pHealth 2020
B. Blobel et al. (Eds.)

doi:10.3233/SHTI200616

Privacy Is Dead – Solutions for Privacy-Enabled Collections and Use of Personal Health Information in Digital Era

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

Abstract. Today's digital information systems and applications collect every day a huge amount of personal health information (PHI) from sensor and surveillance systems, and every time we use personal computers or mobile phones. Collected data is processed in clouds, platforms and ecosystems by digital algorithms and machine learning. Pervasive technology, insufficient and ineffective privacy legislation, strong ICT industry and low political will to protect data subject's privacy have together made it almost impossible for a user to know what PHI is collected, how it is used and to whom it is disclosed. Service providers' and organizations' privacy policy documents are cumbersome and they do not guarantee that PHI is not misused. Instead, service users are expected to blindly trust in privacy promises made. In spite of that, majority of individuals are concerned of their privacy, and governments' assurance that they meet the responsibility to protect citizens in real life privacy is actually dead. Because PHI is probably the most sensitive data we have, and the authors claim it cannot be a commodity or public good, they have studied novel privacy approaches to find a way out from the current unsatisfactory situation. Based on findings got, the authors have developed a promising solution for privacy-enabled use of PHI. It is a combination of the concept of information fiduciary duty, Privacy as Trust approach, and privacy by smart contract. This approach shifts the onus of privacy protection onto data collectors and service providers. A specific information fiduciary duty law is needed to harmonize privacy requirements and force the acceptance of proposed solutions. Furthermore, the authors have studied strengths and weaknesses of existing or emerging solutions.

Keywords. Privacy, trust, personal health information, fiduciary duty, smart contract, digital pHealth

Introduction

The revolution in ICT technology, computers, personal health devices, digitalization, algorithms, big data analytics and artificial intelligence, machine leaning and algorithmic

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

decision making have changed the way how, and the landscape where, personal health information (PHI) is collected, processed, stored and disclosed. Currently, PHI collected and used outside regulated health care environment exists increasingly in digital form and it is processed, stored and shared by computer programs, applications and algorithms via networks [1]. This development has also changed the architecture of information systems collecting and processing PHI (e.g. hospital information systems, eHealth and pHealth systems and systems for personal wellness management) to networked multi-stakeholder eco-systems where PHI is collected using sensors as well as by monitoring and surveillance systems, and processed by algorithms, artificial intelligence and machine learning applications.

This development has changed by whom, where and for what PHI is collected and used, and how PHI is communicated. Detailed surveillance of individual web-surfing is a new normal [2]. Increasingly, number of health related information is collected by others than health care professionals and medical devices, i.e. PHI is collected from wearable and mobile phone sensors, by surveillance systems, web browsers and computer applications [3]. For example a typical smart mobile phone has sensors and sensing devices such as camera, microphone, Bluetooth, magnetometer, GPS position system, ambient temperature and light sensors, barometer, accelometer, proximity sensor and gyroscope. Collection is not limited to personal tools (m-phone, wearable sensors, apps and browser trackers) [4]. Using technology-enabled surveillance and health tracking, we are monitored ubiquitously in public spaces when we drive a car or sit in our work place. In public spaces, surveillance cameras monitor continuously our movements and our behaviour. Today, nearly invisible drones can monitor us and at the same time measure our body temperature on roads. Monitoring of car driver's health condition is another new example of health tracking [5]. Surveillance and health tracking exists almost everywhere, even in our workplaces [6].

Data collection takes regularly place when we are using personal computers and smart phones [7, 8]. Our activities including health related data can be tracked by the browser, our e-mail are harvested by applications or invisible code injected by the manufacturer, the government or by third party applications legally or illegally. There are many other tools developed and sold for collecting of health related data such as self-adhesive patches, pedometers, smart health watches, wearable ECG monitors and a smart toilet. Personal information that is typically collected by those devices and applications includes heart rate, body temperature, sleep patterns, keyboard touching style, movement, location, time being sedentary, eating habit, respiration rate and body acceleration. This is only the beginning, where sensor and dataveillance technology is in its early development state. Data collected by sensors, surveillance systems and programs is processed by applications for weight control, chronic disease management such as diabetes and hypertension control, smoking control, anorexia symptom seeking, oxygen saturation, sleep quality management, stress testing and lifestyle management [4, 9] as well as health outcome and movement behaviours [10-13]. Increasingly, PHI collection, storing and analysis, health tracking and behavioural tracking are performed by commercial vendors.

For what purposes PHI collection and health tracking is done? Typical purposes include early detection of diseases, personal health and wellness management, disease management, but also the development of innovations including new personal heath devices. However, there are also other goals. Public health and health care are looking for cost savings via early detection of diseases and population health management. Medical and biomedical research uses PHI for better understanding causes of diseases

[14]. The novel 5P medicine approach requires huge amount of data for prediction and early detection of diseases [15]. Thereby, PHI such as epigenetic data, health history and history of health-related behaviours is used. Furthermore, PHI is widely used outside the health care domain by industry and governments [16]. In that context, PHI is increasingly understood as commodity or public good [14].

In spite of its many positive use, PHI collection and health tracking has also negative features, as it can lead to [2]:

- Loss of autonomy
- Increased behavioural, social and political control
- Behavioral manipulation and discrimination
- Monitoring of personal health and wellness by the government and work places
- Commodization of PHI and personal health status

Protection of information privacy has been for long "de facto" requirement for information systems processing and disclosing personal health information (e.g. health care information systems, eHealth and pHealth systems). Technological developments and changes in political thinking are currently challenging this. At policy level, discussions of free movement of health data, health data as public good and health monitoring for public health purposes are prospering. Industry sees increasingly health data as "new oil" and PHI as commodity. It is widely understood that in spite of that privacy is a Human Right [17], it is not absolute. In the society, there is increasingly conflighting interest between individual's need for information privacy on one hand and political and economic need for using PHI on the other hand. Decision makers are looking to balance those conflighting needs. Unfortunately, in many cases the need for privacy fails.

Future use of PHI is based on knowledge and communication. It also makes it difficult to build and to guarantee information privacy [18]. Many researchers have noted that in current information society privacy is dead in our current understanding, and in real life it is almost impossible to maintain privacy [7, 19, 20, 21, 22]. In the time of the Internet, social networks and m-phones, privacy has become an illusion and transparency and accountability are only dreams. From data subjects' point of view, the current situation is unacceptable and the future sounds eerily. Therefore, it is necessary to rethink the way we understand privacy and its role of in health information systems, and how sufficient privacy can be implemented in digital pHealth systems. In this paper, the authors will present some answers to this problem.

1. Privacy and the Lifecycle of PHI

Privacy is a vague concept with many definitions. At global level, there is no common agreement of its dimensions. In western countries, privacy is often understood as a personal right to protect the citizens against something (e.g. surveillance) and to exclude them from actions. It also implies saving their autonomy right who, when and for what purposes their PHI is used, or to be informed who and by whom to realize choice and control regarding PHI [23, 24]. The control idea is linked to metaphor of boundary and context, i.e. how to control data flow inside a context, through boundaries or between contexts [3, 14, 23, 25]. The protection approach and the right to be informed of the use of personal information are also central elements in many privacy laws. A widely used

approach in information systems and laws is the notice and choice model (i.e. consent model), where the data requester or user should notify the data subject (DS) of planned data collection, and he or she can use consent to accept or deny the planned use [23].

Both preventive, protective and detective methods and solutions have been used to enforce privacy in today's information systems. High level preventive methods include enforcement of ethical principles, responsibility in the sense of moral and ethical duty (e.g. responsibility to accountability in EU-GDPR), professional codes for duty, risk assessment, guidelines for Fair Information Practices [26], general and domain specific privacy laws (e.g. EU-GDPR and Acts for Patient Rights) [27], contracts (e.g. Service Level Agreements - SLAs), privacy audits, certification, and social navigation [28]. Technology oriented methods for privacy implementation include Privacy Impact Analysis (e.g. analysis of organizations privacy policy). Protective methods and tools such as access control, privacy policy enforcement, notice and consent models, privacy labelling, sticky privacy policies and computational methods for protections(e.g. PET technology such as adding noise to data, data minimization and separation), data anonymization techniques (e.g. k-anonymity and Differential privacy) as well encryption are widely used [29],[30]. Typical methods for detection of privacy breaches and recognition of data misuse are audit trail monitoring and applications for filtering data flows.

The DS's need for privacy covers the whole life cycle of personal information i.e. from data creation and collection to its destruction. This is extremely challenging task in dynamic and pervasive networks where service models such as pHealth, eHealth and digital health and health place and form multi-stakeholder eco-systems, and where data easy to collect and almost impossible to destroy by the DS. In modern digital networks data can be invisible collected, manipulated and shared, and the DS has in real life few or no ways to control the secondary and tertiary use of his or personal information. Another challenge is well known "privacy paradox" [31] i.e. inconsistency between individual's privacy concerns their actual behaviour. Surveys made by researchers have shown that in spite of privacy is a primary concern for individuals in digital networks they regularly self-disclose personal information and even PHI. People also continue to use the services known to misuse data especially in social and other digital networks [31].

Main phases in the life-cycle of PHI are collection, communication, retention, processing, disclosing and destroying, and privacy concerns exist in all of those phases. A weak link is the data collection phase especially situation and place where data is created and collected from. Personal information and PHI are increasingly collected every time we are using personal computers and mobile phone [7]. In computers data is collected both at Browser and application level. Browser level data collection uses typically small code packets (cookies) which are injected to the computer. For a user there are few tools to know and control what data collection programs are doing without destroying the functionality of the service. Direct data collection and transfer made by application is nearly impossible to recognize and prevent because the code used is hidden for the user. Some of intrinsic surveillance apps even encrypt the collected data. Furthermore, the lack of application level transparency and audit trails means that the DS cannot know how PHI is used by the data collector and to whom disclosed.

External health tracking and surveillance in public places is another increasing privacy problem. Currently with it the person has in real life no possibility to know what data is collected, how his or her PHI is used.

Contractual agreement is one of strongest method for privacy protection. Unfortunately here the data subject is the weaker partner and he or she has currently

limited of no power to negotiate contract details with service providers [14]. Instead, they often state their privacy policies in vague terms, present them as "take-or-leave" offer, and also change their privacy policies any time. Legal binding contracts are currently not offered for eCommerce and pHealth customers. Traditional contracts offer limited privacy protection and have no role in privacy protection in digitals environments [32].

By Ruotsalainen traditional privacy approaches discussed have meaningful weaknesses in today's virtual and distributed information environment. Privacy-as-control model is insufficient, privacy boundaries are virtual in digital environment, and it is impossible to control their opacity. Policy based solutions will not work because there is a big asymmetry in power between the DS and data processors, as the DS cannot force the data collector to follow rule expressed by the DS [3, 14]. Furthermore, caused by the lack of reliable information of service provider's privacy features the DS cannot make information-based (rational) choices [33].

Our social life is depending on the use of digital services, and we cannot separate us from networks, eCommerce and eHealth services and from social groups despite privacy is currently almost dead. Because PHI is one of the most sensitive information people have, the authors state that it cannot be a commodity, public good or public data. Therefore, it is necessary to rethink the way we understand and enforce privacy in pHealth and other digital health environments, and how it is possible to prevent unnecessary collection and misuse of PHI. In this paper, the authors study related current work and present a novel solution for trustworthy pHealth.

2. Approaches for privacy enabled digital pHealth

Need for privacy has not disappeared. According to Solove, a society has strong interest in protecting sensitive personal information. At the same time however, privacy at personal level should be balanced against the benefits of society [32]. New approaches should not only respond to this requirement, but they should also be implementable and easy to use in digital information systems. The following new approaches for privacy for information age are presented by researchers:

- Privacy as information fiduciary [34, 35]
- Privacy as Trust [2, 24]
- Privacy as Personal Property [3]

Furthermore, the authors have proposed a novel "privacy by digital smart contract" approach for digital pHealth.

According to Balkin, in digital information systems there are significant knowledge asymmetries between online service providers and end-users [34]. It is very challenging for end-users to understand and verify online companies' documents concerning their information practices. Furthermore, it very difficult for the DS to know what the service provider does with the data and to monitor its use [34]. For protecting personal privacy and preventing data misuse and discrimination, it is necessary to find new legal solution. Balkin proposed a concept of an information fiduciary, i.e., "caused by the power organizations have (e.g. online service providers and cloud companies) to collect, analyse, use, sell, and distribute personal information, they should be understood as information fiduciaries toward their customers and end-users" [34]. Furthermore, they have special duties to behave in a way not do harm to persons and DS. In Balkin's approach, a fiduciary is the duty of loyalty concerning the collection and processing of

personal information, and a fiduciary (e.g. a person, organization, on-line service provider) must act in the interests of the DS.

According to Dobkin, at least 77.4% of websites globally track visitors' data (2016). He stated, the only protection users have is the service provider's privacy policy [35]. He also noted that understanding service providers as "information fiduciaries" may be a solution to balance freedom of speech with data privacy [35]. Dobkin presented how a service provider can breach the fiduciary duty: using data for manipulation, discrimination; sharing their data with third parties without consent; or violating own privacy policies. Also Dobkin proposed a legislative act for the enforcement of fiduciary duties [35].

Fiduciary duty supported by the special Fiduciary Law is an interesting proposal with much strength. It is useful in situations where it is difficult for the DS to conclude contracts. It can also be acceptable for health care providers. Fiduciary duty can be used in different context such as regulated health care, unregulated health service, pHealth research and wellness management. It offers benefits in the case of data surveillance in public spaces. Duty rules should be ethically acceptable, context depending, transparency and publically available. A legally binding duty prevents big companies to set their own privacy standards. Instead, it defines a norm every service provider must follow [35]. The fiduciary duty model has also weaknesses. Because digital services are global, an internationally accepted content of an information duty law for collecting and processing of PHI is needed. For it, a common standard for concepts such as "health service provider" and "personal health information" is necessary. A common definition is also needed for fiduciary relationships. Because the existence of a duty does not guarantee that its requirements are always fulfilled, a mechanism such as monitoring data processors' behaviour is needed to detect duty breaches. Another challenge is that PHI is increasingly used for secondary purposes where the fiduciary relationship can be unclear.

One of newest approaches to privacy is the use social theory and social network theory. It has led to understanding privacy as a social concept [25, 32]. Neil Richards and Ari Waldman have argued that information privacy is a social construct based on trust. According to Richards "thinking of privacy in terms of trust is essential" [2]. Waldman developed Privacy as Trust approach that is not exclusively bound to concepts of choice, autonomy, or seclusion. Instead, it is a social fact as a social norm [24]. In Walman's approach, a private context is also a trusted context. Trust is defined as expectations of others' behaviour, and it is connected to privacy because invasions of privacy are felt as breaches of our expectations in trust. Similarly to Balkin and Dobkin, Waldman uses the concept of information fiduciaries, i.e. the DS and data collectors or processors have fiduciary responsibilities of loyalty. In this model, social norms regulate information flows and injuries to information are injuries to social norms [25]. Legislation addressing the breach of confidentiality is also needed. According to Schwartz et al., fiduciary duty can be understood as a trust builder [36]. Fiduciary duties can be contextual, and therefore Waldman's approach can be seen as extension of Nissenbaum's Privacy as Contextual Integrity model.

In Waldman's Privacy as Trust approach, privacy is defined as social norm, and trust is an expectation of others behaviour. Those definitions let a lot open. Although privacy can be understood as a social construct, there is no guarantee that even in one country exists a common social norm for privacy. There might be different contexts resulting in specific social norms, and big commercial vendors usually have their own. It also remains open who in a context defines the content of that social norm for privacy - a

powerful company or a political group? Another problem is the definition of trust as an expectation, aka a belief, what is inacceptable [14]. It is also unclear, what kind of trust is used (e.g. organizational trust, recommended trust, or disposition to trust) and how trust is created [3]. Dispositional trust (also called 'basic trust') is a general tendency to trust others. Organizational is based on a service user's perceptions or direct measurements that the organization has installed proper safeguards in its information system. Recommended trust is based on others' recommendation (ratings) of the trustworthiness of a service provider based on previous experiences.

In digital environment, a user of pHealth service has not only to trust in a service provider, but also in invisible computer technologies, applications and algorithms. Trust in technology is often a belief that technology use is reliable, secure, and protects information privacy [37]. In real life, this is unfortunately just an illusion because we know a little or nothing of service providers' processes and safeguards. In a pHealth eco-system, there are many data brokers, on-line platforms and Big Health Data operators which use algorithms to analyse collected PHI. In consequence, the service user has no idea how providers work and how trustworthy they are [32]. By the authors belief-based trust is too weak and too easy to manipulate to be acceptable. Instead, computational trust should be used where the level of trust is calculated using information got from previous experiences, direct measurement or monitoring [14]. A challenge is that commercial service provider can be seldom fully transparent in real life. According to Donkin, fiduciary duties are duties of trust, i.e. they are trust builders [35]. The authors state that fiducial duty based on an information duty law is much stronger than belief and can be used in information systems as proxy of organizational duty.

Contract is strong method to protect privacy by agreement of information privacy rules [34]. From a service user point of view however, traditional contracts will not work in dynamic digital networks, eco-systems and platform based services where the responsibility for privacy is shared. First of all, a digital service model includes many independent stakeholders such as tele-operators, platform managers, software and hardware providers and developers. In many cases, the service user even does not know all of them. In real life, it is an unrealistic task for a service user to make privacy contracts at similar level in the beginning of a dynamic session with all possible stakeholders. Furthermore, a single user is the weaker partner in the service process and does not have power to negotiate contracts with service providers which often offer only take-of-leave agreements. Finally, administration of contracts is a demanding task for most service users.

Smart digital contract is a novel solution to overcome weaknesses of traditional contracts. Smart contract is a computer algorithm for the automation of concluding contracts between partners in decentralized environment, i.e., it is digital form of an agreement. A smart contract is a set of computer code intended to validate and enforce a legally binding digital contract. A user can initiate smart contract by sending a request message to execute functions of the contract [38]. If a smart contract is part of Blockchain services, the content and state of the contract is stored to blockchain where it can be easily verified. A benefit of a smart contract is that it can be done easily on-line. A smart digital contract can be also used to inform the service provider how the DS expects their PHI should be used.

The authors have presented an alternative approach to privacy for PHI: "privacy as a personal property" defined by law [3]. According to Baldin, the contractual agreement is similar to property model for privacy [34]. It has been earlier mentioned, that a fiduciary duty is trust creator. Based on those findings, the authors have developed a

novel privacy solution for digital pHealth by combining smart contract, aka privacy as property, and trust as fiduciary informational duty. The authors' proposal is also another model for privacy as trust. In it, trust is not a belief or dispositional trust, but an organizational trust based on a binding contract. Fiduciary privacy duties are defined in a PHI specific law. A challenge is that despite a smart contract has been concluded, this do not entirely guarantee or prevent the service provider to violate its promises. Therefore, a monitoring system such as audit-trail (e.g. encrypted, immutable transaction history) is needed to enable the service user to recognize duty breaches. It is also possible to calculate in advance the expected trustworthiness of the service provider [14, 39]. A technical solution for tamper-proof audit trail is a monitoring service that collects all information about the use of PHI into a Blockchain history repository. This kind of transaction history acts as additional trust builder that enables the DS to verify by whom, when and why their PHI has been used.

A benefit of the authors' solution compared to Walman's approach is that here privacy is not fixed to be a contextual social issue, and the DS can set personal privacy requirements. A weakness is that contracts will not work in the case of surveillance and health tracking in public spaces and governmental surveillance. As another weakness cryptographic solutions require secure key management.

3. Discussion and Conclusions

Currently, PHI is increasingly collected anywhere by computer and mobile phone operating systems and applications as well as and by sensors and by health tracking and surveillance systems. Collected PHI is processed and shared in eco-systems, between platform and cloud application, and processed automatedly by digital algorithms and machine learning. Service providers increasingly expect that the service users either blindly trust them or accept their "take-or-leave" privacy policy. This all has made it difficult for the DS to guarantee their information privacy. Problematic is that current privacy and trust solutions and regulations have proven to be insufficient to protect PHI in digital environment [2, 24]. Furthermore, in today's distributed and pervasive digital environment where PHI is collected, used and distributed, traditional privacy solutions such as consent and access control do not work. This all led to the conclusion that privacy in its current form we understand it is almost dead.

To find a way out of this dilemma, the authors have studied three novel privacy approaches proposed by researchers from the viewpoint of PHI collection, use and disclose. Approaches studied are the concept of informational fiduciary, Privacy as Trust approach and digital by smart contracts. Based on findings got the authors have developed a novel solution that is a combination of fiducial information duty approach, privacy as trust, and privacy by smart contract. Starting point is here a specific (informational) fiducial relationship between the DS and data collector/processor in information systems collecting and processing PHI. This approach has strengths such as: instead of organizational self-regulation based policies, privacy duties are defined by a PHI specific information fiduciary law. Furthermore, the vague term harm, currently applied to describe impacts of data misuse, is not used. Instead the concept duty breach is deployed. Its benefit is that data misuse is a break of contract, so there is no need for the DS to demonstrate the incurance of economic loss or harm.

Globally, it is difficult to find consensus of the meaning of the term privacy and to define what data is private or public. Furthermore, stakeholders in eco-systems and

digital platforms have often different opinions on privacy. Privacy as informational fiducial duty approach avoids this problem by seeing privacy as trust [2, 24].

In this paper, the authors have addressed the following questions:

- How to create trust ?
- How to measure that privacy promises are fulfilled ?
- What kind of regulatory support is needed? and
- How the proposed solution can be realized ?

In the authors' approach, trust is based on law based fiduciary duty and on binding smart contract. Privacy breaches are trust breaches, aka breaks of contractual agreement, i.e. rules which regulate the collection, use and disclosure of PHI. Smart contracts are computer applications, useful also in on-line situations. The content and state of contracts can be stored in tamper-proof blockchain repositories.

A strength of fiduciary duty based privacy as trust solution is that it works not only in personal computer and mobile phone environments but also with external surveillance systems such health tracking in public spaces as well as with governmental systems collecting PHI. The fiduciary duty approach works also with robots, algorithms and machines leaning applications [24]. It also increases radically the information transparency. The content of informational fiducial duties can be standardized and in such a way made acceptable at international level.

The authors' approach is a promising way for the current situation without being perfect. It is plausible that smart contract and regulatory information duty together offer better information privacy than currently widely used blind organizational trust and take-or-leave type privacy promises. Therefore, regulatory privacy duty is more binding than self-regulatory organization privacy promises. Unfortunately, in real life there is no guarantee that in the digital environment where low risk of the discovery of data misuse dominates, every service provider and data broker is benevolent, fulfils the contract and follows duty-based privacy policies. Therefore, the DS should have the possibility to monitor on-line what PHI is collected, and also to check afterwards that contractual requirements are fulfilled.

An interesting question is how information informational fiduciary duty and the EU GDPR are related? The EU GDPR is commitment to constitutional individual rights and it offers individuals new rights such as the right to be informed, the right to erasure, and the right to restrict data processing. The GDPR also requires that data collectors and processor use privacy by design method in developing and building information systems and products. The GDPR still relies on notice and choice concept aka consent [40] and it allows data collection and processing when it "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party" [41].

The informational fiduciary duty model shifts the onus of privacy protection onto data collectors and service providers. In the fiduciary duty model the fiduciary agrees or it is forced by the fiduciary law to act in the principal's (a person or a customer) benefit, and the use personal information must benefit the principal and cannot produce harm [42]. Furthermore, the fiducial approach has power to correct the currently existing information asymmetry between the service provider and the customer. According to Barrett any information fiduciary solution should require duties of loyalty, care, and confidentiality to the customer [40].

The GDPR uses concepts of data controller and data subject. In the fiduciary model the fiduciary is one who has special obligations of loyalty and trustworthiness toward a person aka the principal, the beneficiary, the client or the consumer [34]. According to Balkin the data collector and informational fiduciary concepts are quite similar but the

informational fiduciary approach sets to the fiduciary wider responsibilities [34]. Researcher have also noted that in todays networked and virtual information environment consent approach used by the GDPR is inadequate in protecting customer's information privacy [2, 25]. Furthermore, the GDPR also does not correct the power asymmetry that exists between the customer and the service provider. Instead, by classifying a service provider or a data collector as information fiduciary corrects the power imbalance between service providers and individuals [40].

A fiduciary can have at the same time parallel duties and conflicts in interest (conflicts between duties) can take place. The most typical conflict results from the fiduciary's duty of confidentiality [42]. In spite of that the fiduciary has to act for the principal's benefit and take into account his or her needs [42] organizations and service providers often maximize their own utility over customer's needs (e.g. maximal amount of personal information is collected for business benefit and customer's need for information privacy is disregarded) [43]. According to Laby fiduciary duty includes not using of the customer's information for own or others advantage, and not for maximizing own or organization's utility over customer's benefit and needs [42].

In real life monitoring of how commercial vendors and governmental organizations use collected PHI is difficult to realize because there is a strong need for commercial and official secret that hinder information transparency. Possible solutions to this problem include certification, tamper-proof blockchain based audit-trials and the deployment of intelligent trust monitoring agents. Currently, it is almost impossible for a service user to know what PHI is collected when he or she use personal computer or mobile phone, and therefore, it is also impossible to recognize possible misuse of PHI. Until now manufacturers of computers, mobile phones, platforms and operating systems have shown no willingness to enable the service user to monitor collected data. A solution to this problem is an application for on-line information flow tracking that can be used in mobile phones and personal computers [44]. If needed, it can also enable the DS to minimize (filter) PHI intended to be collected, and also to mark PHI for future inspection. Another challenge to be solved is to inspect which Web applications do act against duty based privacy requirements [45]. In the case of external health tracking and behavioral surveillance monitoring is often impossible. Therefore, other solutions such external independent certification should be used.

The approach proposed by the authors presents a step forward to privacy enabled trusted pHealth. The major remaining challenge is getting the regulatory support needed, i.e. to making governments worldwide to accept an informational fiduciary duty model for PHI collection, and to use the approach of privacy as personal property. The new California Consumer Privacy Act is a small step to this direction. In spite of that it does not define fiduciary duties it requires businesses to disclose what personal information is collected and gives users right to prevent selling of their personal information [35].

References

[1] Ruotsalainen P, Blobel B. Trust –Essential Requirement and Basis for pHealth Services. Stud Health Technol Inform. 2017; 237: 25-33. doi: 10.3233/978-1-61499-761-0-25.
[2] Richards N, Hartzog W. Taking Trust Seriously in Privacy Law, 19 STAN. TECH. L. REV. 431 (2016).
[3] Ruotsalainen P, Blobel B. Health Information Systems in the Digital Health Ecosystem—Problems and Solutions for Ethics, Trust and Privacy. Int. J. Environ. Res. Public Health 2020; 17,9: 3006. doi:10.3390/ijerph17093006.

[4] Santarossa S, Kane D, Senn CY, Woodruff SJ. Exploring the Role of In-Person Components for Online Health Behavior Change Interventions: Can a Digital Person-to-Person Component Suffice? Med Internet Res 2018;20,4:e144). doi:10.2196/jmir.8480.
[5] Shin H-S, Jung S-J, Kim J-J, Chung W-Y, Real Time Car Driver's Condition Monitoring System. Proceedings of the IEEE SENSORS 2010 Conference. doi: 978-1-4244-8168-2/10.
[6] Connolly R, McParland C. Dataveillance in the Workplace: Moving Beyond Divergent Perspectives, Chapter 19. In: Handbook of Research on Strategic Communication, Leadership, and Conflict Management in Modern Organizations, A volume in the Advances in Human Resources Management and Organizational Development (AHRMOD) Book Series IGI Global, Eds. Normore A, Javili M, Long L, January 2017. doi: 10.4018/978-1-5225-0983-7.ch063.
[7] Rose C. Ubiquitous Smartphones, Zero Privacy. Review of Business Information Systems 2012; 16,4: 187. doi:10.19030/rbis.v16i4.7438
[8] Wei Z, Zhao B, Su J. PDA: A Novel Privacy-Preserving Robust Data Aggregation Scheme in People-Centric Sensing System. International Journal of Distributed Sensor Networks, Volume 2013, Article ID 147839, 9 pages, Hindawi Publishing Corporation. http://dx.doi.org/10.1155/2013/147839.
[9] Clemente J, Valero M, Li F, Wang V, Song W. Helena: Real-time Contact-free Monitoring of Sleep Activities and Events around the Bed, IEEE PerCom 2020. https://www.researchgate.net/publication/337926432_Helena_Real-time_Contact-free_Monitoring_of_Sleep_Activities_and_Events_around_the_Bed.
[10] Liang B, Yang N, He G, Huang P, Yong Y. Identification of the Facial Features of Patients With Cancer: A Deep Learning–Based Pilot Study, J Med Internet Res 2020;22(4):e17234). doi: 10.2196/17234.
[11] Wang Y, Min J, Khuri J, Xue H, Bo Xie B, Kaminsky L A, Cheskin L J. Effectiveness of Mobile Health Interventions on Diabetes and Obesity Treatment and Management: Systematic Review of Systematic Reviews, JMIR Mhealth Uhealth 2020;8(4):e15400). doi: 10.2196/15400.
[12] Trifan A, Oliveira M, Oliveira JH. Passive Sensing of Health Outcomes Through Smartphones: Systematic Review of Current Solutions and Possible Limitations. JMIR Mhealth Uhealth 2019;7,8:e12649). doi: 10.2196/12649.
[13] DeSmet A, De Bourdeaudhuij I, Chastin S, Crombez G, Maddison R, Gardon G. Adults' Preferences for Behavior Change Techniques and Engagement Features in a Mobile App to Promote 24-Hour Movement Behaviors: Cross-Sectional Survey Study. JMIR Mhealth Uhealth 2019;7(12):e15707). doi: 10.2196/15707.
[14] Ruotsalainen P, Blobel B. Digital pHealth – Problems and Solutions for Ethics Trust and Privacy. Stud Health Technol Inform. 2019; 261: 31-46. doi:10.3233/978-1-61499-975-1-31.
[15] Blobel B, Ruotsalainen P, How Does ODPR Support Healthcare Transformation to 5P Medicine? Stud Health Technol Inform. 2019; 264: 1135-1139, doi:10.3233/SHTI19403.
[16] Iwaya L H, Fischer-Hübner S, Åhlfeldt R-M, Martucci L A, mHealth: a Privacy Threat Analysis for Public Health Surveillance Systems, 2018 IEEE 31st International Symposium on Computer-Based Medical Systems, DOI 10.1109/CBMS.2018.00015.
[17] WHO Universal Declaration of Human Rights, http://www.un.who.org/en/universal-declaration-human-rights/.
[18] Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information Science 30 January 2015; 347,6221. http://science.sciencemag.org/ on February 15, 2019.
[19] Solove DJ. The End of Privacy? Scientific American October 2008, DOI: 10.1038/ scientificamerican 0908-100.
[20] Taylor K. The End of Privacy: Or Why Your Home is Not Your Castle And Your Data is not Your Own, 6 April 208, https://www.philosophytalk.org/blog/end-privacy.
[21] Rubinstein I S, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, Vol. 3, No. 2, Oxford University Press.
[22] Rubenfield J. The End of Privacy" (2008). Yale Law School, Faculty Scholarship Series. 1552. https://digitalcommons.law.yale.edu/fss_papers/1552.
[23] Marguilis ST. Three Theories of Privacy: an Overview, Chapter 2. In: Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Trepete S and Reinecke L (Eds.), Springer Verlag 2011, e-ISBN 978-3-642-21521-6.
[24] Waldman AE. Privacy as Trust. Cambridge University Press, ISBN 978-1-316-63694-7, DOI:10.1017/978136888667, United Kingdom 2018.
[25] Nissenbaum H. Privacy as contextual Integrity. Washington Law Review, February 2004; 79,1: 119-158.
[26] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[27] EU-GDPR, Art. 5, https://gdpr.eu/article-5-how-to-process-personal-data/

[28] Goecks J, Edwards KE, Mynatt ED. Challenges in Supporting End-User Privacy and Security Management with Social Navigation. Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, Mountain View, CA, USA.
[29] Taviani HT, Moore JH. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies, Computers and Society, March 2001.
[30] Davis II JS, Osoba O. Privacy Preservation in the Age of Big Data: A Survey, RAND Corporation, WR-1161 September 2016, https://www.rand.org/pubs/working_papers/WR1161.html.
[31] Kokalis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, July 2015; 64: 122-134. DOI: 10.1016/j.cose.2015.07.002.
[32] Solove D J. The Digital Person. New York University Press, 2004,ISBN 978-0-8147-4037-8
[33] Presidents' Council of Advisors on Science and Technology (PCAST), Executive Office of the President, President's Council of Advisors on Science and Technology (PCAST). The White House, Washington, DC; December 2010, Realizing the full Potential of Health Information Technology to improve Healthcare for Americans: The path forward. December, URL: www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.
[34] Balkin JM. Information Fiduciaries and the First Amendment. UC Davis Law Review, April 2016; 49,4: Paper No. 533.
[35] Dobkin A. Information fiduciaries in Practice: data privacy and user expectations. Berkeley Technology Law Journal, 2018; 33,1. DOI: https://doi.org/10.15779/Z38G44HQ8.
[36] Schwartz A and Cohn C. "Information Fiduciaries" Must Protect Your Data Privacy. Electronic Frontier Foundation, October 25, 2018
[37] McKnight DH. Trust in Information Technology. In: G. B. Davis (Ed.), The Blackwell Encyclopedia of Management. 2005; Vol. 7 Management Information Systems, Malden, MA: Blackwell, pp. 329-331. Karamitsos I, Papadaki M, Barghuthi NBA. Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, 2018; 9: 177-190. http://www.scirp.org/ journal/jis, ISSN Online: 2153-1242 ISSN Print: 2153-1234.
[38] Ruotsalainen P, Blobel B. Trust Model for Protection of Personal Health Data in a Global Environment. Stud Health Technol Inform. 2017; 245: 202 -206. doi:10.3233/978-1-61499-830-3-1.
[39] Barret L. Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries. Seattle University Law Review 2019; 42,1.
[40] Https://gdpr-info.eu/art-6-gdpr/.
[41] Laby AR. Resolving Conflicts of Duty in Fiduciary Relationships. American University Law Review 2004; 54,1: 75-149.
[42] Valsan R. Fiduciary duties, conflict of interest and proper exercise of judgment', McGill Law Journal, 2016; 62(1): 1-40. https://doi.org/10.7202/1038707ar.
[43] Enck W, Gilbert P, Han S, Tendulkar V, Chun B-G, Cox L P, Jung J, Mcdaniel P, Sheth AN. 2014. TaintDroid: An information flow tracking system for realtime privacy monitoring on smartphones. ACM Trans. Comput. Syst. 32, 2, Article 5 (June 2014), 29 pages, DOI:http://dx.doi.org/10.1145/ 2619091.
[44] Zimmeck S, Wang Z, Zou L, Iyengar, Liu B, Schaub F, Wilson S, Sadeh N, Bellovin S M, Reidenberg J. Automated Analysis of Privacy Requirements for Mobile Apps. In 24th Network & Distributed System Security Symposium (NDSS 2017), NDSS 2017, San Diego, CA, 2017. Internet Society. URL