, descriptors and sharing policies with multiple parties (Pearson and Mont 2011).

3.4.1.3. Individual Feedback on findings and tracking

Available collected data could be used to provide another important functionality, which is the real-time delivery of individual feedback. This can range from simple notification of measurement values with respect to reference threshold up to complex automated decision evaluating findings that could divide people in categories on the basis of people behavior. Complex feedback schemes could raise risks of people sorting and automated feedback replacing human counseling. With 24/7 monitoring, feedback and persuasive nudging by an authority that is external to the self, yet seamlessly

integrated into the environment and one's daily routines, it may become difficult to distinguish between 'true authentic actions' and steered behavior.
Following the illustration of the functional characterization of wearable sensors, additional values important to citizens can be defined in the following sections.

3.4.2. Usability criteria

Aspects relevant to usability evaluation will be considered to assess ease of use and usefulness in interactions with the wearable sensing systems. The analysis will be performed by inspection and will examine the extent to which functionality is compatible with user expectations, ease in accomplishment of desired functions. The analysis will focus on configuration set-up and recognition of tracking conditions and daily activities. Daily activities can be characterized by the way the human body is being sensed in poses and movements such as sitting, standing, walking, etc. There is clearly a tradeoff between informative and unobtrusive sensing. Additional features relevant for user acceptance are battery life, dimensions, costs and appealing of the systems.

3.4.3. By design normativity

By design normativity consists of protective measures relating to safety, privacy and security features pre-embedded in individual wearable sensors.
Concerning safety, wearable sensors should be compliant to the European and international relevant requirements. Devices for medical use should be compliant to the European Directive 93/42/EEC on medical devices. Safety regulations identify requirements for use in electromagnetic environments. Although emerging designs integrate a pack of sensors into a single device, interference effects have not been reported. A number of user recommendations warn against long-term health impacts from exposure to electromagnetic radiation, radio frequency/microwave from wireless technology and recommend safer wired Internet connection. In particular, young children (from birth to 12) exposed to electromagnetic radiation may face risks relating to changes in cell formation, genetic changes, and potential cancers (Safeinschool 2013).

Current wearable sensing systems may also pose significant risks concerning privacy and data protection due to the lack of transparency and awareness on personal data

processing by third parties (e.g. unwanted use and sharing of citizens' health data). Legal guidance by Article 29 Working Party recommends the application of data protection principles (purpose limitation, data minimization, obligation to correctly inform citizens of their rights and appropriate security measures such as data encryption and authentication mechanisms) (Article 29 Working Party 2013). The analysis will review "data protection by design" approaches requiring the provision of data protection safeguards since the conception of the systems and operations, as introduced in the Commission's proposal for the General Data Protection Regulation fostering harmonized and enhanced data protection rules in the EU(EUR-Lex 2012).

Finally, endorsement as best available techniques by technical and environmental authorities will be considered as a distinctive criteria of excellence.

3.4.4. In-design customisations

Complementary to "by-design data protection", "in-design customizations" will be considered as promotion of human agency (e.g. ownership of personal data flow, intentional responsible behaviour instead of mere actant). This new approach will be investigated to make apparent and transparent value-based architectural and structural choices that can be specified by citizens during the development and then decided upon when they actually use the products.

3.4.5. Openness

Openness is necessary to enable collaboration and it can be supported with various degrees.

Minimal openness delivers access to a set of data being made available. Access will vary depending on the content, however it can be expressed as the ability to provide, extract and reuse information from individual tools in an appropriate way, including long-term persistence of data. Essentially data can be released in machine-readable format as a downloadable dataset or similar remote service through a web Application Program Interface (API).

Access is also closely related to numerous quality dimensions of collected data:

- Accuracy as the extent to which data correctly represent the characteristics of the situation or event and should be balanced against implementation costs.
- Completeness as the extent to which data include items necessary to support the application for which they are intended
- Conformance as the extent to which data follow a set of explicit rules or standards for capture, publication and description
- Consistency as the extent to which data does not contain contradictions that would make their use difficult or impossible
- Credibility as the extent to which the data are based or delivered by trustworthy and trusted sources
- Timeliness as the extent to which data correctly reflect the current state of the entity or event and the extent to which the data (in its latest version) is made available without unnecessary delay

Further to access, a second and higher level of openness is transparency that provides information on the processing of the data and the algorithms involved. Building on transparency, the third level of openness is open participation with feedback on observed activity, reactions and proposal for change of processing goals.

3.4.6. Interoperability

IEEE has defined interoperability as the ability of two or more systems to exchange information and to use the information that has been exchanged through interoperable standard based services with defined content (Standards Coordinating Committee of the IEEE Computer Society 1991). Before establishing a multi-vendor standardized protocol through compatible and complementary programs, robust open APIs are needed to enable interaction of different programs on a network. Many software manufacturers provide such open APIs as a means to drive adoption of their tools. However non standardized API can be subject to unilateral change and require maintenance to preserve compatibility.

3.5. Empirical testing of sample devices

Having reviewed the conceptual framework of wearable sensing capabilities in the previous sections, which also serves as basis to establish assessment criteria for their evaluation as trusted and trustworthy technology potentially useful for self-documentation in health monitoring, the present section presents the organization of the empirical testing of sample devices. The most representative devices were selected with the aim of investigating functions and form factors of complex accessories as well as assessing the knowledge that citizens could gather and produce through their usage, both from information provided and direct experience. Products falling into the category of complex accessory were chosen due to their representativeness, as they are the most widespread types currently available on the market and popular among citizens.

The empirical testing was conducted as an inspection-based survey on the features characterizing wearable sensing capabilities. The test analysed each product during one week. The assessment of technical and functional requirements allowed for the verification of product reliability in fulfilling their function normally and the level of trust that can be expected from the knowledge produced by their use. Assessment of non-functional normative, openness and interoperability requirements allowed identifying the level of trustworthiness that users can hold in the used technology. The main results of the evaluation are illustrated in Table 3. The complete description of evaluation results with full details on the requirements of the sensors, including the technical characterization and support for specific digital health platforms is presented in Annex 1.

The evaluation also allowed drawing general remarks and trends as follows.
Technical characterization of wearable technology is provided more extensively for the sensors delivering raw data (cfr. Blood pressure monitor, smart body analyser, Vitaljacket, Bioharness 3, Smart Citizen Kit). However, the specifications only detail range and resolution of the sensing capabilities. Information on calibration and error would be necessary to give more accurate results. The devices delivering interpretative findings provide very little information on the technical characterization and sometimes

no information at all, as in the case of the Withings Aura sleep manager, where no information and specification on the kind of sensor used was given. Further assessment studies would be needed to establish technical references in field use validation of sensors enabling the production of trusted knowledge. Availability of raw data is an important requirement for this task.

3.5.1. Functionalities

Regarding functionality, the reviewed sensors offered a variety of perspectives of the possible solutions available to citizens. Accuracy of tracking devices still needs to be rigorously validated to account for error rates in measurement (Mosbergen 2014), however they serve the purpose of being inspirational in making people become more concerned and active by keeping their behavior under control.
Most of the solutions present in the market cover the full processing data flow from sensing, collection, interpretation and online storage. In commercial solutions, processing steps for interpretation from raw data are not transparent and the rationale behind the derivation of findings results obscure. An example of this is Beddit monitoring. Based on ballistographic measurements, findings of sleep patterns for duration and cycles are produced together with a coaching feedback score on the sleep and advice for sleep improvement (e.g. “do not go to bed if you do not feel tired”).

The lack of transparency on the finding processing raises concerns on their definition derived from unclear authoritative and legitimate sources of medical expertise. Withings Aura active sleep monitoring is another example of lack of transparency on finding processing. In addition to sleep monitoring, the sensor can aid the user to fall asleep or wake with light and sound adapted to his or her sleep status. No specification is provided on which kind of information is effectively processed, monitored and logged by the device. Commercial products are also extremely binding for the type of processing needing to cover the whole stages until online storage. Dedicated components are also necessary requiring a tight coupling of the sensor to the accompanying smartphone application and cannot work one without the other, as the BodyMedia example illustrated. Recent new solutions are being introduced that offer only the sensing and direct access to the raw data from the sensor. Examples are

VitalJacket, Zephyr and Angel (Angel sensor is a low cost sensor for activity monitoring under development) (Angelsensor 2014). These are very promising for the possible development of less binding and alternative processing models. Another trend is the technical improvement from manual towards automatic collection, which however is not enough reliable causing dataset loss when the transfer is not successful.

3.5.2. Usability criteria

Usability evaluation confirms that wristband is the most comfortable and practical form factor for longterm monitoring offering a balanced trade-off between invasiveness of the sensing and the depth of the data generated. Initial efforts and skills are required to learn how to operate wearable sensors, however once learnt, usage is straightforward.

3.5.3. By-design normativity and in-design customisation

Among by design normativity protection measures only safety is currently supported. However, safety information provided to the citizen is extremely diverse across various sensors; certified products for medical devices specify more relevant information on risks and exposure. No security by-design, privacy by-design protective measures and in-design customisations are referenced or provided in the products evaluated. A trend identified in the privacy policies of the commercial devices investigated was to permit "anonymised" or de-identified data to be reused for statistics or further analysis. One potential well-documented risk of such procedure is that of re-identification, where-by previously anonymised data can be re-associated with the identity of the individual it was captured from. Recent research demonstrated the ease with which location data was used to identify an individual, even with coarse datasets, or with sporadic sampling interval (De Montjoye et al. 2013). Further technical verifications would be required to investigate if the data collected and uploaded to the cloud online space effectively comply with the principles of data protection (proportionality, data minimization and anonymization/aggregation of the presented results). By design normativity and in-design customisations could potentially be introduced in a new breed of products that could be realized with the recent sensors offering access to raw sensor data.

Sensor	Functionality	Usability criteria	By design safety	By design security, privacy in-design customization	Openness	Interoperability
Beddit sleep manager	Beddit application semi-automatically launches data collection through start and stop control and needs to be running all night to collect the measurements. Based on the measurements, findings of sleep patterns for duration and cycles are produced and logged in the cloud storage. The sensor accuracy was overall fair as it could track total sleep time night over night	Beddit sensor is a strip laying across the mattress with a sticky tape that fixes to the bed. The strip is very thin so that the user does not feel its presence under the bed sheet. Having to sleep all night with the smartphone active is not comfortable and healthy. The interface presenting the sleep patterns is qualitative and clumsy not providing clear insight on the temporal frames mapping the various types of sleeps	Beddit safety recommendations are limited to avoidance of use with babies or children, liquids or wet. More extensible descriptions of electromagnetic precautionary conditions and applicable regulations could be relevant for users	None	Beddit application API is under development providing services for authentication and access of sleep patterns from cloud storage. Accuracy and completeness of the data made available could not be verified due to the qualitative output of sleep patterns presented to the user. On request of multiple users, access to raw data is supposed to be provided at a later stage	None
Jawbone UP activity monitor	Jawbone UP data is first collected on the sensor and then manually uploaded in the cloud storage. The upload requires the user to insert the sensor in the smartphone, to authenticate with a password to the smartphone application and execute the synchronisation. Manual synchronisation avoids dataset loss. Acquired accelerometer data are processed to produce accurate findings for day and night activity (steps, calories burnt, sound/light sleep, awake time). All findings are stored in the cloud online space. Jawbone UP sensor is accurate and does not track steps while you are driving.	Usage instructions are missing from the packaged product; only after seeing the video tutorial on installation it was possible to test it. Once learned how to use it, the interaction is comfortable though not context ware. The user has to switch between day and night mode, as well as checking the charge status.	Safety recommendations are very limited and advise on device operation avoiding contact with liquids	None	Jawbone UP application API provides access to sensor findings archived in cloud storage. The data made available are accurate and complete with respect to the accurate values presented to the user.	Jawbone UP application API supports the creation of causality links with other external applications (IFTTT ad-hoc connection protocols). The connections can support limited control policies to trigger and communicate updates of sensor findings among the related services. A new version was announced to add support for the Apple Healthkit ecosystem and Apple Health app to track and update information on a user's diet and physical activity. This newest application does not require the company's fitness tracker and could work with over a hundred of other apps and devices.
BodyMedia link armband activity monitor	BodyMedia device was not tested as the app was available for limited countries (US, Canada, Australia, New Zealand), it also required fee subscription to track the data from the BodyMedia website	BodyMedia information on availability and local restriction of use should be better advertised to consumers (e.g. sales conditions). BodyMedia armband is not much confortable, as it must be worn tightly on the upper arm.	Detailed safety instructions describe the electromagnetic environment of use and recommendations for electromagnetic emissions to which user can be exposed when using the sensor	None	BodyMedia API, which provided access to user collected data from the cloud, is discontinued and replaced by Jawbone API	None

Table 3. Results of empirical testing of wearable sensors.

Sensor	Functionality	Usability criteria	By design safety	By design security, privacy in-design customization	Openness	Interoperability
Withings blood pressure monitor	Blood pressure monitor is a semi-automatic sensor where data acquisition is controlled by the smartphone Health Mate application. The application is accessed through password authentication and it uploads acquired raw data directly to the cloud storage where the user can review them. The application provides users informative feedback on conditions and reference values	The design of the blood pressure remote control could be improved to deal with the situation when the pairing is not successful. Acquired data can get lost during upload and the acquisition needs to be repeated. The buttons to launch the interaction appear only if the pairing is successful, which can be confusing for the user	Safety recommendations advise to avoid using the sensor in the presence of liquids and with children. Further recommendations provide electromagnetic specifications of the environment where the device should be used. It is compliant to the European Directive 93/42/EEC on medical devices and is safety certified in the US (FCC regulations)	None	Health Mate application API enables access to user raw data archived in the cloud storage. Data made available are accurate and complete with respect to the values logged in the cloud online space and presented to the user. All collected raw data can also be emailed to third-parties in CSV format	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app
Withings smart scale	The smart body analyser needs the setup of the Health Mate application for the remote wireless connection. The Health Mate application is the same for blood pressure sensor. The data collection of the smart body analyser is fully automatic. It simply requires the user to step on the smart scale. The scale has the ability to recognize more than one user from different weight and/or body fat % composition. The editing of wrong acquisitions could be a functional improvement for the logging	The smart body analyser is a pretty straightforward device not requiring any in-depth learning. Some users might, however, appreciate more information explaining the sensor capabilities and mode of functioning	Safety recommendations report the device is not suitable for people with pacemaker or other internal devices	None	Health Mate application API enables access to a subset of smart body analyser data on weight stored in the cloud. Air quality and temperature are not yet supported, however the data made available are accurate and complete	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.
Withings aura active sleep manager	Similarly to the previous Withings sensor, Aura sleep manager is paired to the Health Mate application, which is the same. Aura sleep manager automatically measures sleep patterns from data acquired by the sleep sensors. Limited details are provided on the sensor technology. As the user sleeps in bed, the data are uploaded to the smartphone placed nearby and running all night. Aura accuracy seems problematic reporting less than half time in bed per night. It is not clear if the issue may be caused by the thickness of mattress or connection leakages	Aura is only available on iOS devices. Interaction with Health Mate application could be better described to explain the sensing set-up (is it really necessary to sleep with a smartphone running?)	Aura complies with EU, US, Canadian conformity checks for radiation exposure. It may be used by children older than 8 yrs and elderly.	None	Health Mate API enables access to findings processed on sleep patterns and stored in the cloud online space	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.

Table 3. Results of empirical testing of wearable sensors (continued).

Sensor	Functionality	Usability criteria	By design safety	By design security, privacy in-design customization	Openness	Interoperability
VitalJacket shirt ECG monitor	Vitaljacket data collection is fully manual. Data are recorded in a secure digital card and transferred to a standalone desktop application to view ECG graphs. Potentially it can evolve towards semi-automatic support and connection to mobile smartphones	Vitaljaket requires effort to place the ECG leads in the correct part of the body. For this task, there are good illustrations both in the instructions and on the t-shirt	Vitaljacket is compliant to the European Directive 93/42/EEC on medical devices	None Potentially, a data collection application could be developed with support of own by-design requirements and in-design customisations	Acquired ECG data can be accessed and visualised in a proprietary viewer provided by the manufacturer. As the data are made available in proprietary format, they cannot be processed	None
Zephyr Bioharness physiological monitor	Bioharness sensor semi-automatically monitors heart and breathing rate while it is worn. Monitored values are sent to the Zephyr Life smartphone application, which can be accessed through password authentication for viewing the readings. Zephyr Life does not support remote data collection, which is only available in a desktop proprietary application used to monitor a group of users or patients	In addition to the chestband, the sensor is also available as a biopatch, which is more comfortable to wear. However, although the biopatch is widely advertised online, it is not ensured to properly function	Bioharness safety instruction for electromagnetic compatibility are generic and only available online. They describe the risk of interference with or from other radio transmitting or medical electrical equipment in close proximity	None Potentially, a data collection application could be developed with support of own by-design requirements and in-design customisations	Bioharness sensor API is available to developers intending to build own data collection environments	None
Smart Citizen health environmen t monitor	The Smart Citizen sensor requires initial configuration of the kit communication channels and online application account. Once the sensor is configured, sensor data are automatically collected and publicly published online.	Once set-up and configured, the Smart Citizen kit runs by itself and the sensor uploads the measured values in the cloud storage. Information provided with the kit and on the website is extremely detailed. One point that could be improved is the provision of calibrated conversions for gas-monitored values. The values are published as resistance output and can only be transformed qualitatively into gas concentrations	The Smart Citizen kit has no electrical hazards	None	Smart Citizen kit API supports the querying of sensor data from the remotely archive in the Barcelona Fab Lab cloud server. The data made available are accurate and complete. The Smart Citizen sensor is fully transparent as all information on the components and software are available online for reproducibility. It is also participatory organised in a community of citizens with an active forum answering requests relating to technical issues and suggestions for improvements	None

Table 3. Results of empirical testing of wearable sensors (continued).

3.5.4. Openness

Openness is well supported across all sensors, although it is most provided as access to the data at the application level (i.e. access to findings and raw data stored in the online

cloud space made available by the application). Sensor level openness is preferable as this ensures access to data acquired from the device in real-time, i.e. raw data. DIY assembled kit and a few recent commercial sensors provide openness at the sensor level (cfr. Smart Citizen Kit, VitalJacket, Bioharness 3 and Angel sensor under development). These are very promising for the development of more transparent and participatory processing models and products.

3.5.5. Interoperability

Interoperability of health sensors and applications is recently being promoted by vendor specific APIs by Google Fit and Apple HealthKit (Spence 2014). Adoption is still in early stages as only HealthKit was realesed in September 2014. Examples of solutions announced to support HealthKit are Jawbone and Withings (Comstock 2014). However, interoperability, portability and aggregation of user data across tools comes at the price of further sharing all personal health data online with Google and Apple, as well as being bound to their architectural framework of wearable health processing. At present Jawbone and Withings applications can already interconnect to other applications with customizations performed by the user through conditional connection protocols. The connections are IFTTT (IF-This-Then-That) predefined recipes to carry out specific actions when users perform commands (IFTTT 2014), for example emailing past months reading from the smart scale to a recipient. IFTTT execution also requires the sharing of personal health data with involved third-parties.

The review of the technical and functional characterization of sample wearable technology showed that current products could provide fair levels of trust as they fulfill their function normally, delivering what it is promised and what the user expects. The production of trusted knowledge for self-documentation requires promotion of specific technical requirements for ensuring accessibility and further validation. Trustworthiness according to criteria of security, privacy and user in-design customization could be much improved by developing specific solutions that enable citizens to protect, control and choose the data flow from the sensor to the interfacing apps and platforms. Recommendations for areas of improvements on features and best practices of trusted and trustworthy wearable sensors will be illustrated in chapter 4.

4. Digital platforms for health activities

The emergence and widest adoption of technological advances including social media, smartphones, games and sensors provide significant opportunities for citizens to be informed by novel tools based on statistics, data and predictions. Being so empowered, citizens can act individually or in collaboration with others drawing on collective experience to take care of their personal and collective health. New opportunities are opening up for citizens to take a more active role in maintaining their health and to demand a greater role in the processes of clinical decision making concerning them.

Following this trend, the concept of healthcare could be extended to become a complex, ongoing, data-rich process of managing acute, chronic, general wellness and enhancement conditions using a wider variety of traditional and non-traditional health resources such as collaborative peer networks (Swan 2009). The transition could be enhanced by the convergence of technical tools contributing to the empowerment of citizens to manage their health more actively. Wearable, social network and web technologies could be integrated into digital platforms with rich user interfaces enabling citizens to collect data about their own body and health, to manage this information, to share it with peers, colleagues and/or with clinicians and even to analyse it to gain knowledge that could help them to improve their health.

To give a general overview on the recent developments in the field, typical categories of the digital platforms for health and wellness will be introduced in the next sections.

4.1. Definition(s) and classification(s) of digital health platforms

Many new virtual spaces from digital health platforms are becoming available online. In these environments individuals with shared interest in self-management of health can find services for measuring, tracking, experimenting, engaging in observations, treatments, research and share their knowledge with others. In general, digital health platforms can be characterized by increased levels of information flow, collaboration, as well as support for quantitative, predictive and preventive aspects.

Based on the type of information exchanged in the online virtual space, most digital health platforms can be categorized according to the following models:

- Health social networks as web-based platforms allowing individuals to create their own personal profile and build a network of connections with other citizens to share information on similar health situations, conditions, symptoms and treatments. Health social networks are primarily directed at patients, but caretakers, researchers and other interested and knowledgeable parties may be able to participate (Swan 2009). Some are oriented towards patients with a specific chronic condition (Tudiabetes 2014), others are more general and open to patients with any chronic condition (Patientslikeme 2014), and a few others target people wanting to change a particular health-risk behavior (eg, smoking cessation) or other health-related lifestyle factors. Services may range from basic emotional support and information sharing, to counseling with physicians, self-reporting of own conditions, collaborative filtering to identify potentially related conditions that patients might be experiencing and match patients in similar situations (Swan 2009). The quantitative data collected enable decision support and hypothesis generation.
- Quantified self-tracking systems as wearable sensor platforms helping citizens to improve various aspects of wellness and health through regular recording and reviewing daily activities and body measured data. Self-tracking wearable sensors are available to track large-scale datasets of the self and record citizens' activity, sleep and diet, as well as providing supplementary services like web-based data management tools (with feedback for introspection and self-experimentation), data sync and storage. Health aspects that are not obviously quantitative such as mood can be recorded with qualitative words that can be mapped to a quantitative scale, or ranked relative to other measures (Swan 2009).

Digital health platforms can also be categorized according to the business model underlying their implementation, as follows

- Commercial digital health platforms aim at centralizing access, logging and management of a wealth of collected sensor data providing free services to end-

users in exchange of the control of their data. The intent is to gather and anonymize large datasets from which to build added value for other third-parties.

- Cooperative digital health platforms are a new model proposed by HealthDataBank where ownership and control is managed by their member citizens and not by shareholders. Members are the primary source and beneficiary of the commercial value of the personal health data determining third-party organizations who can have access to their anonymised data (doctors, researchers, etc.) and how to invest revenues generated by the data exploitation (Hafen, Kossmann and Brand 2014).
- Open-source digital health platforms are web systems for continuous collection, management and sharing of sensory information from third parties body-worn sensors. Although not perfect (for example because of weakness in built-in security), the system is fully made available by researchers and is built around shared standards and reusable components allowing interested parties to expand the functionality of the system. The purpose is to promote rapid authoring, integration, evaluation and adoption of novel personal data capture practices. Examples of opensource digital health platforms are open mHealth (Estrin and Sim 2010) and Fluxtream (Wright 2014).

The brief overview on the trends and developments in digital health platforms shows the extent of the growing interest in the domain presenting various types of solutions that will need to be taken into account during the analysis.

4.2. Scope of the analysis for health activities

Continual advances of wearable sensing technology, as well as their integration into digital health platforms have started to demonstrate potential to bring health care into the everyday life of the citizen, favoring health promotion for disease prevention.
For the purpose of the present analysis we will focus our attention on quantified self-tracking systems, which are the ones where the integration of the sensors is progressing more rapidly.

The analysis will consider a range of platforms relevant for self and community management of health with active engagement of individuals by making them the focal point of the sensing platform and allowing them to collect and share targeted information about their daily patterns and interactions at a community level.
Concerning the integration of the wearable sensors, the analysis will consider as reference set the devices surveyed in chapter 2.

A sample of the most representative platforms was selected to comprehensively address features and set-ups from commercial and open source solutions.
The list of systems is illustrated in Table 4. It allows covering the extent and characteristics of digital health platforms and research approaches available to everyday users.

Following an overview of the general models according to which digital health platforms are typically organised, the next section will outline functional and non functional capabilities for collection, analysis, interactivity and sharing services offered by quantified self tracking systems (i.e. the category of digital health platforms considered in the present analysis).

Digital platform	Category	Integrated sensors	Health activities	Other capabilities
Dacadoo	commercial	BodyMedia, Jawbone Up, Withings blood pressure and smart scale	Goal coaching, logging of movement, exercise, sleep, nutrition and stress	Racings and competitions with members
Fluxtream	open source	BodyMedia, Jawbone Up, Withings smart scale potentially Beddit sleep manager, Withings blood pressure and aura, Vitaljaket, Zephyr Bioharness and Smart Citizen kit	Logging of movement, sleep, nutrition, vitals and daily notes imported from other tools	Sharing with members
HealthMate	commercial	BodyMedia, Withings blood pressure, smart scale and aura	Logging of movement, sleep, vitals	Sharing with members

Table 4. Digital health platforms under review.

4.3. Capabilities of quantified self tracking systems

Quantified self tracking systems are digital health platforms that have evolved and scaled up from wearable sensor applications to collaborative large-scale data collection and processing systems with enhanced sensor processing, interactivity and sharing capabilities. A typical system model describing stakeholders and architectural components is illustrated in Figure 4.

Relevant stakeholders are citizens collecting the data with wearable sensors and capabilities illustrated in chapter 2. To make them persistent, data can be uploaded to a quantified self tracking platform where they can be aggregated and further processed under the responsibility of platform administrator. Depending on the platform capabilities they can also be shared with trusted third party stakeholders (e.g. doctor, other family members, friend). In addition to functional capabilities qualifying the general system model, quantified self-tracking systems can be characterized by non functional features, such as safety, security, privacy and usability. Non functional features share the same definition specified for wearable sensor systems, which will be restated or detailed in the following sections.

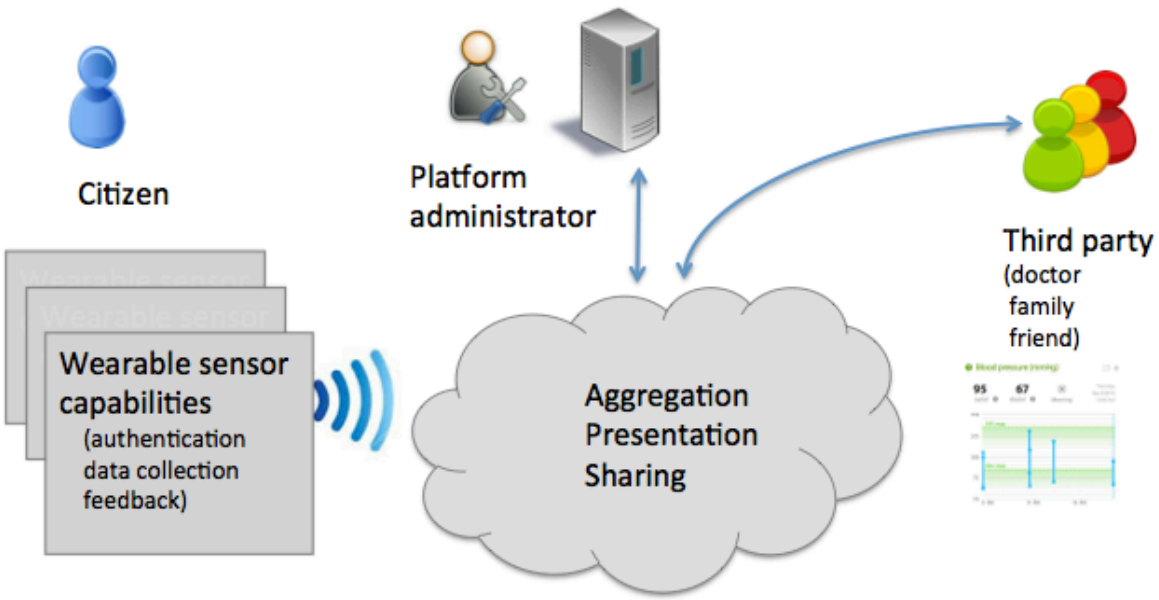

Figure 4. System model of quantified self tracking platform.

4.3.1. Functionalities

Quantified self tracking systems complement wearable sensors for sensing and data collection capababilities offering a number of centralized functionalities for providing enhanced management and a long term repository where collected data are aggregated, processed and represented through various interfaces (statistical data on a map) or remain available to third parties. Typical functional components intervene from the sensing process to the presentation and sharing of the results to citizens and interested third parties, who are trusted stakeholders (e.g. doctor, family members or friends).
To make interaction with the platform more engaging, presentation components can also be enhanced with gamification (i.e. activities can be made enjoyable through the incorporation of elements of game (Deterding, S., et al. 2011) and social networking developments.

4.3.1.1. Data type handling

The component for handling data types is tasked with capturing and integrating different kinds of data. They can be prevalently wearable sensor data, however other data types can also be of interest. Complementary data types can be objective measurements such as profiles of individual exposome (i.e. an individual's lifetime environmental and nongenetic exposures) and records of laboratory tests.

4.3.1.2. Storage

The component ensures the long-term storage of data collected from the sensors. Rather than traditional databases, specific repository can be adapted to the management of sensor readings. This solution creates a uniform and centralized storage that is also responsible for indexing the sensor characteristics to enable applications to discover what is available for their use.

4.3.1.3. Processing

The processing component extracts features of interest from the sensor readings at individual and larger scale. The component analyses the data uploaded in the platform and prepares them for the presentation component.

4.3.1.4. Presentation

The presentation component presents the results obtained by the processing component to citizens. The results are either presented in the form of raw data to allow citizens to analyse them themselves, or in the forms of graphs, maps, and overlays. Presentation services include feedback to inform citizens about how well they are doing in the platform to achieve his/her goals, making progress visible through ranks, levels and scores.

4.3.1.5. Sharing and Interaction

The sharing and interaction component comprise services enabling the distribution of results to other interested and trusted parties. Visibility and access to results could be extended to trusted individuals, like family members. Interaction services could include discussion forums to hold conversations and exchanges messages with friends. Within a platform where people can chat with each other or help each others out, a community can be established.

4.3.2. Usability criteria

Aspects relevant to usability evaluation will be considered to assess ease of use and usefulness in interactions with quantified self tracking systems. The analysis will be performed by inspection and will examine the extent to which functionality is compatible with user expectations, ease in accomplishment of desired functions. The analysis will focus on configuration set-up and management of goal oriented observations. Additional features relevant for user acceptance are effort required to keep the data updated, costs and appealing of the systems.

4.3.3. By design normativity

By design normativity consists of protective measures relating to privacy and security features pre-embedded in digital health platforms. As interactions with digital health platforms are conducted with wearable sensors, no additional safety normativity is required for the management of digital health platforms.

Privacy and data protection are major concerns. Similarly to wearable sensing systems, digital health platforms may also pose significant risks concerning privacy and data protection due to the lack of transparency and awareness on personal data processing by third parties (e.g. unwanted use and sharing of citizens' health data). Legal guidance by Article 29 Working Party recommends the application of data protection principles (purpose limitation, data minimization, obligation to correctly inform citizens of their rights and appropriate security measures such as data encryption and authentication mechanisms) (Article 29 Working Party 2013). The analysis will review "data protection by design" approaches requiring the provision of data protection safeguards since the conception of the systems and operations, as introduced in the Commission's proposal for the General Data Protection Regulation fostering harmonized and enhanced data protection rules in the EU (EUR-Lex 2012).

4.3.4. In-design customisations

Complementary to "by-design data protection", "in-design customizations" will be considered as promotion of human agency (e.g. ownership of personal data flow, intentional responsible behaviour instead of mere actant). This new approach will be investigated to make apparent and transparent value-based architectural and structural choices that can be specified by citizens during the development and then decided upon when they actually use the platforms.

4.3.4. Openness

Openness is necessary to enable collaboration and it can be supported with various degrees.

Minimal openness delivers access to a set of data being made available. Access will vary depending on the content, however it can be expressed as the ability to provide, extract and reuse information from individual tools in an appropriate way, including long-term persistence of data. Essentially data can be released in machine-readable format as a downloadable dataset or similar remote service through a web Application Program Interface (API).

Access is also closely related to numerous quality dimensions of collected data:

- Accuracy as the extent to which data correctly represent the characteristics of the situation or event and should be balanced against implementation costs.
- Completeness as the extent to which data include items necessary to support the application for which they are intended
- Conformance as the extent to which data follow a set of explicit rules or standards for capture, publication and description
- Consistency as the extent to which data does not contain contradictions that would make their use difficult or impossible
- Credibility as the extent to which the data are based or delivered by trustworthy and trusted sources
- Timeliness as the extent to which data correctly reflect the current state of the entity or event and the extent to which the data (in its latest version) is made available without unnecessary delay

Further to access, a second and higher level of openness is transparency that provides information on the processing of the data and the algorithms involved. Building on transparency, the third level of openness is open participation with feedback on observed activity, reactions and proposal for change of processing goals.

4.3.5. Interoperability

IEEE has defined interoperability as the ability of two or more systems to exchange information and to use the information that has been exchanged through interoperable standard based services with defined content (Standards Coordinating Committee of the IEEE Computer Society 1991). Before establishing a multi-vendor standardized protocol through compatible and complementary programs, robust open APIs are needed to enable interaction of different programs on a network. Many software manufacturers provide such open APIs as a means to drive adoption of their tools. However non standardized API can be subject to unilateral change and require maintenance to preserve compatibility.

4.4. Empirical testing of sample platforms

Following the review of the conceptual framework for the analysis of capabilities from digital health platforms in the previous sections, which also serve as basis to establish assessment criteria for their evaluation as trusted and trustworthy technology potentially useful for self-documentation in health monitoring, the present section presents the organization of the empirical testing of sample systems. The most representative systems were selected with the aim of investigating functions and other requirements as well as assessing the knowledge that citizens could gather and produce through their usage, both from information provided and direct experience. Platforms identified as quantified self tracking systems were chosen due to their representativeness, as they are the most widespread types currently available on the market and popular among citizens. The chosen systems provide illustrative examples of the main categories (opensource and commercial software) and features (e-coaching, self-exploration and documentation) currently available to citizens. The empirical testing was conducted as an inspection-based survey on the features characterizing platform capabilities. The test analysed each system during one week. The assessment of technical and functional requirements allowed verifying system reliability in fulfilling their function normally and the level of trust that can be expected from the knowledge produced by their use.

Assessment of non-functional normative, openness and interoperability requirements allowed identifying the level of trustworthiness that users can hold in the used technology. The main results of the evaluation are illustrated in Table 5. The complete description of evaluation results with full details on the requirements of the systems, including the technical characterization and support for integration of specific applications and sensing devices is presented in Annex 2. The evaluation also allowed drawing general remarks and trends as follows.

4.4.1. Functionalities

Limited information is available for the technical characterisation of the analysed platforms. The motivation derives from the relatively novelty of quantified self tracking functionalities and no reference architecture has emerged among the existing ones.

Although all three systems aim to support users in maintaining their health and wellness, each of them follows different approaches and designs. The commercial platform Dacadoo gathers sensor information in order to determine individual health scores, coaching and planning of healthy activities towards goal achievement, however it the rationale for coaching and health score updates remains obscure and is not enough linked to the sensing information.

Platform	Functionality	Usability criteria	By design security and privacy	In-design customization	Openness	Interoperability
Dacadoo	Dacadoo acquires sensor data from connected services to determine an individual health score based on collected data and filled in questionaires. Processing services provide expert coaching and planning of healthy activities towards goal achievement both individually and in teams, although the coaching is not supported by background sensing information. Information at community level is only provided to third parties and not to the individuals. The presentation partially supports visualisation of past sensor measurements in sensor by sensor follow-up graphs. Limited information relating to event notifications can be shared on connected social networks	As the system is aimed at providing a holistic overview of the health status of a person, the interface presents a lot of information on questionnaires, activities and notifications making the user feel lost in the different screens. It is also difficult to perceive insight on general health status resulting from contributions of the different activities performed and information provided	User data are stored encrypted in the platform data centre protected by a security firewall. Data presented to the user are also transferred through secured communication channels. Privacy settings allow setting the profile for sharing of the status information (health score, completion of proposed goals, etc.) and event notifications relating to performed activities. The settings are private, shared with friend only, public	None	None	Interoperability is supported as interconnection to get input from third-party applications and provide notifications to partnering social networks
Fluxtream	Fluxtream is a personal visualisation tool for tracking daily habits, identifying strengths and weaknesses, and getting a comprehensive view on your self-tracking devices and the services used for self-monitoring. Unlike many systems that provide fragmented visions, the system aggregates and recombines multiple data sources to generate summaries and correlations. The diverse data streams are plotted on a common timeline and visited locations are visualized on a map. Collected findings are stored in the cloud online space and can be shared with community friends. Fluxtream also allows to export all findings in CSV files.	The user interface of Fluxtream is cluttered and oriented for scientific users. Analysis and interpretation of collected data are limited to simple presentations based on minimal interpretation, such as extremely low-level data views or long historical event streams. This places the burden of synthesis on the self-tracker.	Data presented to the user are also transferred through secured communication channels. Information can either be private or shared with community friends	None	Fluxtream application API provide calls to the main services supported (authentication, data sharing, data retrieval, export, import and timeline related operations)	Fluxtream application API supports the integration with other external health applications.

Table 4. Results of empirical testing of digital health platforms.

Sensor	Functionality	Usability criteria	By design security and privacy	In-design customization	Openness	Interoperability
Health Mate	Health mate provides logging services to store history of health data and improve behaviour over time. Data can be logged manually or automatically with tracking devices. The system allows setting achievable goals, and send reminders to focus user efforts. In addition to setting goals to overcome, the software suggests tips to move more or better sleep. A trophy system and rankings with friends will motivate the user to follow advice.	The user interface is airy and visual, easing the access to the most important functions at the top of the screen, which is useful for scanning a glance its activity, weight, or air quality at home. The patterns are visualized in separate timelines making it difficult to make correlations and discover trends	Data presented to the user are also transferred through secured communication channels. Information can either be private or shared with community friends	None	Health Mate application API enables access to user raw data archived in the cloud storage. Some collected raw data can also be emailed to third-parties in CSV format.	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The application cloud storage can be connected with external health services. The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.

Table 4. Results of empirical testing of digital health platforms (continued).

The opensource Fluxtream platform provides comprehensive visualization tools for aggregating and combing all monitored data sources in common timeline and location maps for self-exploration of correlations previously unknown. The commercial Health Mate is an intermediary solution between Dacadoo and Fluxtream, as it provides logging of past historical data, as well as coaching, scores and tips. In Dacadoo and Health Mate data are not presented together. When users are tracking different factors either using a single tool or multiple tools, they must consult each corresponding graph separately and there is no way to find relationships within different collected datasets.

All three platforms provide initial features for sharing information with peers and community friends, however they are insufficient for building a shared knowledge space. Interpreting data is confusing and users usually need help to understand the charts or reports that are generated. To figure out what is causing fluctuations in the readings, users must analyse the data themselves or seek help. There are no guidelines or recommendations for decision support based on health status.

4.4.2. Usability criteria

Usability evaluation confirms that visual interactive graphs are the most intuitive and actionable user interfaces for self-documentation and self-exploration. Health Mate provides the best interface among the three, although not fully compatible with the end user tasks. The patterns are visualized on separate timelines making it difficult to find correlations and build new knowledge.

4.4.3. By-design normativity and in-design customization

Among by design normativity protection measures only security and privacy are relevant for digital health platforms.

Minimal security by-design and privacy by-design protective measures are provided. Security by-design consists of ensuring data transfer through secured communication channels between the platform and the user, while privacy by design provide online private spaces that can eventually be shared with community friends. Similarly to wearable sensors, a trend identified in the privacy policies of the commercial systems investigated was to permit “anonymised” or de-identified data to be reused for statistics or further analysis. One potential well-documented risk of such procedure is that of re-identification, where-by previously anonymised data can be re-associated with the identity of the individual it was captured from. Recent research demonstrated the ease with which location data was used to identify an individual, even with coarse datasets, or with sporadic sampling interval (De Montjoye et al. 2013).

No in-design customisations are referenced or provided in the platforms evaluated. Further technical experimentations would be required to investigate the feasibility of encrypted end-to-end storage for providing truly personal archives in the cloud online space. By design normativity and in-design customisations could potentially be introduced in a new breed of platforms that could be realized based on opensource technology.

4.4.4. Openness

Openness is being promoted across multiple platforms, providing access to the data at the application level (i.e. access to findings and raw data stored in the online cloud

space made available by the platform application). Some platforms like Dacadoo prefer not support open API to provide access to collected data, while only import the data from accessible sensing open APIs. Fluxtream and Health Mate fully support open API to provide access to collected findings.

4.4.5. Interoperability

Interoperability of digital health platforms follows the same trend as illustrated for health sensors and applications. Interoperability is recently being promoted by vendor specific APIs by Google Fit and Apple HealthKit (Spence 2014). Adoption is still in early stages as only HealthKit was realesed in September 2014. For example, the Withings platform announced to support HealthKit (Comstock 2014). However, interoperability, portability and aggregation of user data across tools comes at the price of further sharing all personal health data online with Google and Apple, as well as being bound to their architectural framework of wearable health processing. At present services from Withings platform can already interconnect to other applications with customizations performed by the user through conditional connection protocols. The connections are IFTTT (IF-This-Then-That) predefined recipes to carry out specific actions when users perform commands (IFTTT 2014), for example emailing past months reading from the smart scale to a recipient. IFTTT execution also requires the sharing of personal health data with involved third-parties.

The review of the technical and functional characterization of digital health systems for quantified self activities showed that current solutions show variable levels of trust across different designs and intended goals of the platforms, however they can fulfill their function normally, delivering what it is promised and what the user expects.
Comparing open source systems supporting self-reflexivity as against commercial ecoaching ones that rely on persuasive nudging to strengthen individual capacities for self-regulation, more widespread ecoaching systems present more risks to orient users towards stereotyped behaviors and lifestyles, while open source systems supporting self-reflexivity and self-tracking provide increased transparency in accessibility, controllability of data access, usage, and distribution by the individual, and preservation

of precision. The production of trusted knowledge for self-documentation requires promotion of specific technical requirements for ensuring data accessibility and preservation of precision. Similarly to wearable sensors, trustworthiness according to criteria of security, privacy and user in-design customization could be much improved by developing specific solutions that enable citizens to protect, control and customize the whole data flow from the sensor to the interfacing apps and platforms. Recommendations for best practices and areas of improvements towards trusted and trustworthy quantified self tracking platforms will be illustrated in chapter 4.

5. Conclusions

With advances in quantified-self wearable sensors and platforms, it is now possible to capture and record data about nearly all aspects of human health and fitness, including mental, emotional, physiological, lifestyle and social dimensions. By analysing these numbers, people could have a better understanding of their health status and their relationship to the world around them.

However, quantified-self wearable sensors and platforms are in their infancy and still need improvements. The majority of these systems uploads sensor data from the health sensor to the platform provider servers, using a smartphone for transmission of data, and for displaying measurements and results. The present empirical analysis, conducted to explore to what extent trust and trustworthiness of current quantified-self technology is well-grounded, has highlighted concerns on data collection practices and privacy, specifically with regard to how device providers make use of the data obtained. To address these concerns, a number of recommendations are proposed in the following section for ameliorations towards truly citizen-centric developments of personal and community health technology.

In the evaluation performed from data collection practices, a trend was identified concerning the potential risk of re-identification, when previously anonymised data can be re-identified. To avoid potential misuse of health sensitive data, security-by-design and privacy-by-design protective measures should be implemented.

Well-defined policies

A concern needing improvement is the promotion of well-defined policies for ownership, accessibility and control of data, as well as access to raw data, as all these areas still lack clarity. Participants should be granted access to their raw data (both generated by, and uploaded in digital health platforms) to enhance transparent use of technology, better control of health and preservation of precision all throughout the processing flow: from sensor capture to platform reuse of information.

Right to raw data

In order to foster fairness and reciprocity between the data subject and the data collector, best practices for agency enhancement would require that data collectors by default provide data owners with their raw data. This approach would enable data subjects to act upon their considered judgment, and would expand their agency in at least three ways: (i) freedom to decide, (ii) option of independent interpretation/ analysis, and (iii) informed decision about ownership (Lunshof, Church and Prainsack 2014).

Due to the limited validation in low-cost health consumer products, questions arise on the best way to provide result interpretation to citizens/end-users. Are elaborated and interpreted data alternative and preferable to raw non-certified quantitative measurements? Do citizens/users have a moral right of access to raw data? These issues have significant ethical and legal implications (Lunshof, Church and Prainsack 2014).

To avoid misinterpretations and responsibilities concerning 'not yet certified' measurements, the current trend consists in returning to end-users qualitative findings—namely data interpreted through aggregated range values combining different raw data components. An example of this approach is illustrated in the "Every[citizen]Aware" case study where citizens are engaged 'as sensors' to help produce air quality maps throughout the city. Although the monitoring system collects data from eight multiple sensors, only one 'air quality' result is returned to end-users (Everyaware 2014). However, end-users might also be interested in getting raw data or in knowing how data have been manipulated to produce specific representations. Indeed, in this way citizens would become more aware about measurements, their meanings and implications, and more actively involved as co-producers of useful knowledge in validating and improving the tools.

Citizen-centric approach to technology and open-source, independent design

Improvement of acceptance and trustworthiness of quantified-self sensors and platforms should be promoted by adopting a citizen-centric approach to technology development, an "in-design" perspective. Also, independent open source solutions would allow an easier customization to changing requirements, forms of protections, and issues to be addressed, as they promote universal access and redistribution of the software code, including subsequent improvements from users. Current commercial

system architectures are rather inflexible, as confirmed by the trend towards interoperable but bounded services, where all personal health data must be shared with Google and Apple processing platforms.
Independent and alternative design and development initiatives should be opened up to citizens. These should be entitled to propose and validate possible set-ups, choices and limitations through evidence-based and extended, participatory peer-review.

Transparent design

At the same time, manufacturers should enhance transparency creating trust and providing clear information on policies, benefits, limits and risks according to labeling and self-certification standard criteria as proposed by Health on the Net foundation (HON 2010). Every piece of information covering the necessary aspects helps decision makers and/or citizens, in professional settings as well as for private use, to determine whether the technology can be trusted.

End-to-end security measures

A final concern and recommendation addresses the control of security measures for protecting collected data.
While this report primarily focused on the current technical state-of-the-art and on some normative measures aimed at empowering users, the issue of security—not explored here—remains an essential one.
For instance, an emerging approach that could be applied relies on enhanced secure end-to-end architectures with encryption controlled by the end-user. An implementation of such architecture is the SpiderOak back-up system providing cloud-based storage, synchronization and sharing of data, with encryption from end to end (Yadron, and Macmillan 2014). Third party providers do not have the keys to decrypt its customers' files, so its data centers only have encrypted data, adding another layer of protection and enhancing the control of end-users, who become the only custodians of the data.

In order to have trusted and trustworthy wearable sensors and platforms should both function normally, namely deliver what it is promised and what the user expects, and support specific non-functional criteria for usability, by-design normative protection,

in-design customisation, openness, and interoperability. To this end, the proposed recommendations represent essential prerequisites for citizen/user empowerment, and for equitable use and meaningful community participation that it would be otherwise difficult to fully achieve. Improved policies about ownership, accessibility, access to raw data are especially necessary to ensure the preservation of accuracy and precision when data are reused in knowledge production. Normative protective measures, self-certification, peer-review and participatory in-design development are also indispensable to promote a trust-enabling environment, capable of rewarding ethical behavior while preventing improper and malicious activities.

References

References on ethical and legal reflections

References on Privacy-by-Design

Boyle, J. (1996). Shamans, Software and Spleens. *Law and the Construction of the Information Society*, Cambridge MA, Harvard University Press.

Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles. Available at: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf (Accessed 03 Decemebr 2014).

CEC (1995). Commission of the European Communities, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Official Journal L281/31, 23/11/1995.

CEC (2007). Communication COM (2007) 228 from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs) (not published in the OJC).

Gilbert, N. (2007). Dilemmas of Privacy and Surveillance: Challenges of Technological Change, 2007. Available at: http://epubs.surrey.ac.uk/1573/1/fulltext.pdf (Accessed 03 December 2014).

Hoepman, J.H. (2012). Privacy design strategies, October 2012. eprint arXiv:1210.6621. Available at: http://arxiv.org/pdf/1210.6621.pdf (Accessed 03 December 2014).

Hoepman, J. H. (2014). Privacy Design Strategies, Working paper. Available at http://www.cs.ru.nl/J.H.Hoepman/publications/pdp-sec.pdf (Accessed 03 December 2014).

Hustinx, P. (2009). European Data Protection Supervisor's speech "*Privacy by Design: Delivering the Promises*" held in Madrid during the "Definitive Workshop", 2 November 2009.

International Data Protection and Privacy Commissioners (2010). *Privacy by Design Resolution*. 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, Jerusalem, Israel. Available at http://www.justice.gov.il/NR/rdonlyres /F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf (Last accessed 03/12/2014).

Jacobs, B. (2005). *Select before you Collect*, Ars Aequi, 54, 1006-1009.

Lessig, L. (2006). *Code. Version 2.0*, 2nd Edition, New York:Basic Books.
Office of the Information & Privacy Commissioner of Ontario and Registratiekamer. (1995) Privacy-Enhancing Technologies: The Path to Anonymity (Volume I and II), August. Available at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary /?id=329 (Last accessed 04/12/2014).

Pagallo, U. (2009). *Privacy e Design*, Informatica e diritto, XVIII (1), 123-134.

Pfitzmann, A. and Hansen, M. (2010). *Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology*. Available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (Last accessed 03/12/2014).

Pocs, M. (2012). *Will the European Commission be able to standardise legal technology design without a legal method?*, Computer Law & Security Review, 28, 641-650.

Reidenberg, J.R. (1998). *Lex Informatica: The Formulation of Information Policy Rules through Technology*, Texas Law Review, 76 (3), 553-593.

Simon, H. R., (1996). *The Science of the Artificial*, 3rd Edition, Cambridge, MA:MIT Press.

Spiekermann, S. and Cranor, L. F. (2009). *Engineering Privacy*, IEEE Transactions On Software Engineering, 35 (1), 67-82.

Tavani, H. T. (2010). *Ethics and Technology. Controversies, Question, and Strategies for Ethical Computing*, 3rd edition, John Wiley and Sons.

United Kingdom Information Commissioner's Office (2008). *Privacy by Design*. Available at:http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx (Accessed 03 December 2014).

Warren, S. D. and Brandeis, L. D. (1890). *The Right to Privacy*, Harvard Law Review, 4 (5), 193-220.

References on Rights-in-Design

Arendt A (1958), The Human Condition, Chicago IL, University Of Chicago Press.

Art.29 WP (Article 29 Working Party) (2009), Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

EDPS (European Data Protection Supervisor) (2010). Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). OJ C 280, 16.10.2010, p. 1–15.

EGE, European Group on Ethics in Science and New Technologies. 2014. Opinion 28 of the European Group on Ethics in Science and New Technologies, Ethics of Security and Surveillance Technologies, Brussels, 20 May 2014.

Hildebrandt, Mireille. 2008. “Legal and Technological Normativity: more (and less) than twin sisters.” *TECHNE* 12, 3, 169-183.

Hildebrandt, Mireille and Antoinette Rouvroy (eds). 2011. The Philosophy of Law Meets the Philosophy of Technology. Autonomic Computing and Transformations of Human Agency. London:Routledge.

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., Pereira, Â. G. (2014). Building trust in human-Internet of Things relationship. *IEEE Technology and Society Magazine*, Winter, 73-80.

Kroes N. (2011), Internet essentials, OECD High Level Meeting on the Internet Economy, Paris, 28 June.

Lunshof, J.E., Church, G.M., Prainsack, B. (2014). Raw Personal Data: Providing Access. *Science*. 343 (6169), 373-374.

Pereira, A.G. and Tallacchini, M. (2014). Governance of ICT Security: A Perspective from the JRC, Technical Report, Luxembourg: Publications Office of the European Union.

Tallacchini M., Boucher, P., Nascimento, S. (2014). Emerging ICT for Citizens’ Veillance: Theoretical and Practical Insights, European Commission Policy Report, Publications Office of the European Union: Luxembourg.

Winner, L. (1980). "Do Artifacts Have Politics?" *Daedalus*, 109 (1), Winter 1980, 121-136.

References on wearable sensors and health platforms

Angelsensor (2014). Editorial: The first truly open sensor for health and fitness Available at: http://www.angelsensor.com/. (Accessed 09 August 2014).

AirQualityEgg (2014). Editorial: Air Quality Egg. Available at: http://airqualityegg.com/. (Accessed 20 November 2014).

Article 29 Working Party (2013). Opinion 2/2013 on apps and smart devices. *European Commission*, 27 February 2013. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (Accessed 21 November 2014).

Beddit (2014). Editorial: Beddit Sleep Monitor. Available at: http://www.beddit.com/. (Accessed 20 November 2014).

Bitalino (2014). Editorial: What is BITalino? Is it for you? Available at: http://www.bitalino.com/. (Accessed 21 November 2014).

Bodymedia (2014). Editorial: The Leading on-body monitoring system. Accurate information about your body. Available at: http://www.bodymedia.com/. (Accessed 20 November 2014).

Bragi (2014). Editorial: The Dash, the World's First Wireless Smart In Ear Headphones. Available at: http://www.bragi.com/. (Accessed 09 August 2014).

Comstock, J. (2014). Is Fitbit's opt-out drawing the battle lines against HealthKit? *Mobihealthnews*, 9 October 2014. Available at: http://mobihealthnews.com/37249/is-fitbits-opt-out-drawing-the-battle-lines-against-healthkit/. (Accessed 21 November 2014).

De Montjoye, Y. A., et al. (2013), Unique in the crowd: the privacy bounds of human mobility. *Scientific reports*, 3.

Deterding, S., et al. (2011). From game design elements to gamefulness: defining "gamification". *Proc. of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11)*. New York: ACM, 9-15.

Eblen-Zajjur, A. (2003). A Simple Ballistocardiographic System for a Medical Cardiovascular Physiology Course. *Adv. Physiol. Educ.*, 27 (4): 224–229

Everyaware (2014). Editorial: Sensing Air Pollution. Available at: http://www.everyaware.eu/activities/case-studies/air-quality/. (Accessed 21 November 2014).

EUR-Lex (2012). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011. (Accessed 21 November 2014).

Estrin, D. and Sim, I. (2010). Open mHealth Architecture: An Engine for Health Care Innovation. *Science*, 300 (6005), 759-760

Finley, K. (2014). Nest Who? Here's How to Build Your Own Smart Thermostat. *WIRED*, 21 January 2014. Available at: http://www.wired.com/2014/01/open-source-nest/. (Accessed 20 September 2014).

Fitbit (2014). Editorial: Make fitness a lifestyle with Flex. Available: http://www.fitbit.com/uk/flex. (Accessed 20 November 2014).

Forlani, L. (2014). Wearable devices, IDC: 'pronti al decollo anche in Italia'. *Cor.com,* 11 September 2014 Available at: http://www.corrierecomunicazioni.it/tlc/29666_wearable-device-idc-pronti-al-decollo-anche-in-italia.htm. (Accessed 20 November 2014).

Google Developers (2014). Editorial: Google Fit. Available: https://developers.google.com/fit/overview. (Accessed 20 November 2014).

Hafen, E., Kossmann, D. and Brand, A. (2014). Health data cooperatives – citizen empowerment. *Methods of Information in Medicine*. Stuttgart: Shattauer, 53 (2), 82-86

HON (2010). Editorial: Operational definition of the HON code principles. Available at: http://www.hon.ch/HONcode/Webmasters/Guidelines/guidelines.html. (Accessed 21 November 2014).

IFTTT (2014). Editorial: Put the internet to work for you. Available at : https://ifttt.com. (Accessed: 26 October 2014).

Ioannidis, D., et al. (2012). Gait and Anthropometric Profile Biometrics: A Step Forward. *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras, Eds. The Hague: Springer Netherlands, 105–127

Jawbone (2014). Editorial: The path to better starts here. Available at: https://jawbone.com/up#up24. (Accessed 20 November 2014).

Kellion, L. (2014). Samsung reveals Sami health platform. *BBC News Technology,* 28 May 2015. Available at: http://www.bbc.com/news/technology-27612110. (Accessed 09 August 2014).

Kyriacou, P. A. (2010). Biomedical Sensors: Temperature Sensor Technology. *Biomedical Sensors*, D. Jones, Ed. New York: Momentum Press, 1-38

Kounelis, I. et al. (2014). Building trust in human-Internet of Things relationship. *Technology and Society Magazine*. New York: IEEE, 33 (4).

Lunshof, J. E., Church, G. M. and Prainsack, B. (2014). Raw Personal Data: Providing Access. *Science*, 343 (6169), 373–374

Meyer, L. (2014). Check Your Glucose with a Turn of the Wrist: New Biometric Watches Use Light to Non-Invasively Monitor Vital Signs. *The Optical Society*, 10 June 2014. Available at: http://www.osa.org/en-us/about_osa/newsroom/news_releases/2014/check_your_glucose_with_a_turn_of_the_wrist_new_bi/. (Accessed 03 October 2014).

Mosbergen, D. (2014). How Accurate Is Your Activity Monitor? Fitbit, Jawbone And Others Put To The Test. *The Huffington Post*, 20 June 2014. Available online: http://www.huffingtonpost.com/2014/06/20/activity-monitor-accuracy-fitbit-jawbone_n_5516156.html. (Accessed 21 November 2014)

Mun, M. Y. , et al. (2014). PDVLoc: A Personal Data Vault for Controlled Location Data Sharing. *ACM Transactions on Sensor Networks*. New York: ACM, 10 (4), 1–58

Nike (2014). Editorial: Nike+ Fuelband SE. Activity Tracker & Fitness Monitor. Available at: http://www.nike.com/us/en_us/c/nikeplus-fuelband. (Accessed 09 August 2014).

Nymi (2014). Editorial: Put your heart into it. Available at: http://www.getnymi.com/. (Accessed 20 November 2014).

Nuviun (2014, June 26). Editorial: This Headset That Can Tell If You're Depressed or Eating Too Much. *Digital health*, 26 June 2014. Available at: http://nuviun.com/content/blog/this-headset-can-tell-if-youre-depressed-or-eating-too-much. (Accessed 09 August 2014).

Nuviun (2014, August 7). Editorial: Wearable App Allows ALS Patients To Control Devices With Their Minds. *Digital health,* 7 August 2014. Available at: http://nuviun.com/content/news/wearable-app-allows-als-patients-to-control-devices-with-their-minds. (Accessed 09 August 2014).

Patientslikeme (2014). Editorial: Live better, together! Available at: http://www.patientslikeme.com/. (Accessed 21 November 2014).

Pearson, S. and Mont, M. C. (2011). Sticky Policies: An Approach for Managing Privacy across Multiple Parties. *Computer*, 44 (9), 60–68

Peters, J. (2013). "Development of a low-cost mobile sensor-system for participatory measurements of urban air quality." *First International Workshop on*

New Sensing Technologies and Transducers for Air-Quality Monitoring. Barcelona, 20 June 2013.

Profis, S. (2014). Do wristband heart trackers actually work? A checkup. *CNET*, 22 May 2014 Available at: http://www.cnet.com/news/how-accurate-are-wristband-heart-rate-monitors/. (Accessed 10 August 2014).

Rhodes, M. (2014). Now on Sale: A Wearable Device That Tracks Your Baby. *WIRED*, 08 July 2014. Available at: http://www.wired.com/2014/08/now-on-sale-a-wearable-device-that-tracks-your-baby/. (Accessed: 10 August 2014).

Safeinschool (2013). Editorial: Is Wi-Fi Safe for Children?Beware of Health Risks. Available at: http://www.safeinschool.org/2013_03_01_archive.html. (Accessed 21 November 2014).

Samsung (2014). Editorial: SIMBAND Your Body is Talking to You. Available at: http://www.samsung.com/us/globalinnovation/innovation_areas/#simband. (Accessed 09 August 2014).

Scott, M. (2014). Novartis Joins With Google to Develop Contact Lens That Monitors Blood Sugar. *The New York Times*, 15 July 2014. Available: http://www.nytimes.com/2014/07/16/business/international/novartis-joins-with-google-to-develop-contact-lens-to-monitor-blood-sugar.html?_r=0. (Accessed 20 November 2014).

SmartCitizen (2014). Editorial: Citizen Science Platform for participatory processes of the people in the cities. Available at: http://smartcitizen.me/. (Accessed 09 August 2014).

Spence, E. (2014). Google Fit vs Apple HealthKit: Developers Get Preview Access To The Next Smartphone Battleground. *Forbes*, 8 July 2014. Available at: http://www.forbes.com/sites/ewanspence/2014/08/07/google-fit-vs-apple-healthkit-

developers-get-preview-access-to-the-next-smartphone-battleground/. (Accessed 27 October 2014).

Spinelle, L., Gerboles, M. and Aleixandre, M. (2014). Report of laboratory and in-situ validation of micro-sensor for monitoring ambient air pollution. JRC Technical Report. Luxembourg: Publications Office of the European Union.

Standards Coordinating Committee of the IEEE Computer Society (1991). IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries *IEEE Std 610*. New York: IEEE, 1–217

Swan, M. (2009). Emerging Patient-Driven Health Care Models: An Examination of Health Social Networks, Consumer Personalized Medicine and Quantified Self-Tracking. *International Journal of Environmental Research and Public Health*, *6*(2), 492–525

Tallacchini, M., Boucher, P. and Figuereido Do Nascimento, S. (2014). Emerging ICT for Citizens' Veillance: Theoretical and Practical Insights. JRC Scientific and Policy Report. Luxembourg: Publications Office of the European Union

Tate, R. (2014). Apple's Upcoming Health App Is the Start of Something Huge. *WIRED*, 17 March 2014. Available at: http://www.wired.com/2014/03/apple-healthbook-is-just-the-beginning/. (Accessed 09 August 2014).

Thalmiclabs (2014). Editorial: Myo Gesture Control Armband. Available at: https://www.thalmic.com/myo/. (Accessed: 09 August 2014).

Tudiabetes (2014). Editorial: A community of people touched by diabetes. Available at: http://www.tudiabetes.org/. (Accessed 21 November 2014).

VitalJacket (2014). Editorial: VitalJacket Products. Available at: http://www.vitaljacket.com/?page_id=156. (Accessed 09 August 2014).

Withings (2014). Editorial: Smart Body Analyser. Available at: http://www.withings.com/it/smart-body-analyzer.html. (Accessed 21 November 2014).

Wright, A. (2014). Data Exploration with Fluxtream/BodyTrack. Quantified Self Europe Conference. Available at: http://vimeo.com/97117884. (Accessed 21 November 2014).

Yadron, D. and Macmillan, D. (2014). Snowden Says Drop Dropbox, Use SpiderOak. *The Wall Street Journal*, 17 July 2014. Available at: http://blogs.wsj.com/digits/2014/07/17/snowden-says-drop-dropbox-use-spideroak/. (Accessed 21 November 2014).

Zephyr (2014). Editorial: BioPatch Wireless Device. Available at: http://zephyranywhere.com/products/biopatch/. (Accessed 20 November 2014).

Annexes

Annex 1. Results of empirical testing of wearable sensors

Manufacturer	Beddit Ltd
Provider	Amazon
Product	Beddit sleep manager
Cost	149 euro
Battery charge	Not applicable (always wired)
Intended user	Adult, Elderly
Category	Complex accessory
Sensor description	Beddit sensor is a bed strip providing sleep measurements from body forces exerted on the bed. Based on physiological measured parameters extracted from the body forces, quality and quantity of sleep is analysed and presented to the user.
Sensor type	Biomechanical
Sensor model	Ballistocardiography
Sensor range	Not observable
Sensor resolution	Not observable
Sensor calibration	Not observable
Sensor output	Sleep pattern
Operating system	iOS, Android
Connection	Bluetooth 4.0
Form factor	Bed strip
Functionality	Beddit sensor is controlled by an application that can be accessed through password authentication on the smartphone. The application semi-automatically launches data collection through start and stop control and needs to be running all night to collect the measurements. Based on the measurements, findings of sleep patterns for duration and cycles are produced and logged in the cloud storage. The sensor accuracy was overall fair as it could track total sleep time night over night. The application also presents findings to the user in the form of sleep patterns, a feedback score on the sleep and advice for sleep improvement (e.g. do not go to bed if you do not feel tired).
Usability criteria	Beddit sensor is a strip laying across the mattress with a sticky tape that fixes to the bed. The strip is very thin so that the user does not feel its presence under the bed sheet. Having to sleep all night with the smartphone active is not comfortable and healthy. The interface presenting the sleep patterns is qualitative and clumsy not providing clear insight on the temporal frames mapping the various types of sleeps
By design safety	Beddit safety recommendations are limited to avoidance of use with babies or children, liquids or wet. More extensible descriptions of

	electromagnetic precautionary conditions and applicable regulations could be relevant for users.
By design security	None
By design privacy	None
In-design customization	None
Openness	Beddit application API is under development providing services for authentication and access of sleep patterns from cloud storage. Accuracy and completeness of the data made available could not be verified due to the qualitative output of sleep patterns presented to the user. On request of multiple users, access to raw data is supposed to be provided at a later stage.
Interoperability	None
Platform	None Potentially Fluxtream
Manufacturer	Jawbone
Provider	Amazon
Product	Jawbone UP
Cost	149,99 Euros
Battery charge	10 days
Intended user	Children, adult, elderly
Category	Complex accessory
Sensor description	Jawbone UP sensor is a rubber wristband that can be worn to track steps, calories burnt and sleep patterns.
Sensor type	Biomechanical
Sensor model	Accelerometer
Sensor range	Not observable
Sensor resolution	Not observable
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Movement, calories burnt, sleep
Operating system	iOS, Android
Connection	USB
Form factor	Bracelet
Functionality	Jawbone UP data is first collected on the sensor and then manually uploaded in the cloud storage. The upload requires the user to insert the sensor in the smartphone, to authenticate with a password to the smartphone application and execute the synchronisation. Manual synchronisation avoids dataset loss. Acquired accelerometer data are processed to produce accurate findings for day and night activity (steps,

	calories burnt, sound/light sleep, awake time). All findings are stored in the cloud online space. Jawbone UP sensor is accurate and does not track steps while you are driving. After extensive inactivity, the wristband vibrates to trigger attention
Usability criteria	Usage instructions are missing from the packaged product; only after seeing the video tutorial on installation it was possible to test the sensor. Once learned how to use it, the wearing is extremely comfortable. Automatic update would be preferable, as interaction requires continuous user actions to switch between day and night mode, as well as checking the charge status.
By design safety	Safety recommendations are very limited and advise on device operation avoiding contact with liquids
By design security	None
By design privacy	None
In-design customization	None
Openness	Jawbone UP application API provides access to sensor findings archived in cloud storage. The data made available are accurate and complete with respect to the accurate values presented to the user.
Interoperability	Jawbone UP application API supports the creation of causality links with other external applications (IFTTT ad-hoc connection protocols). The application cloud storage can be connected with external health services. The connection can support limited control policies to trigger and communicate updates of sensor findings among the related services. A new version was announced to add support for the Apple Healthkit ecosystem and Apple Health app to track and update information on a user's diet and physical activity. This newest application does not require the company's fitness tracker and could work with over a hundred of other apps and devices.
Health platform	Dacadoo, Fluxtream
Manufacturer	Jawbone
Provider	Amazon
Product	BodyMedia link armband
Cost	95 euro
Battery charge	4 days
Intended user	Adult, elderly
Category	Complex accessory
Sensor description	BodyMedia link armband is a weight management system that records, analyses and reports steps, calories burnt and sleep patterns
Sensor type	Bioelectrical and biomechanical
Sensor model	Electrodermal activity, accelerometer, temperature, heat flux
Sensor range	Not observable
Sensor	Not observable

resolution	
Sensor calibration	Not observable
Sensor error	Not observable
Operating system	iOS, Android
Connection	USB, Bluetooth 4.0
Sensor output	Movement, calories burnt, sleep
Form factor	Armband
Functionality	BodyMedia device was not tested as BodyMedia app is available for limited countries (US, Canada, Australia, New Zealand) and requires fee subscription to review the findings from the BodyMedia online space.
Usability criteria	BodyMedia information on availability and local restriction of use should be better advertised to consumers (e.g. sales conditions). BodyMedia armband is not much confortable, as it must be worn tightly on the upper arm.
By design safety	Detailed safety instructions describe the electromagnetic environment of use and recommendations for electromagnetic emissions to which user can be exposed when using the sensor.
By design security	None
By design privacy	None
In-design customization	None
Openness	BodyMedia API, which provided access to user collected data from the cloud, is discontinued and replaced by Jawbone API
Interoperability	None
Health platform	Dacadoo, Fluxtream
Manufacturer	Withings
Provider	Amazon
Product	Blood pressure monitor 801
Cost	135,54 euro
Battery charge	1000 readings
Intended user	Adult, elderly
Category	Complex accessory
Sensor description	Arm cuff worn to measure the blood pressure remotely by a smartphone
Sensor type	Biomechanical
Sensor model	Blood pressure monitor
Sensor range	Blood pressure 0 – 285 mm Hg, heart rate 40 - 180 beats per minute
Sensor resolution	Blood pressure ±3 mmHg or 2%, heart rate 5%
Sensor calibration	Not observable
Sensor error	Not observable

Sensor output	Blood pressure, heart rate
Operating system	iOS, Android
Connection	Bluetooth 4.0
Form factor	Armband
Functionality	Blood pressure monitor is a semi-automatic sensor where data acquisition is controlled by the smartphone Health Mate application. The application is accessed through password authentication and it uploads acquired raw data directly to the cloud storage where the user can review them. The application provides users informative feedback on conditions and reference values.
Usability criteria	The design of the blood pressure remote control could be improved to deal with the situation when the pairing is not successful. Acquired data can get lost during upload and the acquisition needs to be repeated. The buttons to launch the interaction appear only if the pairing is successful, which can be confusing for the user.
By design safety	Safety recommendations advise to avoid using the sensor in the presence of liquids and with children. Further recommendations provide electromagnetic specifications of the environment where the device should be used. It is compliant to the European Directive 93/42/EEC on medical devices and is safety certified in the US (FCC regulations).
By design security	None
By design privacy	None
In-design customization	None
Openness	Health Mate application API enables access to user raw data archived in the cloud storage. Data made available are accurate and complete with respect to the values logged in the cloud online space and presented to the user. All collected raw data can also be emailed to third-parties in CSV format.
Interoperability	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The application cloud storage can be connected with external health services. The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.
Health platform	Dacadoo, potentially Fluxtream, Withings
Manufacturer	Withings
Provider	Amazon
Product	Smart body analyser
Cost	160 euro
Battery charge	More than 1 yr

Intended user	Children, adult, elderly
Category	Complex accessory
Sensor description	Smart body analyser is a scale measuring weight, fat, heart rate, as well as indoor air quality, temperature and connected to Internet for logging the measured values
Sensor type	Bioelectrical and environmental
Sensor model	Weight sensors
Sensor range	Weight 5 – 180 kg, air quality 396 – 2601 CO2 ppm, temperature -10 – 50 °C
Sensor resolution	Weight 90 g
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Weight, fat mass, heart rate, air quality and temperature
Operating system	iOS, Android
Connection	WiFi
Form factor	Smart scale
Functionality	The smart body analyser needs the setup of the Health Mate application for the remote wireless connection. The Health Mate application is the same for blood pressure sensor. The data collection of the smart body analyser is fully automatic. It simply requires the user to step on the smart scale. The scale has the ability to recognize more than one user from different weight and/or body fat % composition. The editing of wrong acquisitions could be a functional improvement for the logging.
Usability criteria	The smart body analyser is a pretty straightforward device not requiring any in-depth learning. Some users might, however, appreciate more information explaining the sensor capabilities and mode of functioning.
By design safety	Safety recommendations report the device is not suitable for people with pacemaker or other internal devices
By design security	None
By design privacy	None
In-design customization	None
Openness	Health Mate application API enables access to a subset of smart body analyser data on weight stored in the cloud. Air quality and temperature are not yet supported, however the data made available are accurate and complete.
Interoperability	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). Customisations could apply to the cloud storage to connect with external health services. The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS

	8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.
Health platform	Dacadoo, Fluxtream, Withings
Manufacturer	Withings
Provider	Amazon
Product	Aura
Cost	295,99 euro
Battery charge	Not applicable
Intended user	Children (above 8 yrs), adult, elderly
Category	Complex accessory
Sensor description	Aura is an active sleep monitor aiding to fall asleep and wake up with light and sound adapted to the sleep status of the user. Sleep patterns are recorded throughout the night.
Sensor type	Biomechanical
Sensor model	Sleep sensor
Sensor range	Not observable
Sensor resolution	Not observable
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Sleep
Operating system	iOS
Connection	Bluetooth 4.0
Form factor	Under-mattress textile
Functionality	Similarly to the previous Withings sensor, Aura sleep manager is paired to the Health Mate application, which is the same. Aura sleep manager automatically measures sleep patterns from data acquired by the sleep sensors. Limited details are provided on the sensor technology. As the user sleeps in bed, the data are uploaded to the smartphone placed nearby and running all night. Aura accuracy seems problematic reporting less than half time in bed per night. It is not clear if the issue may be caused by the thickness of mattress or connection leakages.
Usability criteria	Aura is only available on iOS devices. Interaction with Health Mate application could be better described to explain the sensing set-up (is it really necessary to sleep with a smartphone running?).
By design safety	Aura complies with EU, US, Canadian conformity checks for radiation exposure. It may be used by elderly and children older than 8 yrs.
By design security	None
By design privacy	None
In-design customization	None
Openness	Health Mate API enables access to findings processed on sleep patterns

	and stored in the cloud online space
Interoperability	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The cloud storage can be connected with external health services. The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.
Health platform	Dacadoo, potentially Fluxtream, Withings
Manufacturer	Biodevices SA
Provider	Biodevices SA
Product	VitalJacket
Cost	990 euro
Battery charge	3 days
Intended user	Adult
Category	Complex accessory
Sensor description	Vitaljacket is a t-shirt and heart monitor
Sensor type	bioelectrical
Sensor model	ECG monitor, accelerometer
Sensor range	0 – 30 mV
Sensor resolution	5%
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Electrical activity of the heart (ECG), movement
Operating system	Android
Connection	USB, Bluetooth 2.1
Form factor	T-shirt with leads
Functionality	Vitaljacket data collection is fully manual. Data are recorded in a secure digital card and transferred to a standalone desktop application to view ECG graphs. Potentially it can evolve towards semi-automatic support and connection to mobile smartphones
Usability criteria	Vitaljaket requires effort to place the ECG leads in the correct part of the body. For this task, there are good illustrations both in the instructions and on the t-shirt, however the task is a bit tedious. Other types of textile electrodes could be envisaged for improving user-friendliness
By design safety	Vitaljacket is compliant to the European Directive 93/42/EEC on medical devices.
By design security	None

By design privacy	None
In-design customization	None Potentially, a data collection application could be developed with support of own in-design customisations
Openness	Acquired ECG data can be accessed and visualised in a proprietary viewer provided by the manufacturer. As the data are made available in proprietary format, they cannot be processed. A suggested improvement would be to use open or standard data format, like open ECG, DICOM.
Interoperability	None
Health platform	Potentially Fluxtream
Manufacturer	Zephyr
Provider	Zephyr
Product	Bioharness 3
Cost	690 euro
Battery charge	2 days
Intended user	Adult
Category	Complex accessory
Sensor description	Bioharness 3 is a chest band with a sensor to measure heart and breathing rate
Sensor type	Biomechanical
Sensor model	accelerometer
Sensor range	Heart rate: 0 – 240 bpm breathing rate: 0 – 120 bpm
Sensor resolution	Heart rate: 1 bpm breathing rate: 1 bpm
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Heart rate, breathing rate
Operating system	Android
Connection	Bluetooth 2.1
Form factor	Chest band and biopatch
Functionality	Bioharness sensor semi-automatically monitors heart and breathing rate while it is worn. Monitored values are sent to the Zephyr Life smartphone application, which can be accessed through password authentication for viewing the readings. Zephyr Life does not support remote data collection, which is only available in a desktop proprietary application used to monitor a group of users or patients.
Usability criteria	In addition to the chestband, the sensor is also available as a biopatch, which is more comfortable to wear. However, although the biopatch is widely advertised online, it is not ensured to properly function.
By design safety	Bioharness safety instruction for electromagnetic compatibility are generic and only available online. They describe the risk of interference with or from other radio transmitting or medical electrical equipment in

	close proximity.
By design security	None
By design privacy	None
In-design customization	None Potentially, a data collection application could be developed with support of own in-design customisations
Openness	Bioharness sensor API is available to developers intending to build own data collection environments and application APIs
Interoperability	None
Health platform	Potentially Fluxtream
Manufacturer	Fab Lab Barcelona
Provider	Fab Lab Barcelona
Product	Smart Citizen Kit
Cost	155 euro
Battery charge	2 days, renewable energy is also provided
Intended user	Children, adult, elderly
Category	Complex accessory
Sensor description	The Smart Citizen kit provides a set of sensors for realtime and independent monitoring of environmental health
Sensor type	Environmental and electrical
Sensor model	Humidity sensor, temperature sensor, microphone, light dependent resistor, gas sensors
Sensor range	Humidity: 0 – 100%, temperature: -40 – 80 °C, CO: 1 – 1000 ppm, NO2: 0.05 – 5 ppm
Sensor resolution	Humidity: 5%, temperature: 0.5 °C
Sensor calibration	Not observable
Sensor error	Not observable
Sensor output	Temperature, humidity, light, noise, CO and NO2 emissions
Operating system	iOS
Connection	WiFi
Form factor	Box kit
Functionality	The Smart Citizen sensor requires initial configuration of the kit communication channels and online application account. Once the sensor is configured, sensor data are automatically collected and publicly published online.
Usability criteria	Once set-up and configured, the Smart Citizen kit runs by itself and the sensor uploads the measured values in the cloud storage. Information provided with the kit and on the website is extremely detailed. One point that could be improved is the provision of calibrated conversions for gas-monitored values. The values are published as resistance output

	and can only be transformed qualitatively into gas concentrations.
By design safety	The Smart Citizen kit has no electrical hazards
By design security	None
By design privacy	None
In-design customization	None
Openness	Smart Citizen kit API supports the querying of sensor data from the remotely archive in the Barcelona Fab Lab cloud server. The data made available are accurate and complete. The Smart Citizen sensor is fully transparent as all information on the components and software are available online for reproducibility. It is also participatory organised in a community of citizens with an active forum answering requests relating to technical issues and suggestions for improvements.
Interoperability	None
Health platform	Potentially Fluxtream

Annex 2. Results of empirical testing of digital health platforms

Owner	Dacadoo AG
Platform	Dacadoo
Cost	4.99 Euro monthly fee
Intended user	Children (above 11 yrs), adult, elderly
Platform description	System used to track and benchmark health and well-being scores facilitating behavioral change through evaluation of body, feelings and daily lifestyle components such as physical activity (exercise and daily steps), nutrition, stress and sleep.
Category	Commercial software
Integrated applications	Dacadoo integrates sensing applications from BodyMedia, Fitbit, Jawbone, Runkeeper, Suunto, Vitadock, Withings to feed sensor data into the platform Integration with Facebook and Twitter social network allows to send notification of events and achievements to the social network community
Functionality	Dacadoo acquires sensor data from connected services to determine an individual health score based on collected data and filled in questionaires. Processing services provide expert coaching and planning of healthy activities towards goal achievement both individually and in teams, although the coaching is not supported by background sensing information. Information at community level is only provided to third parties and not to the individuals. The presentation partially supports visualisation of past sensor measurements in sensor by sensor follow-up graphs. Limited information relating to event notifications can be shared on connected social networks.
Usability criteria	As the system is aimed at providing a holistic overview of the health status of a person, the interface presents a lot of information on questionnaires, activities and notifications making the user feel lost in the different screens. It is also difficult to perceive insight on general health status resulting from contributions of the different activities performed and information provided.
By design security	User data are stored encrypted in the platform data centre protected by a security firewall. Data presented to the user are also transferred through secured communication channels
By design privacy	Privacy settings allow setting the profile for sharing of the status information (health score, completion of proposed goals, etc.) and event notifications relating to performed activities. The settings are private, shared with friend only, public
In-design customization	None
Openness	None
Interoperability	Interoperability is supported as interconnection to get input from

	third-party applications and provide notifications to partnering social networks
Owner	Flutream.com
Platform	Fluxtream
Cost	Free
Intended user	Adult, elderly
Platform description	Fluxtream is a data visualization service aimed at the quantified self community, tracking personal sensor, calendar, and geodata.
Category	Opensource software
Integrated applications	Sensing applications from BodyMedia, Fitbit, Jawbone, Runkeeper, Moves, Zeo, Withings MyMee, QuantifiedMind can feed data to the platform Integration with Flickr, SMS Backup, Last.fm and Twitter allows to collect recording of events and complementary information generated interacting with the phone.
Functionality	Fluxtream is a personal visualisation tool for tracking daily habits, identifying strengths and weaknesses, and getting a comprehensive view on your self-tracking devices and the services used for self-monitoring. Synchronisation of connected devices is manual. Unlike many devices and systems that provide fragmented visions, the system aggregates and recombines multiple data sources to generate summaries and update correlations, which have not thought of. The diverse data streams are plotted on a common timeline and visited locations are visualized on a map. Collected findings are stored in the cloud online space and can be shared with community friends. Fluxtream also allows to export all findings in CSV files.
Usability criteria	The user interface of Fluxtream is cluttered and oriented for scientific users. Analysis and interpretation of collected data are limited to simple presentations based on minimal interpretation, such as extremely low-level data views or long historical event streams. This places the burden of synthesis on the self-tracker.
By design security	Data presented to the user are also transferred through secured communication channels
By design privacy	Information can either be private or shared with community friends
In-design customization	None
Openness	Fluxtream application API provide calls to the main services supported (authentication, data sharing, data retrieval, export, import and timeline related operations)
Interoperability	Fluxtream application API supports the integration with other external health applications.
Owner	Withings

Platform	Health Mate
Cost	free
Intended user	Children, adult, elderly
Platform description	System allows to track health and wellness providing a real-time coaching.
Category	Commercial software
Integrated applications	Sensing applications from BodyMedia, MyFitnessPal, Nike+, RunKeeper, Withings.
Functionality	Health mate provides logging services to store history of health data and improve behaviour over time. Data can be logged manually or automatically with tracking devices. The system allows setting achievable goals, and send reminders to focus user efforts. In addition to setting goals to overcome, the software suggests tips to move more or better sleep. A trophy system and rankings with friends will motivate the user to follow advice.
Usability criteria	The user interface is airy and visual, easing the access to the most important functions at the top of the screen, which is useful for scanning a glance its activity, weight, or air quality at home. The patterns are visualized in separate timelines making it difficult to make correlations and discover trends
By design security	Data presented to the user are also transferred through secured communication channels
By design privacy	Information can either be private or shared with community friends
In-design customization	None
Openness	Health Mate application API enables access to user raw data archived in the cloud storage. Some collected raw data can also be emailed to third-parties in CSV format.
Interoperability	Health Mate application API enables the creation of causality links with external applications (IFTTT ad-hoc connection protocols). The application cloud storage can be connected with external health services. The connection can support limited control policies to trigger and communicate updates of sensor information among the related services. On smartphones and IPADs running the iOS 8, the application was announced to get integrated with the new Apple HealthKit development ecosystem and Health app.

European Commission
EUR 27045 EN – Joint Research Centre – Institute for Security and Protection of the Citizen

Title: Wearable Sensors and Digital Platforms in Health: empowering citizens through trusted and trustworthy ICT technology

Authors: Monica Gemo, Davide Lunardi, Mariachiara Tallacchini

Luxembourg: Publications Office of the European Union

2015 – 100 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series –ISSN 1831-9424

ISBN 978-92-79-44733-4

doi:10.2788/788525

Abstract

Personal wearable sensors have the potential to become the most powerful individuall self-surveillance technology available to citizens. These ubiquitous, networked devices currently offer a breadth of capabilities to sense, digitally enhance and upload data of fine granularity such as body and health measurements, images, location, sound and motion.
However, for wider adoption, it is crucial for citizens/end-users to rely on trusted and trustworthy implementations of wearable sensing technologies. Trusted systems are defined as systems functioning normally and delivering what it is promised and what the user expects, whereas trustworthiness is mostly objectively defined according to specific criteria and can be considered a metric for how much a system deserves the trust of its users. Therefore, in order to establish criteria for trust and trustworthiness, the present report aims to screen and analyse emerging solutions and architectures for verifying that functionalities, motivations and values embedded in their design hold the potential for user empowerment, equitable use and meaningful community participation in digital health platforms. As a whole, the report provides a characterization of emerging wearable sensors and digital platforms for health activities according to identified criteria for trust and trustworthiness. These criteria specifically encompass certain normative features, embedded in the systems and aimed at providing citizens/users with powers of control and choice over the devices. Beside increasing citizens/users' trust, these normative measures—specifically by-design and in design forms of rights protection) also allow to improve agency, namely citizens/users' ability to autonomously control the system. The report offers a detailed analysis of some wearable sensors and platforms providing some recommendations to improve their degree of trust and trustworthiness.

LB-NA-27045-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/788525

ISBN 978-92-79-44733-4