pHealth 2021
B. Blobel and M. Giacomini (Eds.)

doi:10.3233/SHTI210571

How a Service User Knows the Level of Privacy and to Whom Trust in pHealth Systems?

Pekka RUOTSALAINEN[a,1], Bernd BLOBEL[b,c,d]
[a] *Faculty of Information Technology and Communication Sciences (ITC), Tampere University, Finland*
[b] *Medical Faculty, University of Regensburg, Germany*
[c] *eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany*
[d] *First Medical Faculty, Charles University of Prague, Czech Republic*

Abstract pHealth is a data (personal health information) driven approach that use communication networks and platforms as technical base. Often it' services take place in distributed multi-stakeholder environment. Typical pHealth services for the user are personalized information and recommendations how to manage specific health problems and how to behave healthy (prevention). The rapid development of micro- and nano-sensor technology and signal processing makes it possible for pHealth service provider to collect wide spectrum of personal health related information from vital signs to emotions and health behaviors. This development raises big privacy and trust challenges especially because in pHealth similarly to eCommerce and Internet shopping it is commonly expected that the user automatically trust in service provider and used information systems. Unfortunately, this is a wrong assumption because in pHealth's digital environment it almost impossible for the service user to know to whom to trust, and what the actual level of information privacy is. Therefore, the service user needs tools to evaluate privacy and trust of the service provider and information system used. In this paper, the authors propose a solution for privacy and trust as results of their antecedents, and for the use of computational privacy and trust. To answer the question, which antecedents to use, two literature reviews are performed and 27 privacy and 58 trust attributes suitable for pHealth are found. A proposal how to select a subset of antecedents for real life use is also provided.

Keywords pHealth, eCommerce, privacy, trust, antecedents

1. Introduction

According to Lodewjk Bos, pHealth has both personal and personalized Health dimensions and it takes palace in digital environment [1]. Despite that the concept of pHealth is somewhat fuzzy, its focus seems to be how personal health information can be used in patient care and how a person can monitor and manage his or her health and health behavior. pHealth is also a data driven approach where major parts of collected and used personal health information (PHI) is generated by the data subject or patient

[1] Corresponding Author. Pekka S. Ruotsalainen, DSc (Tech.), Adjunct professor, Research professor emeritus, Faculty of Information Technology and Communication Sciences (ITC), Tampere University, Kanslerinrinne 1, 33014 Tampere, Finland; Email:pekka.ruotsalainen@uta.fi

itself or by sensors, wearable technology and motes. Information measured and monitored includes person's vital signs, health behaviors and activities, location, movement, feeling and emotions, social relations, environmental factors and vital signs. Typical pHealth service includes the collection of PHI and the output is processed information (e.g. calculated values and trends), personalized recommendations and guidelines which help the user to monitor and management own health and health behaviors. For data transfer, communication pHealth typically uses existing third party services such as the Internet, wireless networks, and short range digital communication systems. Digital platforms, clouds and application are typically used for data processing, storing and sharing tasks. From this perspective, pHealth, eCommerce, eHealth, mHealth, Internet shopping and social networks look similar. pHealth has also lot of common with the novel 5P medicine approach, as both offer personalized and preventive services for health management. Both approaches also collect wide spectrum of PHI that exceeds radically the content of current regulated EHR [2]. According to Gorini, the future medicine (e.g. 5P medicine) requires patients/person's full psychological and cognitive profile, i.e. information such as health lifestyle, personality, cognitive dispositions, social conditions and psychological state, specific needs and values, habit and behavior patterns, hopes and fears, beliefs, individual characteristics, decision making style, emotional profile, psychological contexts (presence of stress, anxiety, depression) and information about physical, social, and economic environments [3]. In real life, this amount of sensitive personal information cannot be collected by any single organization or service provider. Instead many sources a needed such as social networks (data the person himself/herself discloses), pHealth, mHealth and eHealth applications, eCommerce and Internet shopping services, and public and private health care. That way, they all together form a big data ecosystem. In this ecosystem, pHealth applications can be play a meaningful role as data collector and information source.

Unfortunately, this data driven future of pHealth and 5P medicine raises many new and until now unsolvable privacy and trust problems. The multi-stakeholder natures of the data ecosystem and the huge spectrum of collected and used PHI together make it difficult for the service user to know why, and how much, to trust in pHealth services and the eco-system, and what the actual level of privacy in pHealth is.

There are many reasons, why the service user cannot blindly trust the service provider and expect that necessary privacy safeguards are in place and legal privacy requirements are met in the pHealth ecosystem. First, networks and ecosystems are often multi-stakeholder systems, where commercial stakeholders (e.g. platform operators and non-regulated health service providers) have own business goals, privacy policies and trust behaviors. They often do not see people only as customers. Service users' data is raw material for their products and new businesses [4]. Firms also often do not hold what they have promised in their privacy documents and trust manifestos, and in real life, users have almost no control what data is collected and how it is used and shared [5]. Furthermore, commercial organizations typically expects that people trust them blindly, and organizations' privacy documents are written more to protect them, and they are typically written in a legal language that is difficult to understand. Furthermore, currently widely used security-based privacy protection tools cannot really guarantee privacy.

It is evident that – from service users' point of view – the current situation is unsatisfactory and shall be changed. The authors state that the user of digital services collection and processing sensitive PHI such as pHealth applications need a possibility to evaluate on-line the level of privacy and trust of services and information system behind it. To help the user of pHealth services in decision making on starting to use or

not to use service and how much PHI to disclose, the authors propose the development of an evaluation service solution that is easy to use for a human and that reflects the service user's view point. Two main element of the evaluation system are calculation methods and appropriate input variables (antecedents) used in calculation. In this paper, the authors' focus are antecedents.

2. Privacy and Trust

Information privacy and trust are complex concepts with many approaches and definitions. They are also interconnected in such a way that the amount of positive trust reduces the need for privacy protection. High privacy and trust are prerequisites for successful use of pHealth, eHealth, eCommerce and Internet shopping. Basic privacy types are general privacy and contextual privacy [6]. Widely used information privacy approaches include: privacy as right and control (ability to control); privacy as legal construct; risk based privacy; privacy as contextual integrity; privacy as concerns [7, 8].

Originally, trust was understood to exist between persons, but currently it is accepted that trust also exists between human and organizations, human and computers as well as technology in a general sense. The way trust is understood depends on culture and context. Human trust is a personal trait. Trust is needed in situations where insufficient information is available. Disposition to trust is understood as tendency to trust in others. Other views to trust include subjective probability, belief in trustor's features, attitude, perception and trust as risk and willingness to trust [9, 10].

Trust can be general trust and context- or system-specific trust. In digital information systems, the person (service user) has to trust in organizations, technology, computational features of the information and communication system and computer applications. Computational trust imitates human trust, and at the same time, it enables the service user to estimate the degree of trust. For trust calculation, mathematical model considering changes in trust caused by its antecedents are often used [11].

3. Antecedents for privacy and trust

A widely used approach in eCommerce, Internet shopping and social networks is to assume that the user beliefs that information privacy is guaranteed, and he or she feels that service provider and the network/ecosystem is trusted. Unfortunately, this approach is not true in real life digital information systems. Trust and privacy in pHealth services depends of service providers and computational environments contextual features. Therefore, contextual privacy and trust models should be used instead of general privacy and trust. Contextual privacy and trust require that antecedents used describe contextual features of the service provider and information systems.

To find candidate privacy and trust antecedents for pHealth the authors made a literature review of privacy and trust focused papers published in major journals and covering eCommerce, Internet shopping, social media and eHealth. Because, as discussed in Chapter 1, pHealth uses similar ICT technological solutions and services as eCommerce, Internet shopping and eHealth, the authors expect that privacy and trust antecedents researchers have found valid for them can be also used to evaluate privacy and trust in pHealth.

3.1. Privacy Antecedents

Table 1 presents an aggregated summary of widely used privacy approaches and corresponding antecedent retrieved from a literature review. It is almost impossible for the service user to measure privacy itself. Therefore, and because privacy depends more on cognitions and perceptions than on rational assessments, privacy proxies such as belief, risk, concerns, benefits, perceived harm and other perceptions are widely used as antecedents [6].

Table 1 Privacy approaches and their attributes [12-15]

Privacy approach	Possible antecedents
General privacy	Belief, disposition
Privacy as control and restrict access Privacy as individual right	Knowledge of service provider's practices and information system, direct experiences, past experiences, privacy promises audit-trails, privacy seals, information practices, other's proposals perception
Privacy as concerns	Personality, motivations, perceptions, context information, service user's behaviours, technology used data type, others opinions, perceived severity
Risk based privacy	Assessed risk level, perceived risk in technology, perceived concerns, cost/benefit ratio, perceived harm or impact, privacy seal
Privacy as contextual integrity	Context type and its features, type and sensitivity of data, contextual privacy practices, privacy culture
Privacy as legal concept	Legal requirements, compliance analysis

3.2. Trust Antecedents

In a literature analysis performed by the authors, 58 different trust antecedents were found. The authors classified them into seven groups (customer perception, customer experiences, service provider characteristics, features of the service, information based features, infrastructural factors and external and environmental) provided in Appendix A [9, 12, 16-29]. The biggest group, i.e. service provider (vendor, organization or institute) characteristics, contain 24 antecedents. From another review focused on privacy and trust in eHealth, the authors found that in eHealth privacy, reputation and informational factors (e.g. professionalism of information and medical quality of information) are most meaningful antecedents for the user.

4. Challenges in Evaluation of Privacy and Trust in pHealth

The service user's ultimate goal is to measure the level of actual privacy of the service provider and the surrounding ecosystem, and to know why and how much he or she can

trust in a service provider. In real life, there are many things, which make it difficult to reach this goal. A big challenge is the lack of reliable and accurate information of service provider's privacy and trust features and behaviors. Another challenge is that privacy laws (e.g. the EU-GDPR) are high-level documents without information on implementation details. Laws typically balance industry's business needs and national interest against a person's privacy needs, resulting in insufficient privacy. For example, the EU-GDPR enables service providers to define "mandatory cookies" and what the content of legitimate interest is. Researchers have argued that in digital environment laws are insufficient to give the person reasonable power to control what personal information is collected by service providers and organizations, and how this data is processed and disclosed [30, 31].

Many of the antecedents shown in Table1 and Appendix A such as belief, intention, motivation, benefit, ability, honesty, goodwill, harm and reliability are abstract, difficult to conceptualize and measure, and often proxies for perceptions, opinions or even feelings. Widely used others opinions concerning privacy and trust are unreliable and can be misleading. Perceptions such as perceived risks or perceived harm are more opinions than a description of the real life risks and caused harm. Caused by the lack of reliable information and the vagueness of risk and harm concepts, it is an illusion that a pHealth service user can make credible measurement of privacy risks and possible future harm.

In Table 1 and Appendix A, totally 85 antecedents are shown. A subset should be selected to make them practical for human use. For that purpose, a selection criterion is needed. The authors propose the prioritization of antecedents, which values are available (e.g. third partner privacy seal or audit-trail) or measurable. Other antecedents can be grouped as follows: own previous experiences, own perceptions, other proposals, personal opinions or feeling and beliefs.

5. Discussion

Trust is not only a personal trait, it is also a glue between people, organizations, and information systems. In other words, our society requires trust to function. Therefore, trust is a public good that together with information privacy enables a person to safely use pHealth services and disclose PHI [34]. Unfortunately, it is a common practice in today's eCommerce, Internet shopping, eHealth and pHealth to expect that service users automatically belief that service providers are trustworthy, information privacy is guaranteed (i.e. necessary protection tools and protocols are implemented correctly) and service providers keep their promises (e.g. what is promised in privacy policy documents and trust manifestos). Additionally, it is expected that the user accepts service provider's business rules and the collection of PHI without the possibility to define own rules. In digital information systems, hidden collection of person's behavioral information is a dominant practice, and the service user has no real possibility to know how PHI is used inside information systems and to whom data is disclosed or sold. From a user's point of view, this is an unacceptable situation. Therefore, the authors state that pHealth and eHealth service users need a tool to evaluate the level of privacy, and to know in whom to trust before starting to use services and to disclose PHI.

Because there is a big amount of computation privacy and trust solution available, the authors have focused in this paper on antecedents [6, 35, 36]. For the pHealth service

user, the authors propose a method where the service user evaluates the service provider's privacy and trust using computational method and (as far as possible) in real lively measurable contextual antecedents [33]. Furthermore, they conclude that privacy and trust antecedents of eCommerce, Internet shopping and eHealth are also deployable in pHealth. Based on literature review the authors presented a set of candidate antecedents.

The biggest barriers to implement the author's proposal is the lack of measurable and reliable information describing service provider's and surrounding information system's privacy and trust features and behaviors. Another challenge is that currently widely used privacy and trust approaches do not work in digital environments. The disparity in power between the service user and service provider enables the service provider to use own privacy rules and laws allowing this. To solve those problems, it is necessary to redefine current privacy and trust concepts and move them to virtual and digital environments where pHealth takes place. A novel approach to those problems is, e.g., the definition of privacy as personal property and trust as specific legal fiducial duty [37, 38]. New laws and regulations are also necessary to support those new privacy and trust approaches and to force service providers to publish reliable, detailed and measurable information concerning their privacy practices and trust features and behaviors.

6. Conclusions

Current privacy and trust situation in pHealth resembles the ongoing climate change discussion: researchers know what is going on and what should be done, but industry and governments prefer economic grow and profit orientation. A change is inevitable. If current situation persists, there will be no privacy in the future and a complete loss of trust in anyone. Our PHI is monetarized, and person's privacy needs are overridden by business and political objectives, manipulating people to trust blindly. This way leads to an inhuman, immoral, unethical society.

For overcoming the challenges, the authors have proposed the use of computational methods for privacy and trust evaluation and defined a set of suitable antecedents. The next step is the development of practical solutions enabling the services user an on-line evaluation of information privacy and the possible to trust in a service provider.

References

[1] Bos L. pHealth. Stud Health Technol Inform. 2012; 177, 3-13. doi:10.3233/978-1-51499-069-7-3.
[2] RuotsalainenP, Blobel B. Privacy s Dead – Solutions for Privacy-Enabled Collections and Use of Personal Health Information in Digital Era. Stud Health Technol Inform. 2020; 273, 63-74. doi:10.3233/SHTI200616
[3] Gorini A, Caiani G, Pravettoni G. Psycho-cognitive Factors Orienting eHealth Development and Evaluation, in G. Pravettoni, S. Triberti (eds.), P5 eHealth: An Agenda for the Health Technologies of the Future, Springer Open, https://doi.org/10.1007/978-3-030-27994-3_7
[4] Zuboff S. The Age of Surveillance Capitalism, Public Affairs, ISBN 9781781256855.
[5] Aquisti A, Laura Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information, Science Special Section The end of privacy, Science. 2015 Jan 30; 347 (6221): 509-514 DOI: 10.1126/science.aaa1465, http://science.sciencemag.org/.
[6] Smith, H J, Dinev T, Xu H. Information privacy research: an interdisciplinary review, MIS Quarterly December 2011; Vol. 35 No. 4: 989-1015.

[7] Marguilis ST. Privacy as a Social Issue and Behavioral Concept, Journal of Social Issues 2003; 59 (2): 243-261.
[8] Zwick D. Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce. 1999.
[9] Lilien L, Bhargava B. Trading Privacy for Trust in Online Interactions. Purdue University, West Lafayette, U.S.A.
[10] Jøsang A, Ismail R, Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision, Decision Support Systems, 2007; 43(2): 618-644.
[11] Liu X, Datta A, Lim E-P. StereoTrust: a group based personalized trust model. Proceedings of the 18th ACM conference on Information and knowledge management, 2009. doi: 10.1145/1645953.1645958.
[12] McKnigth H D, Choundhury V, Kacmar C. Developing and line Interactions. Validating Trust Measures for e-Commerce: An Integrative Typology, Information Systems Research, 2002 INFORMS. September 2002; 13 (3): 334–359.
[13] Corbitt B J, Thanasankit T, Yi H. Trust and e-commerce: a study of consumer perceptions, Electronic Commerce Research and Applications 2003; 2 (3): 203-215. doi:10.1016/S1567-4223(03)00024-3.
[14] Barth S, D.T, de Jong MDT, Jungerc M, Hartel PH, Roppelta JC. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources, Telematics and Information. August 2019; 41: 55-69. https://doi.org/10.1016/j.tele.2019.03.003.
[15] Kosa TA, El-Khatib K, Measuring Privacy, Journal of Internet Services and Information Security (JISIS), 2011; 1 (4): 60-73.
[16] Arifin, D M, Antecedents of Trust in B2B Buying Process A Literature Review, 5th IBA Bachelor Thesis Conference, July 2nd, 2015, Enschede, The Netherlands. Copyright 2015, University of Twente, The Faculty of Behavioural, Management and Social sciences.
[17] Pennanen K. The Initial Stages of Consumer Trust Building in e-Commerce: a Study on Finnish Consumers, ISBN 978–952–476–257–1 http://urn.fi/URN:NBN:fi-fe2018062126262.
[18] Meziane F, Nefti S. Evaluating E-Commerce Trust Using Fuzzy Logic, International Journal of Intelligent Information Technologies, October-December 2007; 3(4), 2-3, IGI Global, edited by Vijayan Sugumaran, Hershey, USA.
[19] Vega J A, Determiners of Consumer Trust towards Electronic Commerce: An Application to Puerto Rico, Esic Market Economics and Business Journal January-April 2015; 46 (1): 125-14.
[20] Egger, FN. From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce, Eindhoven University of Technology (The Netherlands), 2003, ISBN 90-386-1778-X.
[21] Grabner-Kräuter S, Kaluscha EA. Consumer trust in electronic commerce: conceptualization and classification of trust building measures, Chapter in 'TRUST AND NEW TECHNOLOGIES' edited by Teemu Kautonen & Heikki Karjaluoto, Edward Elgar Publishing 2008, pp. 3-22.
[22] Brændeland G, Støle K. Using Risk Analysis to Assess User Trust – A Net-Bank Scenario, C.D. Jensen et al. (Eds.): iTrust 2004. Springer LNCS; 2004; 2995: 146–160.
[23] Hussin Ab R C, Macaulay, The Importance Ranking of Trust Attributes in e-Commerce Website, 11th Pacific-Asia Conference on Information Systems, 2007.
[24] Salam A F, Iyer L, Palvia P, Sin R. Trust in e-Commerce. Communications of the ACM, February 2005/Vol. 48, No. 2, pp. 73-77.
[25] Beldad A, de Jong M, Steehouder M, How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust, Computers in Human Behavior 26 (2010) 857–869, Elsevier. doi:10.1016/j.chb.2010.03.013
[26] Yan Z, Holtmanns S. Trust Modeling and Management: from Social Trust to Digital Trust, book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global, 2007, DOI: 10.4018/978-1-59904-804-8.ch013.
[27] Chen CC, Dhillon G. Interpreting Dimensions of Consumer Trust in E-Commerce, Information Technology and Management 4, 303–318, 2003, 2003 Kluwer Academic Publishers. Manufactured in The Netherlands.
[28] Mayer RC, Davis JH and Schoorman FD. An Integrative Model of Organizational Trust,: The Academy of Management Review, Vol. 20, No. 3 (Jul., 1995), pp. 709-734. URL: http://www.jstor.org/stable/258792. 137-154, ISSN 0718–1876 Electronic Version, www.jtaer.com, DOI: 10.4067/S0718-18762010000200009.
[29] Kimi A, Choobineh J. Trust in Electronic Commerce: Definition and Theoretical Considerations, 1060-3425/98,1998 IEEE.
[30] Xu, H, Teo Hock-Hai, Tan BCY. Predicting the adoption of location-based services: the role of trust and perceived privacy risk

[31] Lankton N K, McKnight D H, Tripp J. Technology, Humanness, and Trust: Rethinking Trust in Technology, Journal of the Association for Information Systems, Volume 16, Issue 10, pp. 880-918, October 2015.
[32] Richards, N M, Hartzog W. Taking Trust Seriously in Privacy Law. (September 3, 2015). 19 Stanford Technology Law Review 431 (2016), Available at SSRN: https://ssrn.com/abstract=2655719 or http://dx.doi.org/10.2139/ssrn.2655719
[33] Ruotsalainen P, Blobel B. Health Information Systems in the Digital Health Ecosystem—Problems and Solutions for Ethics, Trust and Privacy Health 2020, Int. J. Environ. Res. Public 2020; 17(9): 3006; doi:10.3390/ijerph17093006.
[34] Engel C. Privacy as a Public Good, Duke Law Journal, Volume 65, Number 3, December 2015.
[35] Pinyol I, Sabater-Mir J. Computational trust and reputation models for open multi-agent systems: a review Artif Intell Rev 2013; 40: 1–25 DOI 10.1007/s10462-011-9277-z.
[36] Sabater J, Sierra C. Review on computational trust and reputation models. Artif Intel Rev 2005; 24(1):33–60.
[37] Ritter J and Mayer A. Regulating Data as Property: A New Construct for Moving Forward, 16 Duke Law & Technology Review 2018; 220-277.
[38] Waldman AE. Privacy as Trust- Information Privacy for an Information age Cambridge University Press, 2108, ISBN 978-1-316-63694-7.

Appendix A Factors impacting to trust formulation in e-services

Perceptions [16, 17, 18, 19, 21, 20, 22, 23, 24]	**Customer experiences** [17, 25, 26, 27]
- Perceived quality of services - Perceived lack of privacy - Perceived lack of customer control - Perceived risks - Perceived trustworthiness, expertise and credibility - Perceived usefulness and perceived ease of use - Perceived predictability and consistency in the vendor's actions - Perception that vendor is honest and concerned about its customers	- Satisfaction with previous online transactions - Past experiences, Purchase experiences - Satisfaction of the product - Feedback and recommendations - How well the observed behaviour of the system meets their own standards - Past behavior and seller keeps promises

Service provider (vendor, organization, institution) characteristics [9, 12, 13, 16, 19, 20, 21, 23,24, 25, 26, 27, 28, 29, 30]

- Responsibility
- Firm type
- Ability or competence, benevolence, integrity, honesty, fairness, faith
- Absence of guarantees
- Appearance
- Competence
- Credibility
- Dependability
- Goodwill
- Familiarity and Friendliness
- Fiduciary and size
- Motivation
- Predictability
- Performance
- Persistence
- Policies e.g. return policy, privacy policy, quarantine policy
- Potential opportunistic behaviors
- Reliability
- Reputation of the company
- Structural assurance and Situational normality
- Values of the seller
- Vendors' presence (Availability of mailing address
- and telephone numbers)

Features of the service [19, 21, 23, 27]

- Service quality (tangibles, reliability, responsiveness, assurance, and empathy and satisfaction)
- Quality certificate
- Lack of customer control
- Service professionalism
- Product price

Information based features [21, 23]

- After sales service
- Existing data and literature
- Information about product and services
- Lack information regarding the behavior or characteristics of the object of trust
- Lack of information concerning IT-technology and privacy safeguards
- Service users' knowledge