PROCEEDINGS OF THE THIRTEENTH INTERNATIONAL CONFERENCE

The possibilities of ethical ICT

ETHICOMP 2013*

University of Southern Denmark, Kolding Campus, Denmark
12 to 14 June 2013

EDITED BY

TERRELL WARD BYNUM
WILLIAM FLEISHMAN
ANNE GERDES
GITTE MØLDRUP NIELSEN
SIMON ROGERSON









University of Southern Denmark
De Montfort University
Southern Connecticut State University
East Tennessee State University

*** ETHICOMP** is a trademark of De Montfort University

Title	The possibilities of ethical ICT
Edited by	Terrell Ward Bynum, William Fleishman, Anne Gerdes, Gitte Møldrup Nielsen and Simon Rogerson
ISBN	978-87-92646-72-9
Local	Kolding, UK
Date	2013
Publisher	Print & Sign University of Southern Denmark

Copyright © 2013
collection of papers as proceedings –University of Sothern Denmark
individual papers – authors of the papers

Papers could subsequently appear in the ETHICOMP electronic journal

No responsibility is accepted for the accuracy of the information contained in the text or illustrations. The opinions expressed in the papers are not necessarily those of the editors or the publisher

CONFERENCE DIRECTORS

Terrell Ward Bynum, Southern Connecticut State University, USA

Anne Gerdes University of Southern Denmark, Denmark

William Fleischman Villanova University, USA

Gitte Møldrup Nielsen, it-vest, networking universities, Denmark

Simon Rogerson, De Montfort University, UK

PROGRAMME COMMITTEE

Alison Adam, Sheffield University, UK
Mario Arias-Oliva, University of Rovira and Virgili, Spain
Andrew Bissett, Sheffield Hallam University, UK
Terrell Ward Bynum, Southern Connecticut State University, USA
Göran Collste, Linköping University, Sweden
Penny Duquenoy, Middlesex University, UK
N Ben Fairweather, De Montfort University, UK
William Fleischman, Villanova University, USA
Anne Gerdes, University of Southern Denmark, Denmark
Krystyna Gorniak-Kocikowska, Southern Connecticut State University, USA
Donald Gotterbarn, East Tennessee State University, USA
Fran Grodzinsky, Sacred Heart University, USA
David Sanford Horner, University of Brighton, UK
Jeroen van den Hoven, Delft University of Technology, The Netherlands
Chuck Huff, St Olaf College, USA
Suzy Jagger, Roehampton University, UK
Thessa Jensen, University of Aalborg, Denmark
Iordanis Kavathatzopoulos, Uppsala University, Sweden
Shalini Kesar, Southern Utah University, USA
Kai Kimppa, University of Turku, Finland
Paul B. de Laat, Rijksuniversiteit Groningen, The Netherlands
Peter Lauritsen, University of Aarhus, Denmark
Antonio Marturano, Sacred Heart Catholic University of Rome, Italy
Keith Miller, University of Illinois at Springfield, USA
Kiyoshi Murata, Meiji University, Japan
Peter Øhrstrøm, University of Aalborg, Denmark
Ugo Pagallo, University of Turin, Italy
Nancy Pouloudi, Athens University of Economics & Business, Greece
Simon Rogerson, De Montfort University, UK
Bernd Stahl, De Montfort University, UK
Stanislaw Szejko, Polish-Japanese Institute of Information Technology, Poland
Teresa Torres Coronas, University of Rovira and Virgili, Spain
Richard Volkman, Southern Connecticut State University, USA
John Weckert, Charles Sturt University, Australia

ADMINISTRATION

Niels Hassø Andersen, University of Southern Denmark, Denmark
Hanne Pihl Bjerre, University of Southern Denmark, Denmark
Søren Borgstrøm, University of Southern Denmark, Denmark
Elsebeth Krogh Frausing, Udvikling Fyn A/S, Denmark
Rune Nørgaard Jørgensen, University of Southern Denmark, Denmark
Pernille Dahl Kragh, University of Southern Denmark, Denmark
Nadja Froda Skriver Kristiansen, University of Southern Denmark, Denmark
Christian Behrendt Juulsen Hansen, University of Southern Denmark, Denmark
Ann Rithaphorn, University of Southern Denmark, Denmark
Kirsten Rudbeck, Udvikling Fyn A/S, Denmark

SUPPORTED BY

Emerald Group Publishing Limited

Institute for the Management of Information Systems (IMIS)

International Society for Ethics and Information Technology (INSEIT)

University of Southern Denmark

The Danish Council for Independent Research, Humanities

KEYNOTE ADDRESSES

Android Ethics
by
Henrik Scharfe
Professor of Information Science
Aalborg University, Denmark

The Death of Big Brother - Surveillance as an Accomplishment
by
Peter Lauritsen
Associate Professor
Aarhus University, Denmark

From Ethics of the Eye to Ethics of the Hand: Outline of a Paradigm Change from Hermeneutics to Phenomenology in the Discourse of Ethics and ICT
by
Ellen Christiansen
Professor in Participatory Design.
Aalborg University, Denmark

TABLE OF CONTENTS

INTRODUCTION 1
Simon Rogerson
KEYNOTE ADDRESSES 5
ANDROID ETHICS
Henrik Scharfe
THE DEATH OF BIG BROTHER - SURVEILLANCE AS AN ACCOMPLISHMENT
Peter Lauritsen
FROM ETHICS OF THE EYE TO ETHICS OF THE HAND: OUTLINE OF A PARADIGM CHANGE FROM HERMENEUTICS TO PHENOMENOLOGY IN THE DISCOURSE OF ETHICS AND ICT
Ellen Christiansen
THE CHALLENGES OF DIGITAL EDUCATION IN THE INFORMATION AGE 6
A. A. Adams
A FRAMEWORK FOR ELECTRONIC BUSINESS ETHICS: A COMPARISON STUDY BETWEEN THE UK AND EGYPT 14
Gomaa Agag and Ibrahim Elbeltagi
ELEARING EVOLUTION: NEW CONCEPTS ON ICT & LEARNING 25
Mario Arias-Oliva and Juan Carlos Yáñez-Luna
DESIGNING "OPEN EDUCATION": HOW DOES THE ICT-BASED SYSTEM FUNCTION AS A NEW MEDIUM OF PARTICIPATION FOR SUSTAINABILITY? 33
Ryoko Asai
ICT SUPPORTED CRISIS COMMUNICATION AND DIALOG 37
Ryoko Asai and Iordanis Kavathatzopoulos
HOW TO RESPECT PRIVACY OF ENERGY CONSUMERS WHILE IMPLEMENTING SMART METERING SYSTEMS 42
Barbara Begier
BIOMETRIC AUTHENTICATION PRACTICES:IDENTITY AS CONVENTION 50
Maren Behrensen
VALUE-BASED DESIGN – AN APPROPRIATE STRATEGY FOR DEVELOPING NEW TECHNOLOGIES 60
Hanne Pihl Bjerre
AN EMPIRICAL RESEARCH DESIGN FOR ANALYZING INFORMATION DIVERSITY IN TWITTER FOR DUTCH AND TURKISH USERS 65
Engin Bozdag and Qi Gao
TOWARDS A GOOD INFORMATION AND COMMUNICATION SOCIETY: BUILDING A TREE OF ACTIONS 73
Gunilla Bradley and Diane Whitehouse
A STATUS REPORT ON DANISH E-GOVERNMENT 76
Christian Bruhn
ON THE ROLE OF ETHICS IN PERSUASIVE DESIGN 85
Sandra Burri Gram-Hansen and Lasse Burri Gram-Hansen
FACING FACISM, UNIQUE BIOMETRIC IDENTIFIERS AND DATA TOTALITARIANISM: SOCIO-TECHNICAL CONSIDERATIONS 92
Alberto Cammozzo
IS/IT ETHICAL ISSUES AS A CORPORATE SOCIAL RESPONSIBILITY: REVISITING STRATEGIC BUSINESS PLANNING UNDER THE LENS OF IS/IT ETHICAL PREOCCUPATIONS 100
Anne Chartier and Bernard Plante
MORAL REASONING IN E-LEARNING GENERATIONS: FROM 1.0 TO 4.0 110
Gonçalo Jorge Morais Costa, Nuno Sotero Alves Silva and Tiago Filipe Rodrigues Fonseca
DEVELOPING ROBUST CAD CURRICULUM BY APPLYING BLENDED LEARNING ENVIRONMENT AND TECHNOLOGY 118
Richard Cozzens

INFORMAL COMMUNICATIVE PRACTICES IN FORMAL SETTINGS: FACEBOOK AS MEDIATOR BETWEEN CONTEXTS 128
Nina Bonderup Dohn and Niels Bonderup Dohn
APPLICATION OF FLORIDI'S INFORMATION ETHICS MODEL IN HIGHER EDUCATION: IMPROVING INFORMATIONAL ABILITIES IN A FIRST YEAR EXPERIENCE CLASS 135
Marsha Driscoll and Tammy Bobrowsky
ETHICOMP IN LATIN AMERICA 142
William M. Fleischman
TOR AND THE DARKNET: RESEARCHING THE WORLD OF HIDDEN SERVICES 150
Catherine Flick and Runa A. Sandvik
"SURGERIOUS TWEEZERS": EXPLORING DOCTORS' PERCEPTION! 157
Tiago Filipe Rodrigues Fonseca, Gonçalo Jorge Morais Costa and Nuno Sotero Alves Silva
PRELIMINARY REFLECTIONS ON A MORAL TURING TEST 167
Anne Gerdes and Peter Øhrstrøm
POWER ETHICS: THE MASSIVE DATA CENTER 175
David Gleason
A NEW FRONTIER IN ICT ETHICS: ROBOTIC CAREGIVERS 177
Krystyna Górniak-Kocikowska
SOCIAL AND COMMUNICATION CHALLENGES FOR AGILE SOFTWARE TEAMS 186
Peggy Gregory and Katie Taylor
HELLO "SMARTER" WEB MARKETING, GOODBYE SOCIAL DISCRIMINATION. REALLY? 192
Frances S. Grodzinsky, Andra Gumbus and Stephen Lilley
AUTOMATED DECEPTIONS, BENEVOLENT AND OTHERWISE 199
Frances Grodzinsky, Keith Miller and Marty J. Wolf
INFORMATION WARFARE - ARE WE ALREADY AT WAR? 207
Olli I. Heimo and Kai K. Kimppa
RESPONSIBILITY IN ACQUIRING CRITICAL GOVERNMENTAL INFORMATION SYSTEMS: WHOSE FAULT IS FAILURE? 213
Olli I. Heimo, Jani S. S. Koskinen and Kai K. Kimppa
COMPUTING FUTURES: MIRACLES, PROPHECY AND PREDICTION 218
David Sanford Horner
ETHICAL ASSESSMENT OF GUARDIAN ANGELS TECHNOLOGY SCENARIOS 224
Veikko Ikonen, Eija Kaasinen, Päivi Heikkilä, Barbara Simpson and Andrea Leu
A MULTIMEDIA LEARNING TOOL TO DEVELOP ETHICAL AWARENESS 235
Suzy Jagger
THE ETHICS OF USER EXPERIENCE DESIGN DISCUSSED BY THE TERMS OF APATHY, SYMPATHY, AND EMPATHY 242
Thessa Jensen and Peter Vistisen
A DISCUSSION OF ETHICS IN WEB BASED KNOWLEDGE MANAGEMENT 247
Jesper Jensen
CURBING THE RHETORIC: HOW WEB 2.0 FURTHER OBFUSCATES THE LEGAL LIMITS OF PROHIBITED SPEECH 253
Ville Kainu and Toni Värttö
DEVELOPING THE NEXT GENERATION OF IT PROFESSIONALS – ENGAGING IT STUDENTS IN THE PRACTICE OF IT PROFESSIONAL ETHICS 261
Terence N Keefe and Lynn Cinderey
RETHINKING EDUCATION: STEM BECOMES A STEAM PROJECT 268
Shalini Kesar
USING TRIPLE LOOP LEARNING IN CONTEXT OF MANAGEMENT OF INFORMATION SYSTEMS SECURITY 274
Shalini Kesar
FROM SEAFARING PROFESSIONALS TO IT PROFESSIONALS 281
Kai Kimppa and Norberto Patrignani
PROBLEMS IN THE USE OF PERSONAL INFORMATION FROM THE POINT OF VIEW OF RELATIONSHIP MARKETING 282
Hiroshi Koga

MISSED CHANCES AND WRONG CHOICES IN PATIENT INFORMATION? AN ETHICAL EVALUATION OF THE FINNISH IMPLEMENTATION OF THE EU DATABASE DIRECTIVE 288
Jani Koskinen and Ville Kainu
DEMOCRACY, HUMAN FALLIBILITY, AND ICT 295
Mikael Laaksoharju and Iordanis Kavathatzopoulos
HOW INFORMATION TECHNOLOGY IN SCHOOL INFLUENCES THE STUDENTS' DEMOCRATIC COMPREHENSION 302
Else Lauridsen
MARKETING THE INFORMATION SOCIETY: SUSTAINABILITY, SPEED AND TECHNOMASS 310
Thomas Taro Lennerfors
ETHICAL DELAY IN EMERGING ICT 316
Richard Lucas
USING WIKI TECHNOLOGY IN THE CLASSROOM 324
Gunver Majgaard
CO-OPERATION AND ETHICAL PROBLEMS IN SOFTWARE INDUSTRIES: THE CASES OF VIETNAM AND NEPAL 331
Michiko Matsushita
PRIVACY, RISK AND PERSONAL HEALTH MONITORING 340
Brent Mittelstadt, N. Ben Fairweather, Neil McBride and Mark Shaw
ETHICAL CONCERNS IN USABILITY TESTING INVOLVING OLDER ADULTS 352
Margrethe H. Møller 352
FUTURE TECHNOLOGIES: AN ETHICAL PERSPECTIVE ON THE DRIVE FOR INNOVATION AND THE INTERNET OF THINGS 360
Denise Oram
E-GOVERNANCE RISK IN JAPAN: EXACERBATION OF DISCRIMINATIVE STRUCTURE BUILT IN THE FAMILY REGISTRATION SYSTEM 362
Yohko Orito, Kiyoshi Murata and Chung Ah Young
SURVEILLANCE-BASED MIGRATION CONTROL AND A SUBSTANTIAL FREEDOM OF MOVEMENT 371
Elin Palm
THE BRAVE NEW WORLD OF SOCIO-TECHNICAL SYSTEMS: CLOUD COMPUTING 377
Norberto Patrignani and Iordanis Kavathatzopoulos
SLOW TECH: TOWARDS GOOD, CLEAN AND FAIR ICT 384
Norberto Patrignani and Diane Whitehouse
HOW TO DESIGN SOFTWARE TAILORED TO THE STAKEHOLDERS' NEEDS? 391
Małgorzata A. Płotka, Donald. Gotterbarn, N. Ben Fairweather and Sara H. Wilford
WORKING ETHICALLY IN PARTICIPATORY RESEARCH WITH CHILDREN 400
Janet C. Read, Peggy Gregory, Gavin Sim and Matthew Horton
DIGITAL DISABILITY DIVIDE IN INFORMATION SOCIETY: THE CASE OF IMPAIRMENTS 405
Neeraj Sachdeva, Anne-Marie Tuikka and Reima Suomi
APPLYING CONTEXTUAL INTEGRITY TO THE CONTEXT OF SOCIAL NETWORKING SITES TRACKING 413
Rath Kanha Sar and Yeslam Al-Saggaf
NEW TECHNOLOGIES AND OLD CULTURES: HOW ICT IS SHAPING AND GETTING SHAPED BY THE INDIAN SOCIETY? 419
Raghubir Sharan , Mahesh Mehendale and Abhay Karandikar
COMPUTER GAMES IN EDUCATION: CONFLICTS AND OVERLAPS! 425
Nuno Sotero Alves da Silva, Gonçalo Jorge Morais da Costa, Piotr Pawlak and Tiago Filipe Rodrigues da Fonseca
EVALUATING RESEARCH QUALITY IN TECHNOLOGY ETHICS 435
Bernd Carsten Stahl, Catherine Flick and Richard Hall
TO MAKE SODIS CLOSER TO THE PROJECT MANAGEMENT PROCESS 441
Stan Szejko and Sara Wilford
TO BEAR THE UNBEARABLE: COLLEGE-LEVEL INFORMATION ETHICS EDUCATION INCORPORATING DISCUSSIONS OF ETHICAL DILEMMAS 450
Takeo Tatsumi, Yoshiaki Nakano, Noriaki Kusumoto, Joji Maeno and Yasunari Harada

RESPONSIBLE RESEARCH AND INNOVATION A TECHNOLOGICAL FIX? A CRITICAL REVIEW OF MOTIVATIONS BEHIND RRI. 457
Job Timmermans
ON THE GLOCALIZED NETIZEN 465
Jin Tong
DIGITAL COMPETENCES AND ENTREPRENEURIAL SELF-EFFICACY AMONG GRADUATE STUDENTS 470
Teresa Torres-Coronas, María-Arántzazu Vidal-Blasco, Mario Arias-Oliva, and Ricard Monclús-Guitart,
CHALLENGES IN ENTERING APPLICATION MARKETS AMONG SOFTWARE PRODUCERS IN DEVELOPING COUNTRIES 478
Anne-Marie Tuikka, Sami Hyrynsalmi, Kai K. Kimppa and Arho Suominen
TRANSPARENCY AS A CORE VALUE IN GOOGLE SEARCH 488
Katrine Juel Vang
ETHICAL IMPLICATIONS OF GOOGLE'S KNOWLEDGE GRAPH 490
Katrine Juel Vang
HOW TO RESIST THE HYPERMORALIST TEMPTATION IN COMPUTER ETHICS 496
Richard Volkman
PRIVACY, THE THEORY OF COMMUNICATIVE ACTION AND TECHNOLOGY 502
Kirsten Wahlstrom and N Ben Fairweather
AUSTRALIA AND DATA RETENTION 511
Matthew J. Warren and Shona Leitch
PRINTABLE GUNS IS AN IDEA WHOSE TIME HAS COME 518
Danny Weston and Catherine Flick
MATURITY, ETHICS AND THE IS PROFESSIONAL (DOES AGE MATTER WHEN IT COMES TO ETHICAL ISSUE AWARENESS?) 524
Sara H. Wilford and Kutoma Wakunuma
AN ANALYSIS OF HIGHER EDUCATION USING FLORIDI'S INFORMATION ETHICS 531
Marty J. Wolf, Colleen Greer, Marsha Driscoll, Siri Anderson and Tammy Bobrowsky
LEARNING COMPUTER ETHICS AND SOCIAL RESPONSIBILITY WITH TABLETOP ROLE-PLAYING GAMES 539
Katerina Zdravkova
INDEX OF AUTHORS 548

PRIVACY, RISK AND PERSONAL HEALTH MONITORING

Brent Mittelstadt, N. Ben Fairweather, Neil McBride and Mark Shaw

Abstract

Personal health monitoring (PHM) systems capable of gathering pervasive physiological and behavioural data are currently in development to supplement existing medical resources. As a technology designed to operate in the private sphere, PHM can digitise, record and analyse the lives of patients, creating opportunities for data sharing, mining and social categorisation. Medical care and health outcomes may be improved through increasingly granular monitoring and personalised interventions, but these outcomes may come at the cost of user privacy and related ethical implications. As an emerging technology, the opportunity remains to proactively respond to the potential normative risks of a PHM-enabled future. In this paper, a critical overview of the treatment of privacy, risk and PHM in academic literature is offered. The current discourse is defined by a conceptually narrow definition of privacy among developers of PHM systems and security architecture, which suggests that emerging PHM systems may fail to meet the context-specific privacy expectations of users.

Keywords

ethics, privacy, risk, security, trust, personal health monitoring, PHM, pervasive health, wearable health, health surveillance, smart home, literature review

1. Introduction

Personal health monitoring (PHM) systems are being developed to supplement medical care with health monitoring outside traditional care environments such as hospitals. The primary factors spurring the development of PHM are the benefits for patients associated with health monitoring at home (c.f. Neild et al., 2004; Ure et al., 2012), and the need to supplement existing medical resources to address the needs of an aging population (Agree et al., 2005; Remmers, 2010; Sadri, 2011; Stuart et al., 2008). Systems are being developed for a range of demographics, with many targeting the elderly and chronically ill.

PHM refers to any electronic device or system that monitors and records data about a health-related aspect of a person's life outside a hospital setting. To qualify as PHM a device must be capable of transferring data to a third party, and be usable by a layperson outside a traditional medical environment such as a hospital. Examples include smart home systems (Demiris and Hensel, 2009) and physiology-sensing 'smart clothes' (Lymberis, 2005). Emerging PHM applications cover a range of tasks within healthcare and public health monitoring, including prevention, treatment, assistance and rehabilitation, as well as occupational and recreational health monitoring (PHM Ethics Consortium, 2012a). Within these areas PHM applications have a range of purposes including longitudinal data monitoring, pattern recognition and diagnosis, lifestyle feedback, and anomaly and emergency detection (PHM Ethics Consortium, 2012b).

PHM is designed to operate within the private sphere. Devices can be carried with the user or installed in private environments, such as the home, creating a public window into private life. The lives of users can be digitised, recorded and analysed by third parties, creating opportunities for data sharing, mining and social categorisation (c.f. Lyon, 2003). These basic functions may improve healthcare through increasingly granular monitoring and personalised interventions, yet they simultaneously create an opportunity for violating user expectations of privacy and related risks. As an emerging technology, the opportunity remains to proactively respond to the potential risks of a PHM-enabled future. However, anticipatory action requires understanding the normative potential of PHM (Kastenhofer, 2011) according to developers, regulators, academics and potential users. To this end, a critical assessment of current academic literature discussing privacy, risk and PHM was

conducted. Gaps in the discussion and conceptual deficiencies were identified, which revealed areas in need of acknowledgement in the development and governance of PHM.

2. Methods

Peer-reviewed articles, reviews and conference proceedings available in four databases (Scopus, IEEE, MEDLINE, and ISI Web of Knowledge) addressing privacy or risk and PHM were reviewed between May and September 2012. The search was without date restrictions, but limited to English language sources.

2.1 Procedure

Sources were located through systematic searching of the databases as well as hand searching and reference tracking. Multiple search techniques were used to ensure comprehensiveness. Recognising 'personal health monitoring' is an emerging term not yet widely used in the literature (Mittelstadt et al., 2011), synonymous and related search terms were used including 'somatic surveillance', 'wearable body sensors', 'pervasive health', 'assistive technologies', 'ambient intelligence', 'health surveillance', 'ambient assisted living', and 'smart home'. All sources were checked to ensure the technology under discussion matched the working definition of PHM, and that a discussion of privacy issues or risks was included.

2.2 Justification

PHM applications often share technological characteristics with ambient intelligence (AmI) and ubiquitous computing (ubicomp) (Bohn et al., 2005). The search technique was designed to limit the results to health applications. It is recognised that privacy issues and risks of non-medical applications of AmI and ubicomp may be relevant to PHM.[1]

The search method was chosen to identify articles explicitly addressing privacy issues and risks of PHM. The results expanded upon a prior literature review of ethical implications of PHM (Mittelstadt et al., 2011), in which privacy was identified as a major theme. Given the frequency with which privacy appears in discussions of ethics of PHM, it was deemed appropriate to conduct a separate review to develop a fuller understanding of its meaning and usage within discourse on PHM. 'Risk' was also added to the search terminology on the basis of criticisms at ETHICOMP 2011 of the prior review, which suggested normative dimensions of emerging technologies are often discussed in terms of 'risk', and evaluated through 'risk assessments', without any mention of ethics.

2.3 Data Analysis

All articles underwent content analysis to develop a narrative overview of treatments of privacy and risk. Key terms were identified, interpreted and combined into themes present across multiple articles in a process analogous to grounded theory (c.f. Strauss and Corbin, 1994). Words and passages were highlighted that appeared to refer to privacy, risk, or normative claims. Highlighted segments were coded. Similar codes were assigned to themes. The frequency with which codes appeared was used as a starting point for discussion of results.

3. Results

A total of 527 articles were identified for review, 81 of which met the inclusion criteria of explicitly discussing aspects of privacy or risk and PHM. Of the reviewed literature, 33 sources discussed designing a PHM system or underlying security or privacy architecture, 20 were empirical studies into

[1] For a discussion of ethical aspects of AmI and ubiquitous computing, See: (Bohn et al., 2005; Brey, 2005).

user, family or professional attitudes towards PHM, 12 reviewed literature about privacy, risk or security aspects, nine were theoretical analyses or conceptual discussions, five analysed normative dimensions of future scenarios of PHM usage and two were risk assessments. The following sections present a narrative overview of the literature, divided into conceptual themes which emerged. Two general types of privacy emerged: information privacy and personal privacy.

Before proceeding with the overview, definitions are required for terms used in presenting the results. The creators or subjects of data (e.g. who the data is 'about)' are denoted as 'users'. This title highlights the interaction between persons and PHM systems, which creates the data affecting privacy. Persons or organisations that handle the data once created are referred to as 'data custodians'. Other stakeholders include the rest of the parties who interact with or possess a claim to the data. For simplicity they are referred to as 'stakeholders'. A 'misuse' of data is any use (e.g. searching, analysis, comparison) to which the user has not consented.

3.1 Information Privacy

A majority of the reviewed literature focused on aspects of controlling and disseminating data about oneself. Information privacy was interpreted as the right to control data about oneself and limit third-party access (c.f. Chan et al., 2009; Demiris, 2009; Jea et al., 2008; Mitseva et al., 2008; Mittelstadt et al., 2011; Tentori et al., 2006; Tiwari et al., 2010; Van De Garde-Perik et al., 2006; van Hoof et al., 2007). At its narrowest, information privacy was equated with hiding personally identifiable information from unauthorised parties (Ahamed et al., 2007b; Garcia-Morchon et al., 2011), and was seen as quantifiable (Srinivasan et al., 2008). Concerns over data control were common among participants in empirical studies (Coughlin et al., 2007; Courtney, 2008; Little and Briggs, 2009; Melenhorst et al., 2004; Wilkowska et al., 2010). Unauthorised access or identification of the user may be prevented through anonymisation at data collection (c.f. Agrafioti et al., 2011), with access policies allowing chosen actors access to identifiable data (Bagüés et al., 2007b; Garcia-Morchon et al., 2011; Subramaniam et al., 2010) for acceptable purposes (Beaudin et al., 2006; Chakraborty et al., 2011; Massacci et al., 2009). Transparency of relationships between data collected and purposes of collection is central to protecting privacy of users (Giannotti and Saygin, 2010), who make decisions regarding acceptable uses.

Information privacy empowers users to control the information revealed to others about themselves, limiting opportunities for unwanted disturbances and exploitation, caused by an information imbalance. Information enables regulation, behavioural control and social sorting by those with greater access (Kosta et al., 2010), so controlling information flow enhances dignity, autonomy and privacy. Thus, information privacy acts as a check on the power of organisations and data custodians (Friedewald et al., 2007; Moncrieff et al., 2009). Risks associated with uses of personal data beyond those found acceptable (or consented to) by users require "strict guidelines of confidentiality" to prevent unwanted personalised marketing and personalised insurance premiums (Kosta et al., 2010; Percival and Hanson, 2006), or exclusion or discrimination against (non)users wishing to limit access to their personal data (Brey, 2005). To limit possibilities of data misuse and come closer to an ideal of informed consent, information about temporal limitations and purposes for data use need to be available to users before data gathering (Kosta et al., 2010).

Despite empowerment attached to information privacy, absolute control over personal data may not be a necessity for PHM to be accepted by users. Empirical studies into attitudes towards PHM revealed a preference to forego information privacy in emergency situations (Rashid et al., 2007; Steele et al., 2009), which highlights the need to find a balance between the desire to control data and enjoy the benefits of services which require that data. A similar balance is expressed in preferences towards PHM for data gathering over human intrusion into the home (c.f. Essén, 2008). User-end policies have been proposed as a solution which allows users to pre-define a customized level of privacy meeting their expectations (Friedewald et al., 2007; Garcia-Morchon et al., 2011; Massacci et al.,

2009).[2] Privacy tools such as these are said to enable users to freely move between and interact with a range of PHM systems without negotiating individual privacy agreements, while respecting the necessity of informed consent (c.f. Bagüés et al., 2007b).

Security

Although not explicitly searched for, security emerged as a theme in information privacy literature. Privacy and security were frequently conceptually interchangeable (c.f. Ahamed et al., 2007a; Armac et al., 2009; Busnel and Giroux, 2010; Chan et al., 2008; Dhukaram et al., 2011; Elkhodr et al., 2011; Garcia-Morchon et al., 2009; Mana et al., 2011; Stuart et al., 2008; Wang et al., 2008); ensuring system security through appropriate frameworks and encryption algorithms was taken to guarantee user privacy. The concepts can be differentiated by their ends: security is concerned with guaranteeing the *quality* of the data collected by and passing through a system in terms of "confidentiality, integrity and availability" (Giannotti and Saygin, 2010), enabling users to protect *privacy* by controlling dissemination of personal data. Under this distinction, security mechanisms may alert a user to unrecognised flows of information between systems and stakeholders (Moncrieff et al., 2009), which could be limited to respect the user's information privacy.

Security risks were defined in terms of interception, modification and falsification of sensor data (Acharya and Kumar, 2010; Lim et al., 2010), and authentication scheme (Giannetsos et al., 2011; Massacci et al., 2009; Subramaniam et al., 2010).[3] Security frameworks including key management schemes, encryption algorithms and (actor-based) authentication mechanisms were seen as protecting the confidentiality, integrity and flow of information passing through PHM systems (Acharya, 2010; Chan et al., 2009; Fragopoulos et al., 2010; Giannotti and Saygin, 2010).[4] In these terms, security features protect a user's ability to control and trust his data—the conceptual confusion seen in the reviewed literature is therefore unsurprising.

Trust

Trust, understood as a security concept, emerged in the reviewed literature as necessary component for PHM systems to be seen as 'privacy enhancing' (c.f. Bagüés et al., 2010; Chakraborty et al., 2011; Coughlin et al., 2009; Dhukaram et al., 2011; Rashid et al., 2007; Wang et al., 2008; Yuan et al., 2007), when privacy is interpreted as control over personal data. Trust is defined in the context of information privacy as an interaction between a system which collects and processes data, users which provide the data, and stakeholders who access it. A lack of trust in a system has been linked to reluctance among potential users to use systems (Brey, 2005; McLean, 2011). Users 'place trust' in systems and stakeholders to handle their data responsibly, which facilitates and secures data sharing (Bagüés et al., 2010; Kosta et al., 2010; Little and Briggs, 2009). Trust can be understood as a sum of the credibility, motivation, transparency and responsibility of a system. Credibility is linked to 'loyalty' or 'reputation' (Little and Briggs, 2009; Rashid et al., 2007); a stakeholder must be seen as responsible or credible enough to handle sensitive personal data. Motivation refers to the intentions of stakeholders, or how they intend to use the data of users. Monitoring of parameters or putting data to uses beyond those explicitly agreed upon by users was taken to undermine trust. These motivations, and intended uses of data, should be transparent to users, as should the sum of data collected and held about them. To achieve trust, systems must allow users to review and control their data.

---

[2] User ownership of personal data has also been suggested as a solution to data mining risks presented by PHM (Pentland, 2009); this solution would, however, present a significant barrier to the realisation of legitimate commercial and research interests, and would require sophisticated legislation detailing appropriate third party uses of personal data without the explicit consent of the data owners.

[3] An extensive review of technical security risks is provided by Armac et al (2009).

[4] Confidentiality refers to limiting access to data to stakeholders with authorisation (Giannetsos et al., 2011; Giannotti and Saygin, 2010).

3.2 Personal Privacy

Personal privacy describes aspects of privacy not directly related to control of data. Personal privacy was interpreted to mean the right to be left alone or not monitored by a third party (c.f. Demiris and Hensel, 2009; Dorsten et al., 2009; Mittelstadt et al., 2011; Pallapa et al., 2007; Wilkowska et al., 2010), which affects feelings of intimacy and control over 'private space' (Gaul and Ziefle, 2009; Ziefle et al., 2011).[5] Personal privacy can also be understood as a freedom, to "escape being observed or accessed when desired" (Essén, 2008), implying a social duty to respect the desire for isolation of others. The introduction of PHM may cause a gradual loss of personal privacy (Steele et al., 2009), particularly among smart home systems (Coughlin et al., 2007; Demiris, 2009; Dorsten et al., 2009). Monitoring technologies can create a psychological disturbance, sometimes called obtrusiveness (c.f. Hensel et al., 2006; Nefti et al., 2010), expressed in a feeling of 'being watched'; certain technologies, particularly cameras (Caine et al., 2006; Demiris et al., 2004; Leone et al., 2011; Stowe and Harding, 2010; Tiwari et al., 2010; Zwijsen et al., 2011), produce greater perceived violations of personal privacy in this regard.

Personal privacy is a multifaceted concept, defined by interactions between social individuals, ICT and the natural world. As seen in the reviewed literature, personal privacy includes:

- **Physical Privacy** – Physical accessibility of a person to others, defined by physical borders, such as doors and walls (Bowes et al., 2011; Brey, 2005; Essén, 2008; Little and Briggs, 2009). This can also be interpreted as a right to possess and protect personal space (Kosta et al., 2010), such as a home.
- **Social Privacy** – Control over social interaction through geographical distance, group membership and location. It is connected to physical privacy (Bagüés et al., 2007a; Coughlin et al., 2007; Little and Briggs, 2009), and can contribute to social isolation.
- **Decisional Privacy** – Absence of undesired interference from others in making decisions (Bowes et al., 2011; Essén, 2008). Decisional privacy enables the expression of autonomy.

Physical and social privacy are placed at risk by PHM capacities to transmit data to third parties (Brey, 2005; Friedewald et al., 2007), or move personal data past privacy protecting natural, social, spatial, temporal, ephemeral and transitory borders (c.f. Marx, 2001). PHM increases the interconnectness of users and stakeholders through data sharing which blurs the boundaries between 'public' and 'private' spaces and data.

Decisional privacy is placed at risk by monitoring when interpreted by users as a form of electronic surveillance; awareness of monitoring can affect behaviour (Essén, 2008), especially risk taking among seniors (Percival and Hanson, 2006; Remmers, 2010) which can represent a desire to retain independence at home, despite safety risks. Monitoring may also lead to 'labelling' of users as 'health impaired' or 'at-risk' (McLean, 2011; Percival and Hanson, 2006; Rigby, 2007), further limiting behavioural freedom (Kosta et al., 2010). Alternatively, the user's home may be increasingly freed from external interference by reducing the need for carer visits. Whether this outcome is desirable, particularly among the mentally impaired and physically frail, remains a question of appropriate balances between safety, autonomy and self-determination (c.f. Remmers, 2010). The need for 'self-care' among users can also be reduced by violations of decisional privacy, if for example PHM takes the decision to call for help out of the hands of the user (Bowes et al., 2011). In this case, user privacy is violated through automatic sharing of personal data, which causes intrusion of a third party into a user's private space.

3.3 Information and Personal Privacy Overlap

[5] The distinction between personal and information privacy was not always upheld in the reviewed literature, with control over dissemination of personal information occasionally understood as a form of personal privacy (c.f. Bagüés et al., 2010).

The conceptual distinction between information and personal privacy is not always clear. By controlling the dissemination of personal information, a person may be spared future physical, social and decisional disturbance from third parties, such as friends, family and service providers (c.f. Friedewald et al., 2007). Many privacy risks described in the literature cannot clearly be separated into information or personal privacy. For example, the visibility of a PHM system to others can cause the user to experience stigma (McLean, 2011), because the device's visibility transmits information to others without the user's consent, while also influencing behavioural and decisional freedom in public.

Technological 'Need' and Privacy

Monitoring is understood to inherently raise questions of privacy, but potential violations can be justified on the basis of 'need' for the technology, derived perhaps from safety concerns related to health (Steele et al., 2009; Zwijsen et al., 2011), or to delay a move to residential care (Essén, 2008; McLean, 2011; Remmers, 2010; Townsend et al., 2011). This type of 'tradeoff' demonstrates the potential for PHM to simultaneously violate and enhance privacy. A tradeoff was often presented between personal privacy and safety, particularly among the mentally impaired (Landau et al., 2010; Ojasalo et al., 2010; Stowe and Harding, 2010), as well as frail elderly (Courtney, 2008; Courtney et al., 2008; Melenhorst et al., 2004; Steele et al., 2009) and chronically ill persons (Neild et al., 2004; Salih et al., 2011). In this context, it was suggested that personal privacy could be simultaneously enhanced by reducing need for carer or family visits (Essén, 2008; Ojasalo et al., 2010), but reduced by the presence of a monitoring device invading the user's 'private' sphere. In community care situations, personal privacy is typically desired with regard to other patients, rather than carers. However, in the home the opposite is true (Essén, 2008); freedom from professional carers enabled by PHM can increase the tradeoffs, in terms of privacy, autonomy and other ethical values, that are seen as acceptable. These tradeoffs may be seen as a necessary part of aging, with increasing susceptability to health problems (Steele et al., 2009), though this view should not be applied generally to associate 'aging' with reduced expectations of privacy, or to justify increased privacy violating interventions.

3.4 The Absence of Risk

"Privacy" and "risk" were treated as independent concepts in the search terminology. Initial expectations were that 'risk' would prove to be a robust concept, revealing ethical and social dimensions of PHM beyond those identified in the previous literature review (Mittelstadt et al., 2011), given that risk is often used as a generic term to refer to the normative dimensions of (emerging) technological artefacts (c.f. Busnel and Giroux, 2010; Hilty et al., 2004; Kastenhofer, 2011; Morris, 2000). The discussion of risk in the reviewed literature is limited almost exclusively to privacy and security implications (Lim et al., 2010; Nefti et al., 2010; Pentland, 2009; Sadri, 2011) or risk taking behaviours of seniors (Percival and Hanson, 2006; Remmers, 2010). Risk was rarely conceptualised as a future-oriented concept, as seen in risk assessments of future scenarios (c.f. Friedewald et al., 2007; Kastenhofer, 2011). The inclusion of 'risk' as an independent concept did not contribute content beyond themes addressed. The exception was a risk assessment identifying normative aspects of pervasive computing including environmental and human effects of non-ionizing radiation, stress imposed on users, restriction of consumers' and patients' freedom of choice, threats to ecological sustainability, and dissipation of responsibility in computer-controlled environments (Hilty et al., 2004).

4. Discussion

PHM privacy discourse, represented in the reviewed literature, overwhelmingly addresses protection of information privacy through security measures, while dedicating far less attention to the importance of personal privacy and context-specific norms (c.f. Nissenbaum, 2004). This finding is especially true of sources discussing the development of PHM systems and underlying security architecture, of which only three mention aspects of personal privacy (Bagüés et al., 2007a; Neild et al., 2004; Pallapa et al., 2007). While other types of sources addressed personal privacy, few references were found to

background normative theory or theories of privacy. In many sources discussion of privacy, risk and related concepts was very brief, limited to few sentences or paragraphs, although longer discussions were not rare (c.f. (Brey, 2005; Friedewald et al., 2007; Gaul and Ziefle, 2009; Little and Briggs, 2009; Remmers, 2010; Ziefle et al., 2011). Privacy was often seen as a hurdle to be overcome to make systems acceptable to users by protecting their right to control their data (c.f. Zwijsen et al., 2011), rather than as a broad normative concept with context and user-specific norms.

These results reveal two significant gaps in the literature: (1) system and security developers fail to explain their understanding of privacy and related concepts (e.g. security, trust, confidentiality) from a theoretically informed position; and (2) aspects of personal privacy which cannot be addressed through system and security development receive comparatively little attention. This suggests a disconnect exists between theoretical and applied disciplines, in which theoretical development of privacy as a normative concept fails to inform development of PHM systems and underlying security architecture.

Explicit definitions and discussions acknowledging the conceptual complexity of privacy were scarce in security-oriented literature[6], suggesting that systems are being designed and secured under the impression that privacy protections function generically across a variety of contexts. This fails to acknowledge the context-sensitivity of (expectations of) privacy (Nissenbaum, 2004), and risks presenting systems as 'privacy-enhancing' (c.f. Subramaniam et al., 2010) which are merely technically secure: "The idea is tempting: once we solve security, that is, once we are able to achieve authenticity and trusted communications, privacy will be a by-product that follows inevitably from a secure environment…The important aspect to realize is that security might not be the panacea it appears to be, and it might not need to be that panacea either" (Langheinrich, 2001). When privacy is seen as a complex, multi-faceted normative concept inspiring a rich history of normative theory, the simplistic, 'one-size-fits-all' approach to security in PHM appears insufficient.

The narrow conception of privacy, by which privacy is reduced merely to control of data, risks simplifying future discourse, design and governance of PHM by ignoring personal, context-sensitive aspects of privacy. Current discourse risks devaluing experiences of users falling outside of the narrow scope of privacy defined in terms of data. Furthermore, it is problematic to claim that a PHM system or security mechanism is 'privacy-enhancing' (c.f. Garcia-Morchon et al., 2009; Pallapa et al., 2007) without demonstrating awareness of the conceptual complexity of privacy, and underlying theories of privacy. The need to expand the scope of the discourse has been recognised (Caine, 2009), but remains largely unrealised as evidenced by the relatively few sources which provide in-depth discussions of aspects of privacy beyond security or data control.

This feature of current discourse may be a result of application developers lacking expertise in security (Busnel and Giroux, 2010), privacy and ethical theory, while simultaneously failing to acknowledge research in these areas.[7] This is not to suggest that developers need to engage in theorising, especially in reporting on new systems, security measures and frameworks in conference proceedings and academic journals. Rather, what was lacking from 'applied' discussions in the reviewed literature was *awareness* of the complexity of privacy, security and risk, and the ethical and social scientific works which demonstrate the difficulties associated with 'universal', acontextual conceptions of privacy (c.f. Nissenbaum, 2004). The literature suggests developers understand privacy one-dimensionally: privacy is control over data about oneself, and is guaranteed through security mechanisms. If this simplified conception becomes embedded in system design, users face a future of 'privacy enhancing' health monitoring systems which may fail to meet their privacy expectations in practice. To mitigate this risk, developers and regulators need to better explicate their conception of privacy and its theoretical foundations, and identify how it is translated into system design. Furthermore, achieving a context-sensitive understanding of privacy requires understanding attitudes and expectations of stakeholders (McLean, 2011), as well as practice-internal norms

[6] Of the 81 sources reviewed, only 27 explicitly defined privacy or risk.

[7] The limitation of privacy to data control, dissemination and security aspects by developers matches Westin's influential conception of privacy as the right of individuals "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others" (1970).

(MacIntyre, 1984; Nissenbaum, 2004) of information dissemination and fair usage unique to the context(s) in which a particular PHM application will be used. Empirical research (c.f. Gaul and Ziefle, 2009; Little and Briggs, 2009; Ziefle et al., 2011) and participatory design methods (c.f. Genus and Coles, 2005; Joss and Bellucci, 2002) which address these needs are readily available, and need to be explicitly utilised by developers.

By failing to address personal privacy in the design of PHM systems and security, the design discourse is ignoring intrusions by third parties into the 'private' lives of users unrelated to data dissemination (see: Section 3.2). Data sharing is at the heart of such disturbances, yet describing the normative character of these violations in purely informational terms misses the disturbing aspect of the intrusion—it is the fact that data is being collected or shared, rather than the content of the data, which is seen as problematic. In other words, PHM systems disturb users through the introduction of third parties into their private spaces and decisions. This aspect of PHM, which can be described in terms of psychological obtrusiveness (c.f. Hensel et al., 2006), has not yet received the attention it deserves in the literature, perhaps because its solution does not lie (only) in 'designing for security'.

The importance of correcting this deficiency in the discourse also lies in the great potential for PHM to violate privacy expectations of users in collecting and handling extremely sensitive personal data. PHM gathers data about health, often within the confines of the home (Rashid et al., 2007). Systems are being implemented to monitor these sensitive domains, yet it is doubtful that users understand the systems' potential, in terms of violations of privacy and data mining (Beaudin et al., 2006). Data can be collected and presented in potentially distressing or revealing formats, connections can be identified between seemingly unrelated pieces of information, and a range of unforeseeable secondary uses of increasingly rich longitudinal data sets are possible. Users may assume that developers and data custodians have 'protected them' from unanticipated consequences through appropriate privacy policies (Rashid et al., 2007), creating a space in which privacy violations can occur beyond the awareness of the user.[8]

5. Conclusion

The results of this review reveal that the current discourse of privacy, risk and PHM is dominated by concerns related to controlling the dissemination of personal information. While in-depth discussions of non-information aspects of privacy do exist, they have failed to impact upon the discourse surrounding system development and security, which generally operate upon a narrow definition of privacy as 'information privacy'. It follows that systems designed to meet myopic interpretations of privacy may fail to meet the privacy expectations of future users of PHM. To improve the discourse, background normative theories of privacy, autonomy and self-determination (c.f. Hoven, 2008; Nissenbaum, 2004; Rossler, 2004), among others, need to applied to improve the development and governance of PHM.

Acknowledgements

This research was funded by a studentship from De Montfort University, to build upon two European Union funded projects, PHM-Ethics (Grant agreement no.: 230602) and ETICA (Grant agreement no.: 230318). The implicit contribution of the other partners in those projects is acknowledged.

References

Acharya, D., 2010. Security in Pervasive Health Care Networks, in: Mobile Data Management (MDM), 2010 Eleventh International Conference On. pp. 305–306.

Acharya, D., Kumar, V., 2010. A secure pervasive health care system using location dependent unicast key generation scheme, in: 3rd Workshop on Ph.D. Students in Information and Knowledge Management, PIKM'10, Co-located with 19th International Conference on Information and Knowledge Management, CIKM'10. Toronto, ON, pp. 87–90.

[8] This situation raises a philosophical question regarding whether a user must 'care about' their privacy for violations of privacy to occur. Unfortunately, addressing this complex topic goes beyond the scope of this review.

Agrafioti, F., Bui, F.M., Hatzinakos, D., 2011. Medical biometrics in mobile health monitoring. Security and Communication Networks 4, 525–539.

Agree, E.M., Freedman, V.A., Cornman, J.C., Wolf, D.A., Marcotte, J.E., 2005. Reconsidering substitution in long-term care. Journals of Gerontology - Series B Psychological Sciences and Social Sciences 60, S272–S280.

Ahamed, S.I., Talukder, N., Haque, M.M., 2007a. Privacy challenges in context-sensitive access control for pervasive computing environment, in: 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous 2007. Philadelphia, PA.

Ahamed, S.I., Talukder, N., Kameas, A.D., 2007b. Towards privacy protection in pervasive healthcare, in: 3rd IET International Conference on Intelligent Environments, IE'07. Ulm, pp. 296–303.

Armac, I., Panchenko, A., Pettau, M., Retkowitz, D., 2009. Privacy-friendly smart environments, in: NGMAST 2009 - 3rd International Conference on Next Generation Mobile Applications, Services and Technologies. Cardiff, pp. 425–431.

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

Bagüés, S.A., Zeidler, A., Valdivielso, C.F., Matias, I.R., 2007a. Disappearing for a while, in: 6th ACM Workshop on Privacy in the Electronic Society, WPES'07, Held in Association with the 14th ACM Computer and Communications Security Conference. Alexandria, VA, pp. 80–83.

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

Beaudin, J.S., Intille, S.S., Morris, M.E., 2006. To Track or Not to Track. J Med Internet Res 8.

Bohn, J., Vlad Coroamă, Marc Langheinrich, Friedemann Mattern, Rohs, M., 2005. Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. Institute for Pervasive Computing. CiteSeerX.

Bowes, A., Dawson, A., Bell, D., 2011. Ethical Implications of Lifestyle Monitoring Data in Ageing Research. Information, Communication & Society.

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

Busnel, P., Giroux, S., 2010. Security, privacy, and dependability in smart homes, in: 8th International Conference on Smart Homes and Health Telematics, ICOST 2010. Seoul.

Caine, K.E., 2009. Visual sensing devices in home-care systems, in: 1st ACM Workshop on Security and Privacy in Medical and Home-Care Systems, SPIMACS "09, Co-located with the 16th ACM Computer and Communications Security Conference, CCS"09. Chicago, IL, pp. 61–62.

Caine, K.E., Fisk, A.D., Rogers, W.A., 2006. Benefits and privacy concerns of a home equipped with a visual sensing system, in: 50th Annual Meeting of the Human Factors and Ergonomics Society, HFES 2006. San Francisco, CA, pp. 180–184.

Chakraborty, S., Choi, H., Srivastava, M.B., 2011. Demystifying privacy in sensory data, in: 2011 9th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011. Seattle, WA, pp. 38–43.

Chan, M., Campo, E., Estève, D., Fourniols, J.-Y., 2009. Smart homes — Current features and future perspectives. Maturitas 64, 90–97.

Chan, M., Estève, D., Escriba, C., Campo, E., 2008. A review of smart homes. Computer Methods and Programs in Biomedicine 91, 55–81.

Coughlin, J.F., D'Ambrosio, L.A., Reimer, B., Pratt, M.R., 2007. Older adult perceptions of smart home technologies, in: 29th Annual International Conference of IEEE-EMBS, Engineering in Medicine and Biology Society, EMBC'07. Lyon, pp. 1810–1815.

Coughlin, J.F., Lau, J., D'Ambrosio, L.A., Reimer, B., 2009. Adult children's perceptions of intelligent home systems in the care of elderly parents, in: 3rd International Convention on Rehabilitation Engineering and Assistive Technology, ICREATE '09.

Courtney, K.L., 2008. Privacy and senior willingness to adopt smart home information technology in residential care facilities. Methods of Information in Medicine 47, 76–81.

Courtney, K.L., Demiris, G., Rantz, M., Skubic, M., 2008. Needing smart home technologies. Informatics in Primary Care 16, 195–201.

Demiris, G., 2009. Privacy and social implications of distinct sensing approaches to implementing smart homes for older adults. Conference proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference 2009, 4311–4314.

Demiris, G., Hensel, B., 2009. "Smart homes" for patients at the end of life. Journal of Housing for the Elderly 23, 106–115.

Demiris, G., Rantz, M., Aud, M., Marek, K., Tyrer, H., Skubic, M., Hussam, A., 2004. Older adults' attitudes towards and perceptions of 'smart home' technologies. Informatics for Health and Social Care 29, 87–94.

Dhukaram, A.V., Baber, C., Elloumi, L., Van Beijnum, B.J., De Stefanis, P., 2011. End-User perception towards pervasive cardiac healthcare services, in: 2011 5th International Conference on Pervasive Computing Technologies for Healthcare and Workshops, PervasiveHealth 2011. Dublin, pp. 478–484.

Dorsten, A.M., Sifford, S.K., Bharucha, A., Mecca, L.P., Wactlar, H., 2009. Ethical perspectives on emerging assistive technologies. Journal of Empirical Research on Human Research Ethics 4, 25–36.

Elkhodr, M., Shahrestani, S., Cheung, H., 2011. Ubiquitous health monitoring systems. Journal of Computer Science 7, 1465–1473.

Essén, A., 2008. The two facets of electronic care surveillance. Social Science & Medicine 67, 128–136.

Fragopoulos, A.G., Gialelis, J., Serpanos, D., 2010. Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures, in: 12th IEEE International Conference on e-Health Networking, Application and Services, Healthcom 2010. Lyon.

Friedewald, M., Vildjiounaite, E., Punie, Y., Wright, D., 2007. Privacy, identity and security in ambient intelligence. Telematics and Informatics 24, 15–29.

Garcia-Morchon, O., Falck, T., Heer, T., Wehrle, K., 2009. Security for pervasive healthcare, in: 2009 6th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous 2009. Toronto,ON.

Garcia-Morchon, O., Falck, T., Wehrle, K., 2011. Sensor network security for pervasive e-health. Security and Communication Networks 4, 1257–1273.

Gaul, S., Ziefle, M., 2009. Smart home technologies, in: 5th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society, USAB 2009. Linz.

Genus, A., Coles, A., 2005. On Constructive Technology Assessment and Limitations on Public Participation in Technology Assessment. Technology Analysis & Strategic Management 17, 433–443.

Giannetsos, T., Dimitriou, T., Prasad, N.R., 2011. People-centric sensing in assistive healthcare. Security and Communication Networks 4, 1295–1307.

Giannotti, F., Saygin, Y., 2010. Privacy and Security in Ubiquitous Knowledge Discovery Ubiquitous Knowledge Discovery, in: Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 75–89.

Hensel, B.K., Demiris, G., Courtney, K.L., 2006. Defining Obtrusiveness in Home Telehealth Technologies. Journal of the American Medical Informatics Association 13, 428–431.

Hilty, L.M., Som, C., Köhler, A., 2004. Assessing the human, social, and environmental risks of pervasive computing. Human and Ecological Risk Assessment 10, 853–874.

Jea, D., Liu, J., Schmid, T., Srivastava, M., 2008. Hassle free fitness monitoring, in: 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, HealthNet'08. Breckenridge, CO.

Joss, S., Bellucci, S., 2002. Participatory technology assessment. Centre for the Study of Democracy, University of Westminster, London.

Kastenhofer, K., 2011. Risk Assessment of Emerging Technologies and Post-Normal Science. Science Technology Human Values 36, 307–333.

Kosta, E., Pitkänen, O., Niemelä, M., Kaasinen, E., 2010. Mobile-centric ambient intelligence in Health and Homecare. Science and Engineering Ethics 16, 303–323.

Landau, R., Werner, S., Auslander, G.K., Shoval, N., Heinik, J., 2010. What do cognitively intact older people think about the use of electronic tracking devices for people with dementia? A preliminary analysis. International psychogeriatrics / IPA 22, 1301–1309.

Langheinrich, M., 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems, in: Abowd, G., Brumitt, B., Shafer, S. (Eds.), Ubicomp 2001: Ubiquitous Computing, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 273–291.

Leone, A., Diraco, G., Siciliano, P., 2011. Topological and volumetric posture recognition with active vision sensor in AAL contexts, in: 4th IEEE International Workshop on Advances in Sensors and Interfaces, IWASI 2011. Savelletri di Fasano, Brindisi, pp. 110–114.

Lim, S., Oh, T.H., Choi, Y.B., Lakshman, T., 2010. Security issues on wireless body area network for remote healthcare monitoring, in: 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC 2010, 2010 IEEE International Workshop on Ubiquitous and Mobile Computing, UMC 2010. Newport Beach, CA, pp. 327–332.

Little, L., Briggs, P., 2009. Pervasive healthcare, in: 2nd International Conference on PErvasive Technologies Related to Assistive Environments, PETRA 2009. Corfu.

Lymberis, A., 2005. Wearable health systems and applications, in: 2005 27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEE-EMBS 2005. Shanghai, pp. 4149–4152.

Lyon, D., 2003. Surveillance as social sorting. Routledge, London.
MacIntyre, A.C., 1984. After virtue. University of Notre Dame Press.
Mana, M., Feham, M., Bensaber, B.A., 2011. Trust key management scheme for wireless body area networks. International Journal of Network Security 12, 75–83.
Marx, G.T., 2001. Murky conceptual waters. Ethics and Information technology 3, 157–169.
Massacci, F., Nguyen, V.H., Saidane, A., 2009. No purpose, no data, in: 1st ACM Workshop on Security and Privacy in Medical and Home-Care Systems, SPIMACS "09, Co-located with the 16th ACM Computer and Communications Security Conference, CCS"09. Chicago, IL, pp. 53–57.
McLean, A., 2011. Ethical frontiers of ICT and older users. Ethics and Information Technology 13, 313–326.
Melenhorst, A.-S., Fisk, A.D., Mynatt, E.D., Rogers, W.A., 2004. Potential Intrusiveness of Aware Home Technology. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 48, 266–270.
Mitseva, A., Wardana, S.A., Prasad, N.R., 2008. Context-aware privacy protection for wireless sensor networks in hybrid hierarchical architecture, in: International Wireless Communications and Mobile Computing Conference, IWCMC 2008. Crete, pp. 773–778.
Mittelstadt, B., Fairweather, B., McBride, N., Shaw, M., 2011. Ethical Issues of Personal Health Monitoring, in: ETHICOMP 2011 Proceedings. Presented at the ETHICOMP 2011.
Moncrieff, S., Venkatesh, S., West, G., 2009. A framework for the design of privacy preserving pervasive healthcare, in: 2009 IEEE International Conference on Multimedia and Expo, ICME 2009. New York, NY, pp. 1696–1699.
Morris, J., 2000. Rethinking Risk and the Precautionary Principle. Butterworth-Heinemann.
Nefti, S., Manzoor, U., Manzoor, S., 2010. Cognitive agent based intelligent warning system to monitor patients suffering from dementia using ambient assisted living, in: 2010 International Conference on Information Society, i-Society 2010. London, pp. 92–97.
Neild, I., Heatley, D.J.T., Kalawsky, R.S., Bowman, P.A., 2004. Sensor Networks for Continuous Health Monitoring. BT Technology Journal 22, 130–139.
Nissenbaum, H., 2004. Privacy as Contextual Integrity (SSRN Scholarly Paper No. ID 534622). Social Science Research Network, Rochester, NY.
Ojasalo, J., Seppälä, H., Suomalainen, N., Moonen, R., 2010. Better technologies and services for smart homes of disabled people, in: 2010 2nd International Conference on Software Technology and Engineering, ICSTE 2010. San Juan, PR, pp. V1251–V1259.
Pallapa, G., Roy, N., Das, S., 2007. Precision, in: ICSE 2007 Workshops: First International Workshop on Software Engineering for Pervasive Computing Applications, Systems, and Environments, SEPCASE'07. Minneapolis, MN.
Pentland, A. et al., 2009. Using Reality Mining to Improve Public Health and Medicine. White Paper (Commissioned by Robert Wood Johnson Foundation).
Percival, J., Hanson, J., 2006. Big brother or brave new world? Critical Social Policy 26, 888–909.
PHM Ethics Consortium, 2012a. PHM-Ethics - Final Report (No. GA 230602). PHM Ethics Consortium.
PHM Ethics Consortium, 2012b. PHM-Ethics - Deliverable D7-9.1: Report on Validation Results (No. D7-9.1). Ernst-Moritz-Arndt-University Greifswald.
Rashid, U., Schmidtke, H., Woo, N., 2007. Managing disclosure of personal health information in smart home healthcare, in: 4th International Conference on Universal Access in Human-Computer Interaction, UAHCI 2007. Beijing.
Remmers, H., 2010. Environments for ageing, assistive technology and self-determination. Informatics for Health and Social Care 35, 200–210.
Rigby, M., 2007. Applying emergent ubiquitous technologies in health. International journal of medical informatics 76, S349–S352.
Rossler, B., 2004. The Value of Privacy, 1st ed. Polity.
Sadri, F., 2011. Ambient Intelligence. ACM Computing Surveys 43, 36.1–36.66.
Salih, R.M., Othmane, L.B., Lilien, L., 2011. Privacy protection in pervasive healthcare monitoring systems with active bundles, in: 9th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, ISPAW 2011 - 2011, ICASE 2011, SGH 2011, GSDP 2011. Busan, pp. 311–315.
Srinivasan, V., Stankovic, J., Whitehouse, K., 2008. Protecting your daily in-home activity information from a wireless snooping attack, in: 10th International Conference on Ubiquitous Computing, UbiComp 2008. Seoul, pp. 202–211.
Steele, R., Lo, A., Secombe, C., Wong, Y.K., 2009. Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. International journal of medical informatics 78, 788–801.
Stowe, S., Harding, S., 2010. Telecare, telehealth and telemedicine. European Geriatric Medicine 1, 193–197.

Strauss, A., Corbin, J., 1994. Grounded theory methodology, in: N. K. Denzin Y. S. Lincoln (Ed.), Handbook of Qualitative Research. Sage Publications, Inc, Thousand Oaks, CA, US, pp. 273–285.

Stuart, E., Moh, M., Teng-Sheng, M., 2008. Privacy and security in biomedical applications of wireless sensor networks, in: Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium On. pp. 1–5.

Subramaniam, C., Ravi, A., Nayak, A., Thunuguntla, S., 2010. Actor based domain specific privacy model for U-healthcare system, in: 6th International Conference on Digital Content, Multimedia Technology and Its Applications, IDC2010. Seoul, pp. 381–385.

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

Tiwari, P., Warren, J., Day, K.J., McDonald, B., 2010. Some non-technology implications for wider application of robots assisting older people. Health Care and Informatics Review Online 14.

Townsend, D., Knoefel, F., Goubran, R., 2011. Privacy versus autonomy, in: Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS. pp. 4749–4752.

Ure, J., Pinnock, H., Hanley, J., Kidd, G., McCall Smith, E., Tarling, A., Pagliari, C., Sheikh, A., MacNee, W., McKinstry, B., 2012. Piloting tele-monitoring in COPD. Primary Care Respiratory Journal 21, 57.

Van de Garde-Perik, E., Markopoulos, P., De Ruyter, B., 2006. On the relative importance of privacy guidelines for ambient health care, in: NordiCHI 2006: 4th Nordic Conference on Human-Computer Interaction - Changing Roles. Oslo, pp. 377–380.

Van den Hoven, J., 2008. Information Technology, Privacy, and the Protection of Personal Data, in: Information Technology and Moral Philosophy, Cambridge Studies in Philosophy and Public Policy. Cambridge University Press.

Van Hoof, J., Kort, H.S.M.D., Markopoulos, P., Soede, M., 2007. Ambient intelligence, ethics and privacy. Gerontechnology 6.

Wang, K., Sui, Y., Zou, X., Durresi, A., Fang, S., 2008. Pervasive and Trustworthy Healthcare, in: Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference On. pp. 750 –755.

Westin, A.F., 1970. Privacy and Freedom. Bodley Head.

Wilkowska, W., Gaul, S., Ziefle, M., 2010. A small but significant difference, in: 6th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering, USAB 2010. Klagenfurt.

Yuan, W., Guan, D., Lee, S., Lee, Y.K., 2007. The role of trust in ubiquitous healthcare. Presented at the HEALTHCOM 2007: Ubiquitous Health in Aging Societies - 2007 9th International Conference on e-Health Networking, Application and Services, pp. 312–315.

Ziefle, M., Röcker, C., Holzinger, A., 2011. Medical technology in smart homes. Presented at the 35th Annual IEEE International Computer Software and Applications Conference Workshops, COMPSACW 2011, pp. 410–415.

Zwijsen, S.A., Niemeijer, A.R., Hertogh, C.M.P.M., 2011. Ethics of using assistive technology in the care for community-dwelling elderly people. Aging and Mental Health 15, 419–427.