Journal of *Personalized Medicine*

Article

Future pHealth Ecosystem-Holistic View on Privacy and Trust

Pekka Ruotsalainen [1,*] and Bernd Blobel [2]

[1] Faculty of Information Technology and Communication Sciences (ITC), Tampere University, 33100 Tampere, Finland
[2] Medical Faculty, University of Regensburg, 93053 Regensburg, Germany; bernd.blobel@klink.uni-regensburg.de
* Correspondence: pekka.ruotsalainen@tuni.fi

Abstract: Modern pHealth is an emerging approach to collecting and using personal health information (PHI) for personalized healthcare and personalized health management. For its products and services, it deploys advanced technologies such as sensors, actuators, computers, mobile phones, etc. Researchers have shown that today's networked information systems, such as pHealth ecosystems, miss appropriate privacy solutions, and trust is only an illusion. In the future, the situation will be even more challenging because pHealth ecosystems will be highly distributed, dynamic, increasingly autonomous, and multi-stakeholder, with the ability to monitor the person's regular life, movements, emotions, and health-related behavior in real time. In this paper, the authors demonstrate that privacy and trust in ecosystems are system-level problems that need a holistic, system-focused solution. To make future pHealth ethically acceptable, privacy-enabled, and trustworthy, the authors have developed a conceptual five-level privacy and trust model as well as a formula that describes the impact of privacy and trust factors on the level of privacy and trust. Furthermore, the authors have analyzed privacy and trust challenges and possible solutions at each level of the model. Based on the analysis performed, a proposal for future ethically acceptable, trustworthy, and privacy-enabled pHealth is developed. The solution combines privacy as personal property and trust as legally binding fiducial duty approaches and uses a blockchain-based smart contract agreement to store people's privacy and trust requirements and service providers' promises.

Keywords: privacy; trust; holistic view; fiducial duty; privacy law; smart contract

Citation: Ruotsalainen, P.; Blobel, B. Future pHealth Ecosystem-Holistic View on Privacy and Trust. *J. Pers. Med.* **2023**, *13*, 1048. https://doi.org/10.3390/jpm13071048

Academic Editor: Yi Guo

Received: 10 May 2023
Revised: 18 June 2023
Accepted: 21 June 2023
Published: 26 June 2023

1. Introduction

Nowadays, we live in almost borderless digital environments where products are increasingly interchangeable with intellectual and informational goods and services [1]. They also require the availability of "Big Data" related to human's experiences, relationships, behaviors, and environments. Novel health service models such as tele-health, mHealth, pHealth, eHealth, and digital health are examples of those services. pHealth focuses on personal/personalized health and health care services, and it presents a horizontal view of health care, eHealth, and mHealth [2]. Modern pHealth services are data-driven and vary in focus and size. The pHealth service can be a sensor system that is focused on a dedicated personal health or wellness problem, or it can be a personal health recommender system using a holistic view of a person's health [3]. Nowadays, pHealth services are increasingly part of a dynamic, multi-stakeholder, cross-organizational, cross-border, and cross-jurisdictional ecosystem. In pHealth, technological innovations have always been adapted on the front lines. Currently, the deployment of smart sensors, mobile devices, wireless networks, web technologies, digitalized services, Cloud platforms, algorithms, artificial intelligence (AI), machine learning (ML), and blockchains for online personalized health services is common. Ongoing paradigm shifts in health care from organization-centered and reactive healthcare to person-centered preventive and predictive care are well adapted in pHealth [4].

Today's information technology enables Web sites, computer applications, and networks to routinely collect, use, store, and share all kinds of personally identifiable information (PII) about a person's health problems, including health-related information about the person's life. Modern sensors, wearables, and smart wrists have the ability to measure a person's physical activity, blood pressure, heart rate, quality of sleep, social activities, stress, emotions, and mood [5]. Furthermore, behavioral activities are invisibly tracked online when using computers, mobile phones, and health services via networks [6,7]. According to Zuboff, almost unlimited data collection and surveillance are daily practices in the digital age [8]. Video surveillance systems in public spaces can monitor our social and health-related behaviors. Data analytics companies both sell our raw data and use our PII in the form of behavioral profiles and predictive products [9].

The Internet of Things (IoT) and artificial intelligence of things interfaces (AIoT) are new emerging technologies that enable real-time data collection. According to Ziegeldorf et Al., the IoT moves the collection of personal data and behaviors from the internet and public spaces to homes and working places [10]. The novel neurotechnology has the ability to go even further. According to Berger et al., it can impact technology indirectly through wearable devices that read data from the head and also write data using neuromodulation. According to Berger et al., in the future, neurotechnology may have the ability to influence people's behavior, emotions, values, and thoughts [11].

During the last few years, both the public sector and private organizations have shown increasing interest in the collection and use of personal health data for innovations, new products, and services, and they have built technology environments such as ecosystems where services offered are dependent on the collection of PHI, users' behaviors, and interactions [12]. This development has raised the question of the ownership of PHI and whether or not health data should be understood as a public good (a commodity produced without profit for all) or personal property [13]. Currently, there is no unanimous answer to this question. According to Piasecki et al., the ownership concept cannot solve problems associated with the sharing of PHI [14]. In a workshop report, Crossmann et al. summarize that health care data should be established as a public good [15]. Taylor sees that nowadays, data as a public good model fits best with corporate reality and existing models for data sharing [16]. On the other side, propertization of personal information, according to Schwarz, responds best to people's concerns about privacy [17]. The new European Health Data Space proposal goes even further by considering health data according to the common good model. In this proposal, health data is understood to include not only EHR and clinical trials but also the content of PHR and personal wellness data [18].

These days, the Internet brokers and data giants have well understood the commercial value of health data and the potential of AI and have adapted and established the business model of data collection and commercialization [19]. Increasing commercialization of PHI is a big problem for human rights, and it raises the danger that, in the future, expected economic benefits will override people's needs for privacy and autonomy. It is notable that the United Nations has confirmed that privacy remains a human right even in the digital age, and "sharing health data as a public good requires making data available with the right degree of openness or restriction to achieve maximum benefit, while reducing any potential for harms" [20]. It is evident that privacy is a big problem in real-life networks and ecosystems [21]. Therefore, information privacy is inevitable in the digital age [22]. Researchers have shown that traditional security-based privacy protection solutions cannot guarantee privacy, and a person cannot control the collection, use, and sharing of his or her personal information (PII) in today's networked information systems [2].

Building trust in a dynamic ecosystem is a big challenge for the service user. In today's information systems, it is widely expected that people blindly trust organizations' and service providers' promises that they process PII fairly. In other words, it is expected that a service user believes without any proof that structures such as guarantees, regulations, promises, legal recourse, and procedures are in place (i.e., structural assurance) and that the environment is in proper order (i.e., situational normality) [23]. Unfortunately, researchers have shown that in real life, this is far from true. And in dynamic multi-stakeholder ecosystems, it is almost impossible to know who and why to trust [24]. Furthermore, researchers have observed that digital information systems are seldom designed with privacy in mind, i.e., in today's digital information systems, trust is only an illusion [25,26]. As pHealth services are built over the same general ITC technology used in commercial information systems and platforms, they share the same privacy and trust concerns [26–29]. It is a specific feature of pHealth ecosystems that some of the stakeholders can be non-regulated health care providers or private organizations. This means that parts of personal health information (PHI) collected and used are not regulated by health care-specific laws. Together with the sensitivity of PHI collected and used, this raises additional privacy concerns, especially because the content and implementation of privacy laws vary in different countries [30].

The future of pHealth has the potential to offer personalized, preventive, and predictive services to its service users. However, for it to be successful, it needs a huge amount of PHI and health-related personal behavioral data covering a person's regular life, social relations, economic activities, and psychological status [2]. This data (i.e., personal big health data) can be used for different analyses, to calculate detailed personal health profiles, to detect changes in personal health and disease, and to develop new applications such as personal health recommendation services [3]. According to researchers, future pHealth will rely on Internet of Things (IoT)-based data collection and advanced computer methods such as machine learning (ML), artificial intelligence (AI), and deep learning (DL) [27,29,30]. It is evident that in the future, pHealth privacy and trust challenges will be much bigger than they are today. To realize even a part of the promises of data-driven pHealth (e.g., innovations, new products, better health, and economic growth) and to prevent short- and long-term negative consequences for human values such as privacy, dignity, integrity, and autonomy, it is necessary to find new solutions for privacy, trust, and ownership of PHI.

This paper is an extension of the work originally presented to the pHealth 2022 Conference [2]. In that paper, the authors have studied methods and solutions that have the ability to prevent the situation where PHI can be invisible collected, shared, and misused, where there is no information privacy, and where predefined trust in technology and service providers' fairness is just expected [22,27]. As healthcare-specific laws and general privacy regulations grant several rights to the data subject (e.g., access to their own health data, rectification, objection, data portability, and the right to block data sharing), this paper is focused on the collection, processing, storage, and sharing of PHI that takes place outside the health care domain and medical research [31]. The authors' starting point is that future pHealth should be ethically acceptable, trustworthy, and empower the service user or data subject (DS) to maintain information privacy by expressing their own privacy needs and expectations. For future pHealth, potential ICT solutions and their weaknesses are discussed, and the authors also propose a holistic set of principles and solutions that, when used together, have the power to make future pHealth ethically acceptable and trustworthy.

The rest of the article is organized as follows: Chapter 2 briefly summarizes the main features of widely used privacy and trust models and the principles of information ethics. In chapter 3, the authors define how the pHealth ecosystem is understood in this paper and present a user's view of it. In Chapter 4, privacy and trust challenges existing in current pHealth ecosystems are discussed. Then (Chapter 5), features of new privacy and trust approaches developed by researchers are analyzed. In chapter 6, a five-level holistic model and a formula describing factors that influence the level of privacy and trust in an ecosystem are presented. In Chapter 7, the authors propose a holistic solution for a trustworthy, privacy-enabled, and ethically acceptable pHealth ecosystem. Chapter 8 covers the limitations of this paper and outlines the necessary future steps needed to reach the authors' goal.

2. Privacy, Trust and Information Ethics

Privacy and trust are vague, dynamic, situational, and context-dependent concepts with many definitions [2,27,32]. Almost all cultures value privacy, but they differ in how they obtain it [33]. It is widely accepted that privacy is a human and constitutional right [34]. Information privacy is a subset of the concept of privacy [35]. According to Floridi, two theories of information privacy are popular: the reductionist interpretation and the ownership-based interpretation. The first theory looks for undesirable consequences caused by the misuse of data, and the second theory defines that a person owns his or her information (privacy is defined in terms of intellectual property) [36]. According to Smith et al., the person who owns PII can also trade privacy for other goods or services [37]. For Decew, privacy is a common value because all individuals value some amount of privacy [33].

At a general level, privacy addresses the question "what would we like others to know about us". In western countries, privacy is widely based on concepts of autonomy and informational self-determination, which refer to a person's right and expected ability to control the flow of his/her own personal information. This implies that a person has the right to control when, by whom, and why personal information is collected and shared, and to protect himself/herself against surveillance, unnecessary data collection and processing, dissemination, unauthorized use, and harm caused by the unfair use of PII [38–40].

Other widely used privacy models are privacy as a concern, legal construct, risk-based concept, behavioural concept, and social good [27,41,42]. The concept of privacy as a commodity understands privacy as an economic good that can be traded. The privacy as a concern approach refers to individuals' anxiety regarding the collection, processing, and unfair use and sharing of data. Privacy as a regulative (legal) construct tries to regulate the way data is collected, used, and shared [43]. The risk-based approach to privacy focuses on risks such as harm caused by unnecessary data collection, misuse, disclosure, surveillance, and behavioral manipulation [44,45].

In real life, the nature of privacy and the lack of availability of reliable privacy related information make the measurement of the actual (objective) level of privacy challenging [45]. Furthermore, researchers have found that privacy preferences vary drastically from individual to individual. They can change over time and are context-dependent [46]. Furthermore, in many countries, privacy is not an absolute right. Instead, it can be balanced with, or overridden by, others' concerns and priorities, including business needs, public safety, and national security. According to Friedewald, the right to privacy requires a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions [22]. A meaningful challenge is that, while technical solutions provide some protection against data misuse, the existence of such protection does not necessarily mean that users will disclose more information [47].

Some researchers have pointed out that current privacy models do not work in distributed and digital information systems, and there is a need to redefine how we understand privacy [21,48]. Furthermore, Friedewald has proposed that in the digital age, the concept of privacy should be expanded to include the following aspects: privacy of the person, privacy of personal behavior and actions, privacy of personal communication, privacy of data and images, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy) [22].

According to Sætra, an individualistic model of privacy is insufficient, and privacy should be understood as a public good, i.e., everyone in a society should have the right to enjoy privacy [49]. DaCosta has proposed a novel privacy-as-property approach. Its fundamental idea is that "you have the right to control yourself, and this property interest in oneself extends to the external objects you own, including your data" [50]. Acquisti et al. have proposed that in the digital age, privacy should include not only personal data but also behaviors and actions, personal communication, thoughts and feelings, and associations [51].

Traditionally, trust is understood to exist between persons; however, researchers agree that trust is also needed between a person and an organization (organizational trust) and between a person and technology (trust in technology) [29]. Trust is needed in situations where the trustor has insufficient information about the features and behavior of the trustee [52]. Therefore, to build a relationship of trust, there must be confidence that the other partner will act in a predictable manner [39]. Trust can also be defined as a personal expectation of other partners' future behavior [53]. Trust is widely understood as a disposition, attitude, belief, feeling, expectancy, psychological state, personal trait, social norm, subjective feature, willingness to be vulnerable, and perception based on one's own previous experiences or others' recommendations. Trust has been understood as the willingness to depend on other parties expected or unexpected actions without the ability to monitor or control them [54]. Perceived trust is a personal opinion based on information gleaned from one's own senses or from others. Computational trust is an algorithmic imitation of human-based measured features of the trustor and the used information system. Thus, trust is often based on emotions or feelings, which also include cognition. According to Ikeda, trust can be based on justifiable reasons such as laws and science [55]. That kind of trust, aka "rational trust" is based on rational arguments [56]. In the case of rational trust, the trustor should have facts on which the trust is based [57].

In digital information systems, people should increasingly trust technology. According to Mc Knight, trust in technology is often a belief that the technology used is reliable, secure, and protects information privacy, and that appropriate governance is established and enforced [58]. Furthermore, the level of trust depends on the understanding of the system and its behavior, i.e., the system's willingness and ability to correctly perform [59].

Ethics is a set of principles and concepts that judge whether a behavior is right or wrong. The basic principles of general ethics are autonomy, justice, non-maleficence, privacy, and solidarity. Normative theories of ethics include consequence-based theories, duty-based theories, rights-based theories, and virtue-based theories to guide how to interact properly with others [60]. Information ethics (which is closely related to computer ethics) is an applied ethics that focuses on the relationship between the creation, organization, dissemination, and use of information and the ethical standards and moral codes governing human conduct in society [61]. Information ethics intertwines with other areas of applied ethics such as computer ethics, data ethics, internet ethics, engineering ethics, and business ethics. In this paper, the authors emphasize that information ethics covers not only humans but also any actor in the ecosystem, such as applications and technologies, including implantable and wearable devices. As today's networked information systems, or more generally, ecosystems, impact human values such as life, health, happiness, freedom, knowledge, resources, power, and opportunity in many ways, researchers have highlighted that information systems should function in an ethically acceptable way [62]. The European Union has proposed the following ethical principles for information systems using AI: The system must not negatively affect human autonomy, violate the right to privacy, or directly or indirectly cause social or environmental harm to an individual. Instead, the system should support freedom and dignity. Furthermore, the AI system should be accountable and transparent to its stakeholders and end-users [63]. The authors state the above-discussed ethical principles as mandatory for all information systems processing PHI.

3. User View on Privacy and Trust in pHealth Ecosystems

The concept "ecosystem" was originally developed in the fields of ecology and biology [64]. Today, it is transferred to many other contexts and widely used in the field of information science to describe networked communities consisting of interconnected and interrelated technical and non-tangible elements [54]. Typical non-tangible elements are data, digital services, and stakeholders. Technical elements include networks, platforms, programs, and communication lines. Architecture presents its structure, function, and relations [64]. The goal of the ecosystem is to create value for all stakeholders [64]. A pHealth ecosystem is typically a socio-technical system that is characterized by its stakeholders' business models, roles, and relations, its services and products, information flows, the information itself, and the underlying infrastructure [65]. Nowadays, pHealth ecosystems are increasingly platform ecosystems. In the pHealth ecosystem, there can be conflicting objectives; e.g., stakeholders want to maximize their profit by collecting and using a maximal amount of PHI, and users try to minimize short- and long-term harms through disclosed data while at the same time getting benefits from services. In pHealth ecosystems, a service user typically has a direct connection to one service provider. On the other hand, other parts of the ecosystem, including its other stakeholders, architecture, deployed privacy technology, regulations, business goals, and relations, are usually invisible to the service user, i.e., the ecosystem looks at the service user as a black box (Figure 1).

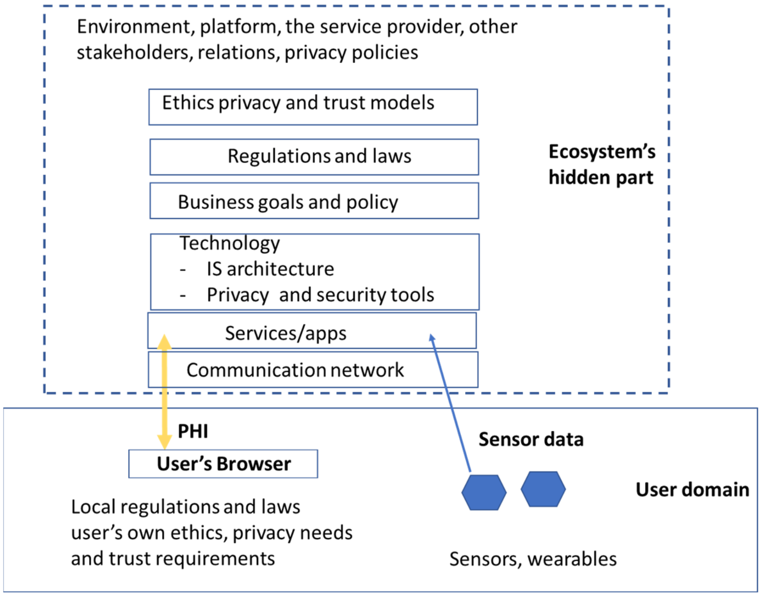
Environment, platform, the service provider, other stakeholders, relations, privacy policies
Ethics privacy and trust models
Regulations and laws
Business goals and policy
Technology
- IS architecture
- Privacy and security tools
Services/apps
Communication network
Ecosystem's hidden part
PHI
User's Browser
Sensor data
User domain
Local regulations and laws user's own ethics, privacy needs and trust requirements
Sensors, wearables

Figure 1. Users' view on pHealth ecosystem.

This means that the service user is strongly dependent on the service provider's willingness to use and share the service user's PHI ethically and fairly. The service user cannot build trust in the pHealth ecosystem and make privacy-based decisions without sufficient information about the ecosystem's invisible features, which the service provider should make available. According to Dobkin, service providers who collect and utilize user data are fiduciaries to customers [66], and the information fiduciary duty of service providers could ensure that they use data only in ways that are consistent with users' expectations [67]. This implies that there exists a specific informational and fiducial relationship between the service user and service provider in pHealth ecosystems. Thereby, the service provider has an obligation to act in the best interests of the service user.

4. Privacy and Trust Challenges in pHealth Ecosystems

When we currently use information systems, we leave trails that expose our interests and traits that expose our actions, beliefs, intentions, and targets of interests to commercial entities and also to our governments [51]. On the Web, there are tens of thousands of health apps collecting and using PHI [32]. In today's information systems, a person's behavioral health data is systematically and secretly collected by Web service providers, health apps, and Web platforms. According to Dobkin et al., at least 77.4% of Websites globally track visitors' data and people's behavior [66]. Zuboff has noted that behavioral tracking is not only used to measure body signals but also our physical and social behaviors and how we use information systems [8]. Therefore, persons do not have sufficient knowledge of what information other people, organizations, and firms have about them, by whom and how that information is used, and what the consequences are for the data subject (DS). This situation is often described by decision-makers and firms as a win-win situation, i.e., people, organizations, firms, and society benefit from data sharing. Unfortunately, in real life, benefits to a person are often only promises or beliefs, and invisible data collection and sharing not only breaches trust and privacy, but it can also generate harm to the person.

Researchers have shown that traditional privacy solutions such as notification and choice (consent) as well as fair information processing principles have failed to guarantee privacy in today's networked environment. Although the new privacy regulations, such as the EU-GDPR, oblige companies to specify how the collected data is used, in real life, organizations' privacy policies (if available) are written in a legalistic and confusing manner and are difficult to understand and use [68]. For the same reasons, transparency in the form of an organization's privacy policy does not work well. Furthermore, many big Web actors and service providers simply do not care about privacy laws [45,69]. Finally, the service user's privacy decision takes place in a complex, multidimensional situation, and his or her bounded rationality makes rational privacy choices difficult [70].

Currently, most Web services are free of charge for the consumer, but in real life, people are paying for the use of services through disclosed PII (i.e., PII is traded and monetarized). The option of buying an application with the option of not disclosing personal information to the company, which may subsequently sell that data, does not exist [68]. Service providers and platform managers often expect that they can freely use and sell disclosed data [2]. Service providers are also prioritizing their business needs and benefits over service users privacy needs. There is also a tension between public and commercial interests in collecting and using PII on the one hand and people's needs for privacy on the other. Industry widely sees personal information as raw material for products and services and society as a public good. This makes it challenging to balance a person's individual need for privacy on the one hand and the use of PII for meaningful public benefits or for making profit on the other [27].

The unlimited collection of a person's behavioral data is a big problem in today's digital information systems. Behavioral data talks about our routines, habits, and medical conditions. Behavioral data can also be used to uniquely identify individuals [71] and web-browsing behavior [72]. Another problem is that in ecosystems, the DS cannot know how data will be used in the future, what its potential uses are, or whether other people's PHI will be linked to it [73].

Lack of trust is also a meaningful problem in ecosystems, where the user has to trust not only the service provider but also other frequently unknown stakeholders and surrounding information technology. In ecosystems, the service user does not have reasonable knowledge of stakeholders' trust features and relations and has no power to negotiate privacy rules and safeguards or force the service provider or platform manager to take personal privacy and trust needs into account [2]. Instead, the service user is typically forced to accept a service provider's privacy promises (policy) and trust manifesto in the form of a take-it-or-leave-it approach [66]. Unfortunately, commercial service providers often have low incentives to enforce strong privacy policies, and they often do not keep the privacy promises expressed in their policy documents [73,74]. This all indicates that policy-makers and technology firms fail to provide the user with reasons to trust, and codes of conduct and privacy policies will not provide sufficient reasons to trust [75].

As discussed earlier, the vagueness of privacy and trust concepts makes it difficult to conceptualize and measure them and to make them understandable for computer programs. To solve this problem, different proxies such as service level agreements, external third-party seals, service provider's privacy policy documents, reputation, direct observations, and degree of compliance with laws or standards have been used instead [27]. Preserving behavioral privacy requires more sophisticated approaches than just removing direct identifiers (IP address, social security number (SSN), blurring a face) or intuitive quasi-identifiers (gender, age, ethnicity) from databases [72].

Consequently, a person today has just a few or no possibilities to maintain privacy in networked information systems, and therefore just a few reasons to trust. According to Goldberg, the service user can only use feelings or personal opinions as measures of the level of privacy and trust [39], reject the use of the service, filter the amount of PII he or she is willing to disclose, or add noise to data before disclosure [76]. This all indicates that the current situation is unsatisfactory.

5. Novel Approaches for Privacy and Trust

As discussed earlier, current privacy and trust models and solutions are insufficient to provide an acceptable level of privacy in networked and highly distributed information systems. Furthermore, a service user has few or no reasons to trust the service provider or the ecosystem as a whole. To solve these problems, researchers have created different privacy and trust approaches and solutions. Most of them focus on reducing the negative consequences of the use and sharing of personal information by offering more control and the possibility of using computer-understandable policies. There are also solutions, providing insight that the control model and the use of consent are inadequate and that a more radical solution is needed (Table 1).

Table 1. Examples of new privacy and trust approaches and solutions.

Approach	Examples of Solutions
More personal control Transparency	Privacy nudges User tailored privacy Personalized privacy Person/Patient controlled or PHR Personal privacy policies Explainable trust
Ownership model	Privacy as intellectual property
Duty based model	Informational duties Trust as duty
Regulatory model	Trust as legal binding duty Accountability Privacy risk analysis
Computational models	Calculated level of privacy Calculated trust
Contractual models	Privacy negotiation Smart contract
Cryptographic based models	Blockchain Differential privacy Homomorphic encryption
Obfuscation methods Disclosure limitation	Data hiding by masking Adding noise or laying
Architectural solutions	Edge/Fog computing Federated learning
Ethics based approaches	Ethical design Ethical agents
Distributed trust approaches	Blockchain

The aim of the privacy as control approach is to give the DS or service users more control over what data they wish to share with whom and how and for what purposes the data can be used. Privacy nudges offer the person a ready-made template to make personal choices. On the other side, it is only a normative "one-size-fits-all" solution to make normative assumptions about the value of privacy [77]. User-tailored privacy solutions offer the user more flexibility by automatically tailoring IS's privacy settings to fit the user's privacy preferences [78]. As AI applications have the ability to predict a user's privacy preferences by determining privacy needs based on the user's previous data sharing history, AI can be used to contextually tailor a user's privacy needs.

The person-controlled EHR (Electronic Health Record)/PHR (Personal Health Record) approach gives a person full control over his/her own PHI (e.g., the person grants or rejects granular access to the stored PHI in a context). Typically, rules that are expressed in the form of personal policies and data encryption methods are used together. The encrypted data can be stored on a blockchain [79]. Yue et al. have proposed a person-controlled blockchain solution that enables the patient to own, control, and share their own data securely without violating privacy [71].

Computational privacy models use mathematical methods to calculate the level of privacy using measured attributes and mathematical methods. According to Ruotsalainen et al., computational privacy offers a better approximation for the actual level of privacy than risk probabilities and privacy perceptions [48]. A contractual agreement, such as a legally binding service level agreement (SLA), is widely used between organizations. Ruotsalainen et al. have proposed the use of legally binding digital (Smart) contracts between the pHealth customer and service provider [27,80]. A smart contract is a set of rules that can be executed in a network of mutually distrusted nodes without the need for a centralized, trusted authority [81]. To guarantee the integrity, availability, and non-repudiation of the contract, it can be stored on a Blockchain. In a smart contract, the service user's personal privacy policy is part of the contract between the person and the pHealth service provider. The personal policy can regulate not only how the service provider uses PHI but also the sharing and secondary use of PHI in the ecosystem [54].

New cryptographic solutions such as encryption, differential privacy, k-anonymity, and homomorphic encryption offer ways to maintain privacy. Homomorphic encryption allows some calculations with the data without decryption [82]. Architectural solutions such as edge-and-fog computing can also support privacy. The edge consists of human-controlled devices, such as PCs, smart phones, IoT devices, personal health devices, and local routers [83]. In edge computing, the processing of sensitive data takes place at the local level, and the Edge router controls the data flow between the edge domain and other worlds [84].

Some researchers have stated that the current privacy and trust models are unsatisfactory and that a radical (paradigmatic) change is necessary [54]. According to Ritter, today's highly distributed information systems, such as ecosystems and the Internet of Things (IoT), have raised legal questions such as who is the owner of PHI and behavioral personal data by defining a new class of property by legislation [85]. He also noted that today's defensive privacy laws should be expanded to support new contractual models such as smart contracts, and the consumer should have a veto right concerning privacy [85]. Another radical solution is to make the person the legal owner of his or her PHI. This informational property rights model gives the person the power and ability to define how and by whom PHI is used. According to Samuelson, the informational property rights model empowers individuals to negotiate with organizations and firms about how data is used [86]. Koos has proposed a variant of this model where the PHI can be licensed by the customer [87]. Ruotsalainen et al. have proposed PHI as a personal property model, where a person defines policies for the use and sharing of PHI in the ecosystem [27]. To be effective, the property model requires legal support [85]. The property model can also be expanded to cover a person's behavioral data.

Trust creation by information and explanations regarding how information systems function seems to make information systems more trustworthy [88]. Challenges in this transparency model are the lack of reliable information about system trust features and the fact that explanations and increased information overload the user in a situation. To outweigh this, Ruotsalainen et al. have proposed for pHealth the use of a computational trust model that is based on information about the ecosystem's measured/published features. In this solution, a Fuzzy Linguistic method is used to calculate the merit of service (fuzzy attractiveness rating) for the whole ecosystem [48]. Depending on the quality of the available attributes (i.e., attributes should be measurable if possible), this model can support the idea of building rational trust.

A radical approach is the use of the concept of informational duties instead of privacy. Information duties imply that individuals and institutions acting as data controllers or processors have specific information duties towards data subjects [89,90]. For privacy, Balkin has proposed the deployment of the concept of information fiduciary as a specific duty [67]. Fiduciaries must act in the interests of another person, i.e., a fiduciary has a responsibility to accept and act based on privacy needs expressed by a person. Fiduciaries also have obligations of loyalty and care toward another person and the responsibility not to do harm [67]. Therefore, according to Barret, the information fiduciary model has the power to strengthen equality and autonomy in the digital society and to offer better privacy protection [91]. According to Dobkin, the principle of the information fiduciary should be legally imposed as a duty in digital information systems [66].

The fiduciary relationship, as a legal duty, can also be used as a trust builder. According to Mayer, trust in fiduciary relationships is based on the professional's competence and integrity [92]. Waldman sees that privacy in an information-sharing context is a social construct based on trust. He has proposed for privacy the privacy as trust model. According to Waldman, privacy as trust creates a fiduciary relationship between data subjects and users. In this approach, a private context is also a trusted context [38].

Blockchain technology can be used as a trust builder because it offers decentralized trust. In blockchain, people do not need interpersonal trust, but users must trust mathematics, algorithms, and indirectly, the creators of the blockchain system [93].

In an ecosystem, a single privacy or trust solution alone is hardly a silver bullet, and the combination of different methods shown in Table 1 offers a better solution. Ruotsalainen et al. have developed a solution that combines privacy as a personal property model, trust as a fiducial duty, a legally binding smart contract, and blockchain-based repositories for pHealth [27]. Thereby, the smart contract is a digital SLA agreement the service provider has a legal duty to follow.

As already mentioned, the information processing in the pHealth ecosystem should be ethically acceptable. Therefore, pHealth information systems should be compliant with the principles of information ethics (non-maleficence, beneficence, justice, and respect for autonomy). Hand has proposed a solution for an ethical information system that is based on the following ethical principles: integrity, honesty, objectivity, responsibility, trustworthiness, impartiality, nondiscrimination, transparency, accountability, and fairness [94].

6. A Holistic View to Privacy and Trust in pHealth Ecosystems

As discussed in earlier chapters, the authors expect that future pHealth will be part of a highly distributed and dynamic multi-stakeholder ecosystem, i.e., an information system that collects and shares all kinds of PHI and intensively uses AI, ML, and DL for detailed personal health analysis. In an ecosystem, some stakeholders can be virtual; PHI and results are shared not only between the user and the service provider but increasingly with other stakeholders across contexts and jurisdictions [2]. Furthermore, stakeholders in the pHealth ecosystem often have different business and privacy policies as well as trust features. To dare to use offered services, the user needs to know the aggregated level of privacy and reasons to trust not only a service provider but the ecosystem as a whole. In this chapter, the authors create a holistic solution to this challenge.

According to Holt et al., in modern highly distributed ecosystems, infrastructure, policies, citizen rights, national and international regulations and laws, as well as cultural preferences and corporate policies, make the maintenance of privacy and trust an extremely complex task [95]. Elrik has noted that ecosystem interrelations between members define how the ecosystem works, and a holistic approach to privacy is needed [96]. The authors state that in future pHealth ecosystems, privacy and trust cannot be built using a single method or solution. Instead, a holistic, systemic view is needed. Furthermore, for privacy and trust, a user-centric approach should be used [47].

For the future pHealth ecosystem, the authors have created a holistic, six-level, user-centric conceptual model (Figure 2). This model also supports the idea of explainability, i.e., that service users of the ecosystem should understand how their PHI is processed and used and how their privacy and trust needs are implemented by different stakeholders. The authors also expect that explainability fosters trust in the ecosystem [97].

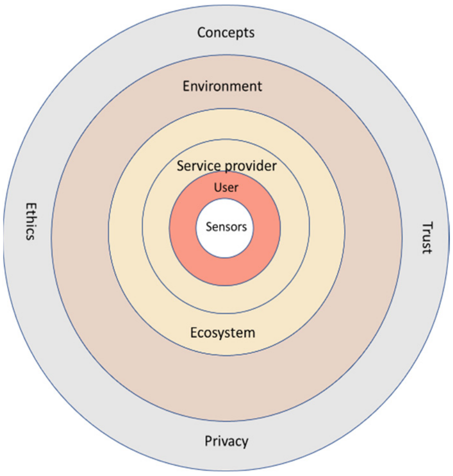

Figure 2. User centric five-level conceptual model for future pHealth ecosystem.

For each level of the conceptual model, the authors have analysed from the user's point of view the privacy and trust challenges and their possible solutions. The content of Table 2 creates a holistic view of privacy and trust in a future pHealth ecosystem.

Using the "Conceptual Model of Everyday Privacy in Ubicompo" developed by Lederer et al. [98], as a starting point, the authors have conceptualized the influence of privacy and trust factors discussed in Table 2 and developed the following formula:

$$\text{Level of privacy and trust} = \text{f}\ (\text{M, E, Te, IA, SR, SP, KN, USPr, USPt, DS}) \tag{1}$$

where

M = Models for ethics, privacy, and trust
E = Environment (e.g., Laws, regulations, standards) [98]
Te = technology (e.g., safeguards, encryption) [99]
IA = Information architecture [98,100]
SR = stakeholders' privacy and trust features and their relations [48]
SP = service provider's privacy and trust features (attributes) [48]
KN = knowledge [101]
USPr = service user's privacy needs
USPt = service users trust requirements and trust threshold
DS = sensitivity of data [98].

Using the analysis made in the previous chapter and the content of Table 2, the authors have also developed a proposal for an ethically acceptable, trustworthy, and privacy-enabled pHealth ecosystem. Concerning the ethical model, the authors state that consequentialism (i.e., consequences to a person caused by the collection, use, and disclosure of PHI) alone is insufficient for future pHealth. Instead, the authors propose that a combination of consequentialism, duty ethics, and utilitarianism (i.e., the use of PHI should be available to improve the population's health) should be used in the environment. Furthermore, the privacy as personal property model is proposed to be used. This implies that the DS or service user has legal ownership of their own PHI, including personal health behaviors.

Table 2. Holistic view to privacy and trust in a future pHealth ecosystem.

Levels	Content	Possible Solutions	Challenges
Concepts and models	Ethical model, principles and values	Consequentialism Utility or duty ethics.	Stakeholders’ ethical models, values and principles are seldom known
	Trust model	Trust as informational duty Computational trust	Stakeholders’ privacy and trust models used are not known Stakeholders do not do what they have promised in privacy documents
	Privacy model	Privacy as property Personal tailored privacy	Privacy and trust responsibilities are often unclear
Environment	Laws, standards and Golden Rules	New laws needed to: -Force transparency of privacy and trust features -Strengthen the role of person -Restrict hidden collection of the PHI	Ecosystem is highly distributed and cross-border Conflighting laws and privacy and trust models Laws should be global
Ecosystem	Stakeholders’ relations and privacy and trust features.	Transparency of business and privacy policies, stakeholders’ relations, and features.	Stakeholders’ business and policies vary. Stakeholder´s relations, privacy and trust features of information systems are not known
	ICT-architecture and technology	Edge and blockchainb architectures Federated computing	Management of encryption keys Regulatory compliance and accountability.
The service provider	Business model, Privacy policy Trust features of processes and applications	Data encryption	DS´s policy and stakeholser´s business policy can be conflighting Measurements of possible harm and the level of trust and privacy
User/DS (Physical view)	Users and the DS personal privacy and trust models. Expression of user´s privacy and trust needs	Personal privacy policies Tools to collect data and calculate the actual level of trust and privacy Evaluations of expected benefits and possible harms. Smart contracts Data encryption	No reason to trust Lack of: -Privacy and trust related data -Regulatory support -Practival tool for privacy management -Power to make contract ór negotiate No audit trails
Data and sensors (perception)	Raw data from sensors Self-disclosed PHI	Lite point-to point- encryption of data at sensor level	Data integrity, reliability and availability Lack of computational power for encryption

As the service user in the pHealth ecosystem is fully dependent on service providers’ fairness and knowledge concerning privacy and trust features of the ecosystem (Chapter 3), the authors propose for the trust model a solution where trust is a legally binding fiducial duty. Thereby, the service provider and other stakeholders have the legal duty not to prioritize their own business benefits but to take into account service users privacy needs [2,27]. It is also necessary that the service provider publish not only the trust and privacy features of its own information system but also proof of accountability. For this purpose, the service provider must enable the service user to access the audit trail concerning the use of collected PHI. New laws are also needed to strengthen the position of the service user. First, a transparency law is inevitable, which enables the service user to know how and by whom his or her PHI is collected and used and to be aware of what behavioral health data is collected. Secondly, a law for privacy as informational property and a law that supports legal, binding smart collection contracts are needed. The service user should have the choice of a paid pHealth application without health data collection and behavioral tracking.

New information architectures, such as blockchain-based information systems and edge architecture, offer increased privacy compared with currently widely used Cloud platform solutions. Therefore, they are good candidates for future pHealth systems. Federated learning (FL) is another interesting architectural solution. Encryption as a default principle should be used everywhere where it is possible (e.g., homomorphic encryption or differential privacy).

7. A Proposal for Privacy Enabled and Trustworthy for pHealth Ecosystem

Based on previous analysis and the holistic view (Chapter 6), the authors have developed a proposal (an example) of how a high level of privacy and trust can be reached in the pHealth ecosystem. It is assumed that any person has the right to control themselves, including data that describes their own thoughts, behaviors, emotions, values, and personal health-related information [50], and privacy is understood as the amount of power a person has against others control and manipulation over them. The proposal is called a hybrid solution by the authors because it is not aimed at superseding current general privacy protection laws such as the EU GDPR and laws regulating the collection and use of clinical data in health care. The authors' proposal combines PHI as personal property, trust as a fiduciary duty for the service provider and other stakeholders processing PHI in the ecosystem, and a legally binding smart contract that is stored in a blockchain-based repository [27,102]. Property is a special personal property that cannot be traded to any private organization and is not monetarized [103]. Property is an allocation of power to the DS to define what is a fair collection and use of data and how PHI can be used and shared. This power also enables the DS to exclude others [104]. The property should be supported by a new property law. Other elements in this proposal are transparency, edge architecture, data encryption at the sensor, and communication levels.

8. Discussion

Even though information privacy and a high level of trust are prerequisites for successful pHealth, researchers have shown that in ecosystems, current privacy approaches and solutions do not offer a level of privacy acceptable for the service user, so trust is just an illusion. This indicates that future pHealth cannot be built on current privacy models and technology [27]. Furthermore, even the most modern privacy laws, such as the EU-GDPR, rely on insufficient privacy as the notice and choice concept (aka consent model) and on risk analysis that is inadequate in a future pHealth environment [105,106]. Concerning trust, service users are widely expected to blindly trust companies' promises [75]. This all means that, until today, policy makers and technology firms have failed to provide people with reasons to trust information systems and have left users of digital networks and services vulnerable. There are many new technical, architectural, and mathematical privacy and trust solutions, but the authors state that none of them alone is sufficient because privacy and trust in ecosystems are interconnected and holistic system problems.

In this paper, the authors have developed a user-centric five-level conceptual model for privacy and trust in the pHealth ecosystem and a formula for its privacy and trust factors. For each level of the model, the authors have analysed privacy and trust challenges and their possible solutions. The results are shown in the template to provide a holistic view of privacy and trust. The template and the formula have many use cases. The service user can use them to evaluate the level of privacy and trust in pHealth. Furthermore, the service provider can use the template and formula to assess what knowledge should be disclosed to the user. Finally, a developer of a pHealth information system can use the template to plan the required privacy and trust services.

The authors have also made proposals for a future ethical, trusted, and privacy-enabled pHealth ecosystem. Here, PHI and health-related behaviors and emotions are the service user's/DS's personal property. Therefore, the DS has the power to express its own privacy and trust needs to the service provider and other ecosystem stakeholders. Transparency and accountability make it possible for the service user to estimate the actual level of privacy and trust in the ecosystem. For estimating the level of trust, the authors propose the use of computational methods [48]. In the proposed solution, users' privacy and trust needs are stored in the form of computer-understandable policies and smart contracts on the blockchain. The legal binding duty concept in the model (fiducial duty) can guarantee fair information processing in the whole ecosystem.

Nevertheless, there are also challenges to be solved. According to Notario et al., ethical concepts, privacy, and trust principles and laws are typically described using high-level terms, and it is difficult to translate them into technical requirements and to support service users concerns and expectations [107]. Some researchers have argued that blockchain technology does not need trust to operate because there is no centralized trust anchor. Instead, according to De Flilippi, blockchain technology produces confidence (and not trust) [108]. Trust in the blockchain is nevertheless necessary because users need trust in the developers and the implementation of algorithms, mathematical knowledge, and cryptographic tools. The authors state that organizational trust and trust in technology are essential elements of ecosystems. What is needed is a commonly accepted definition of the meaning of organizational trust [93].

A big challenge in the authors' proposal is that it requires new internationally accepted regulations and laws. Nowadays, there is no guarantee that policy makers have the intention to enact necessary legislation and force big internet vendors to support and implement laws that can strongly impact their current money-making model. Instead, the responsibility to manage online privacy has been increasingly transferred to service users [109]. Another challenge is to make organizations understand that only systems that behave ethically can be trusted [39]. Some researchers have also argued that a law for data as personal property may be difficult to construct, and this kind of property approach will cause economic losses and less innovation. The authors see that the hybrid approach discussed in this paper is, from the service user's/DS's point of view, a more preferable solution than PHI as a public/common good and current laws.

The authors state that despite researchers' efforts to develop innovative technological privacy solutions, they alone will hardly make future pHealth ecosystems ethical and trustworthy and guarantee information privacy. Instead, it is necessary to start the development of next-generation pHealth ecosystems using a holistic view and a system-theoretical, context-aware, architecture-centred, ontology-based, and policy-driven approach [110] as standardized in ISO 23903:2021 Health informatics: interoperability and integration reference architecture: model and framework [111]. Therefore, the privacy and trust approaches and solutions discussed in this paper will be deployed. It is also necessary to understand privacy and trust in ecosystems at the system level and create new laws to strengthen a person's position. The new solution should also support transparency and explainability. In the long run, global harmonization of how privacy and trust are understood and international regulations are also needed. In agreement with Schneiderman, the authors state that the future pHealth ecosystem shall be created and operated to respect, promote, and protect internationally recognized human rights [112].

Author Contributions: P.R. is the main writer of the original draft; B.B. participated in the development of the draft and made meaningful work in reviewing and editing the article. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cohen, J.E. *Between Truth and Power*; Oxford University Press: Oxford, UK, 2019; ISBN 978-0-91-763754-8.
2. Ruotsalainen, P.; Blobel, B. Privacy and Trust in pHealth—Past, Present and Future. In Proceedings of the pHealth 2022, Oslo, Norway, 8–10 November 2022; Blobel, B., Yang, B., Giacomini, M., Eds.; IOS Press: Amsterdam, The Netherlands, 2022. [CrossRef]
3. Sun, Y.; Zhou, J.; Ji, M.; Pei, L.; Wang, Z. Development and Evaluation of Health Recommender Systems: Systematic Scoping Review and Evidence Mapping. *J. Med. Internet Res.* **2023**, *25*, e38184. [CrossRef] [PubMed]
4. Gellerstedt, M. The digitalization of health care paves the way for improved quality of life. *Syst. Cybern. Inform.* **2016**, *14*, 1–10.
5. Aalbers, G.; Hendrickson, A.T.; MPVanden, A.M.; Keijsers, L. Smartphone-Tracked Digital Markers of Momentary Subjective Stress in College Students: Idiographic Machine Learning Analysis. *JMIR Mhealth Uhealth* **2023**, *11*, e37469. [CrossRef] [PubMed]
6. Rose, C. Ubiquitous Smartphones, Zero Privacy. *Rev. Bus. Inf. Syst. Fourth Quart.* **2012**, *16*, 187–192. [CrossRef]
7. Wei, Z.; Zhao, B.; Su, J. PDA: A Novel Privacy-Preserving Robust Data Aggregation Scheme in People Centric Sensing System. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 147839. [CrossRef]
8. Zuboff, S. *The Age of Surveillance Capitalism*; Profile Books Ltd.: London, UK, 2019; ISBN 9781781256855.
9. Lamdan, S. *Data Cartels*; Stanford University Press: Stanford, CA, USA, 2023; ISBN 978-1-5036-3371-1.
10. Ziegeldorf, J.H.; Morchom, O.C.; Wehle, K. Privacy in the Internet of Things: Threats and Challenges, Security and Communication networks. *Secur. Commun. Netw.* **2013**, *7*, 2728–2742. [CrossRef]
11. Berger, S.; Rossi, F. AI and neurology: Learning from AI ethics and an expanded Ethics Landscape. *Commun. ACM* **2023**, *66*, 58–68. [CrossRef]
12. van Hoboken, J. *Chapter 10 in Book Human Rights in the Age of Platforms*; Jorgensen, R.F., Ed.; The MIT Press: Cambridge, MA, USA, 2019. Available online: https://mitpress.mit.edu/9780262039055/human-rights-in-the-age-of-platforms/ (accessed on 17 April 2023); ISBN 9780262353946.
13. Hazel, S. Personal Data as Property (7 August 2020). Syracuse Law Review, Forthcoming. Available online: https://doi.org/10.2139/ssrn.3669268 (accessed on 17 April 2023).
14. Piasecki, J.; Cheah, P.Y. Ownership of individual-level health data, data sharing, and data governance. *BMC Med. Ethics* **2022**, *23*, 104. [CrossRef]
15. Grossmann, C.; Goolsby, W.A.; Olsen, L.A.; McGinnis, J.M. *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary*; The National Academies Press: Washington, DC, USA, 2010. [CrossRef]
16. Taylor, L. The ethics of big data as a public good: Which public? Whose good? *Phil. Trans. R. Soc. A* **2016**, *374*, 20160126. [CrossRef]
17. Schwartz, P.M. Property, Privacy, and Personal Data. Available online: https://ssrn.com/abstract=721642 (accessed on 17 April 2023).
18. Health Data as a Global Public Good. Available online: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en (accessed on 17 April 2023).
19. Dickens, A. From Information to Valuable Asset: The Commercialization of Health Data as a Human Rights Issue. *Health Hum. Rights J.* **2020**, *22*, 67–69.
20. Health Data as a Global Public Good. Available online: https://cdn.who.int/media/docs/default-source/world-health-data-platform/events/health-data-governance-summit/preread-2-who-data-governance-summit_health-data-as-a-public-good.pdf?sfvrsn=2d1e3ad8_8 (accessed on 17 April 2023).
21. Gstrein, O.J.; Beaulien, A. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philos. Technol.* **2022**, *35*, 3. [CrossRef] [PubMed]
22. Friedewald, R.F.; Wrigth, D. Seven types of privacy. In *European Data Protection: Coming of Age*; Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y., Eds.; Springer Science+Business Media: Dordrecht, The Netherlands, 2013. [CrossRef]
23. McKnight, D.H.; Choudhury, V.; Kacmar, C. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. In *The Blackwell Encyclopaedia of Management*; Davis, G.B., Ed.; Management Information Systems; Blackwell: Malden, MA, USA, 2002; Volume 7, pp. 329–331.
24. Ruotsalainen, P.; Blobel, B. How a Service User Knows the Level of How a Service User Knows the Level of Privacy and to Whom Trust in pHealth Systems? *Stud. Health Technol. Inf.* **2021**, *285*, 39–48.
25. Gupta, P.; Akshat Dubey, A. E-Commerce-Study of Privacy, Trust and Security from Consumer's Perspective. *Int. J. Comput. Sci. Mob. Comput.* **2016**, *5*, 224–232.
26. Rubenfield, J. *The End of Privacy*; Yale Law School, Faculty Scholarship Series: New Haven, CT, USA, 2008.
27. 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*, 3006. [CrossRef]
28. Rubinstein, I.S. Big Data: The End of Privacy or a New Beginning? In *International Data Privacy Law*; Oxford University Press: Oxford, UK, 2013; Volume 3.
29. Ruotsalainen, P.; 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. [CrossRef]
30. Sharma, S.; Chen, K.; Sheth, A. Towards Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems. *IEEE Internet Comput.* **2018**, *22*, 42–51. [CrossRef]

31. Hansen, J.; Wilson, P.; Verhoeven, E.; Kroneman, M.; Kirwan, M.; Verheij, R.; van Veen, E.-B. *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*; EU DG Health and Food Safety, Publication Office of the European Union: Luxemburg, 2021; ISBN 978-92-9478-785-9. [CrossRef]
32. Joinson, A.; Houghton, D.J.; Vasalou, A.; Marder, B.L. Digital Crowding: Privacy, Self-Disclosure, and Technology. In *Privacy Online*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2011; pp. 33–45.
33. DeCew, J.; Zalta, E.N. (Eds.) Privacy, the Stanford Encyclopedia of Philosophy; Zalta, E.N., Ed. Available online: https://plato.stanford.edu/archives/spr2018/entries/privacy/ (accessed on 17 April 2023).
34. WHO. Universal Declaration of Human Rights. Available online: https://www.un.who.org/en/universal-declaration-human-rig (accessed on 17 April 2023).
35. Bélanger, F.; Crossler, R.E. Privacy in the Digital age: A Review of Information Privacy Research in Information systems. *MIS Q.* **2011**, *35*, 1017–1041. [CrossRef]
36. Floridi, L. Ontological interpretations of informational privacy. *Ethics Inf. Technol.* **2006**, *7*, 185–200. [CrossRef]
37. Smith, H.J.; Dinev, T.; Xu, H. Information privacy research: An interdisciplinary review. *MIS Q.* **2011**, *35*, 989–1015. [CrossRef]
38. Waldman, A.E. *Privacy as Trust*; Cambridge University Press: Cambridge, UK, 2018; ISBN 978-1-316-63694-7. [CrossRef]
39. Goldberg, I.; Hill, A.; Shostack, A. *Trust, Ethics, and Privacy*; Boston University Law Review, Boston University, School of Law: Boston, MA, USA, 2001; Volume 81, pp. 407–421.
40. Schwarz, P.M.; Treanor, W.M. The New Privacy, 101 MICH. L. REV. 2163. 2003. Available online: https://repository.law.umich.edu/mlr/vol101/iss6/3 (accessed on 17 April 2023).
41. Marguilis, S.T. Privacy as a Social Issue and Behavioral Concept. *J. Soc. Issues* **2003**, *59*, 243–261. [CrossRef]
42. Becker, M. Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy. *Ethics Inf. Technol.* **2019**, *21*, 307–317. [CrossRef]
43. Zwick, D. *Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce*; University of Rhode Island: Kingston, RI, USA, 1999; Available online: https://www.researchgate.net/profile/Nikhilesh-Dholakia/publication/236784823 (accessed on 17 April 2023).
44. Bhatia, J.; Breaux, T.D. Empirical Measurement of Perceived Privacy Risk. *ACM Trans. Comput.-Hum. Interact.* **2018**, *25*, 1–47. [CrossRef]
45. Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *Eur. J. Inf. Syst.* **2013**, *22*, 295–316. [CrossRef]
46. Wisniewski, P.J.; Page, X. Chapter 2: Privacy Theories and Frameworks. In *Modern Socio-Technical Perspectives on Privacy*; Bart, P., Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 15–41.
47. Motti, V.G.; Berkovsky, S. Chapter 10 Healthcare Privacy. In *Modern Socio-Technical Perspectives on Privacy*; Bart, P., Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 203–231.
48. Ruotsalainen, P.; Blobel, B.; Pohjolainen, S. Privacy and Trust in eHealth: A Fuzzy Linguistic Solution for Calculating the Merit of Service. *J. Pers. Med.* **2022**, *12*, 657. [CrossRef]
49. Sætra, H.K. Privacy as an aggregate public good. *Technol. Soc.* **2020**, *63*, 101422. [CrossRef]
50. DaCosta, S. Privacy-as-Property: A New Fundamental Approach to The Right to Privacy and The Impact This Will Have on the Law and Corporations. CMC Senior Theses. 2635. 2021. Available online: https://scholarship.claremont.edu/cmc_theses/2635 (accessed on 17 April 2023).
51. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and Human Behavior in the Age of Information. *Science* **2015**, *347*, 509–514. [CrossRef]
52. 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. *Comput. Hum. Behav.* **2010**, *26*, 857–869. [CrossRef]
53. Nojoumian, M. Rational Trust Modelling, Decision and Game Theory for Security. In Proceedings of the 9th International Conference, GameSec 2018, Seattle, WA, USA, 29–31 October 2018; Bushnell, L., Poovendran, R., Başar, T., Eds.; Lecture Notes in Computer Science. Springer International Publishing: Berlin/Heidelberg, Germany, 2017. [CrossRef]
54. Ruotsalainen, P.; Blobel, B. Transformed Health Ecosystems Challenges for Security, Privacy, and Trust. *Front. Med.* **2022**, *9*, 827253. [CrossRef]
55. Ikeda, S. Is it a rational trust. In *Modern Socio-Technical Perspectives on Privacy*; Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, M., Romano, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2022. [CrossRef]
56. Pedersen, N.J.L.; Ahlström-Vil, K.; Kappe, K. Rational trust. *Synthese* **2014**, *191*, 1953–1955. [CrossRef]
57. Saariluoma, P.; Karvonen, H.; Rousi, R. Techno-Trust and Rational Trust in Technology–A Conceptual Investigation. In *Human Work Interaction Design. Designing Engaging Automation*; HWID 2018. IFIP Advances in Information and Communication Technology; Springer: Cham, Switzerland, 2019; Volume 544. [CrossRef]
58. McKnight, D.H. Trust in Information Technology. In *The Blackwell Encyclopaedia of Management*; Davis, G.B., Ed.; Management Information Systems; Blackwell: Malden, MA, USA, 2005; Volume 7, pp. 329–331.
59. Balfe, N.; Sharples, S.; Wilson, J.R. Understanding Is Key: An Analysis of Factors Pertaining to Trust in a Real-World Automation System. *Hum. Factors* **2018**, *60*, 477–495. [CrossRef]

60. Yueh, H.-P.; Huang, C.-Y.; Lin, W. Examining the differences between information professional groups in perceiving information ethics: An analytic hierarchy process study. *Front. Psychol.* **2022**, *13*, 954827. [CrossRef] [PubMed]
61. Reitz, J.M. Online Dictionary for Library and Information Sciences. 2014. Available online: https://www.abc-clio.com/ODLIS/odlis_i.aspx (accessed on 17 April 2023).
62. Terrell, B. "Computer and Information Ethics", The Stanford Encyclopedia of Philosophy (Winter 2017 Edition), Zalta, E.N., Ed. Available online: https://plato.stanford.edu/archives/win2017/entries/ethics-computer/ (accessed on 17 April 2023).
63. European Commission, Ethics by Design and Ethics of Use Approaches for Artificial Intelligence, 25 November 2021. Available online: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf (accessed on 17 April 2023).
64. Guggenberger, T.M.; Möller, F.; Haarhaus, T.; Gür, I.; Otto, B. Ecosystem Types in Information Systems, Twenty-Eight European Conference on Information Systems (ECIS2020), Marrakesh, Morocco. Available online: https://aisel.aisnet.org/ecis2020_rp/45/ (accessed on 17 April 2023).
65. Benedict, M. Modelling Ecosystems in Information Systems—A Typology Approach. In Proceedings of the Multikonferenz Wirtschaftsinformatik 2018, Lüneburg, Germany, 6–9 March 2018.
66. Dobkin, A. Information fiduciaries in Practice: Data privacy and user expectations. *Berkeley Technol. Law J.* **2018**, *33*, 1. [CrossRef]
67. Balkin, J.M. Information Fiduciaries and the First Amendment. *UC Davis Law Rev.* **2016**, *49*, 1183.
68. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Gov. Inf. Q.* **2022**, *39*, 101679. [CrossRef]
69. O'Connor, Y.; Rowan, W.; Lynch, L.; Heavin, C. Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Comput. Sci.* **2017**, *113*, 653–658. [CrossRef]
70. Knijnenburg, B.P. *A User-Tailored Approach to Privacy Decision Support*; University of California: Los Angeles, CA, USA, 2015; Available online: https://escholarship.org/uc/item/9282g37p (accessed on 17 April 2023).
71. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
72. Hanish, S.; Arias-Cabarcos, P.; Parra-Arnau, J.; Strufe, T. Privacy-Protecting Techniques for Behavioral Data: A Survey. *arXiv* **2021**, arXiv:2109.04120v1.
73. Huckvale, K.; Prieto, J.T.; Tilney, M.; Benghozi, P.-J.; Car, J. Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. *BMC Med.* **2015**, *13*, 214.
74. Papageorgiou, A.; Strigkos, M.; Politou, E.; Alepis, E.; Solanas, A.; Patsakis, C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* **2018**, *6*, 9390–9403. [CrossRef]
75. Kerasidou, C.X.; Kerasidou, A.; Buscher, M.; Wilkinson, S. Before and Beyond Trust: Reliance in Medical AI. *J. Med.* **2020**, *48*, 852–856. Available online: https://jme.bmj.com/content/48/11/852 (accessed on 17 April 2023). [CrossRef]
76. Richards, N.; Hartzog, W. Taking Trust Seriously in Privacy Law. *Stanf. Tech. Law Rev.* **2016**, *19*, 431. [CrossRef]
77. Wilkinson, D.; Sivakumar, S.; Cherry, D.; Knijnenburg, B.P.; Raybourn, E.M.; Wisniewski, P.; Sloan, H. Work in Progress: User-Tailored Privacy by Design. In Proceedings of the USEC'17, San Diego, CA, USA, 26 February 2017; ISBN 1-1891562-47-9. [CrossRef]
78. Knijnenburg, B.P. Chapter 16 User-Tailored Privacy. In *Modern Socio-Technical Perspectives on Privacy*; Bart, P., Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2022. [CrossRef]
79. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *24*, 131–143.
80. Ruotsalainen, P.; Blobel, B. *Digital pHealth–Problems and Solutions for Ethics Trust and Privacy, pHealth 2019*; Blobel, B., Giacomini, M., Eds.; IOS Press: Amsterdam, The Netherlands, 2019; pp. 31–46. [CrossRef]
81. Uriarte, R.B.; Zhou, H.; Kritikos, K.; Shi, Z.; Zhao, Z.; De Nicola, R. Distributed service-level agreement management with smart contracts and blockchain. *Concurr. Comput. Pract. Exp.* **2020**, *33*, e5800. [CrossRef]
82. Gursels, S. Privacy and Security Can you engineer privacy? *Commun. ACM* **2014**, *57*, 20–23. [CrossRef]
83. Lopez, G.P.; Montresor, A.; Epema, D.; Datta, A.; Higashino, T.; Iamniychi, A.; Barcellos, M.; Felber, P.; Riviere, E. Edge-centric computing: Vision and Challenges. *ACM SIGCOMM Comput. Commun. Rev.* **2015**, *45*, 37–42. [CrossRef]
84. Cao, X.; Tang, G.; Guo, D.; Li, Y.; Zhang, W. Edge Federation: Towards an Integrated Service Provisioning Model. *IEEE/ACM Trans. Netw.* **2020**, *28*, 1116–1129. [CrossRef]
85. Ritter, J.; Anna Mayer, A. Regulating Data as Property: A New Construct for Moving Forward. *Duke Law Technol. Rev.* **2018**, *16*, 220–277. Available online: https://scholarship.law.duke.edu/dltr/vol16/iss1/ (accessed on 17 April 2023).
86. Samuelson, P. Privacy As Intellectual Property? *Stanf. Law Rev.* **2000**, *52*, 1125. [CrossRef]
87. Koos, S. Protection of Behavioural Generated Personal Data of Consumers. In Proceedings of the 1st Workshop Multimedia Education, Learning, Assessment and Its Implementation in Game and Gamification, Medan, Indonesia, 26 January 2019. [CrossRef]
88. Blanco, S. Trust and Explainable AI: Promises and Limitations. In Proceedings of the ETHICOMP 2022, Turku, Finland, 26–28 July 2022; Koskinen, J., Kimppa, K.K., Heimo, O., Naskali, J., Ponkala, S., Rantanen, M.M., Eds.; University of Turku: Turku, Finland, 2022; pp. 246–257; ISBN 978-951-29-8989-8.

89. Rossi, A.; Lenzini, G. Transparency by design in data-informed research: A collection of information design patterns. *Comput. Law Secur. Rev.* **2020**, *37*, 105402. [CrossRef]
90. EU-GDPR. Available online: Htpps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-2016950&qid=1532348683434 (accessed on 17 April 2023).
91. Barret, L. Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries, 42 SEATTLE U. L. REV. 2019; p. 1057. Available online: https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/5/ (accessed on 17 April 2023).
92. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An Integrative Model of Organizational Trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. Available online: http://www.jstor.org/stable/258792.137-154 (accessed on 17 April 2023). [CrossRef]
93. Lumioneau, F.; Schilke, O.; Wang, W. Organizational trust in the age of the fourth industrial revolution: Shifts in the nature, production, and targets of trust. *J. Manag. Inq.* **2022**, *32*. [CrossRef]
94. Hand, D.J. Aspects of Data Ethics in a Changing World: Where Are We Now? *Big Data* **2018**, *6*, 176–190. [CrossRef] [PubMed]
95. Holt, J.; Malčić, S. The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union. *J. Inf. Policy* **2015**, *5*, 155–178. Available online: https://www.jstor.org/stable/10.5325/jinfopoli.5.2015.0155 (accessed on 17 April 2023). [CrossRef]
96. Elrik, E.L. The ecosystem concept: A holistic approach to privacy, protection. *Int. Rev. Law Comput. Technol.* **2021**, *35*, 24–45. [CrossRef]
97. Ferrario, A.; Loi, M. How Explainability Contributes to Trust in AI. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT'22), Seoul, Republic of Korea, 21–24 June 2022; ACM: New York, NY, USA, 2022; p. 10. [CrossRef]
98. Lederer, S.; Mankoff, J.; Dey, A.K. *A Conceptual Model and Metaphor of Everyday Privacy in Ubiquitous Computing Environments*; Report No, UCB/CSD-2-1288; University of California: Berkeley, CA, USA, June 2002.
99. Wiedemann, K.-P.; Hennings, N.; Varelmann, D.; Reeh, M.-O. Determinants of Consumer Perceived Trust in IT-Ecosystems. *J. Theor. Appl. Electron. Commer. Res.* **2010**, *5*, 137–154. [CrossRef]
100. Najib, W.; Sulityo, S. Widyawan, Surveys on Trust Calculation Methods in Internet of Things. *Procedia Comput. Sci.* **2019**, *161*, 1300–1307. [CrossRef]
101. Truong, N.B.; Um, T.-W.; Lee, G.M. A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things. In Proceedings of the 19th International ICIN Conference–Innovations in Clouds Internet and Networks, Paris, France, 1–3 March 2016.
102. Sattler, A. From Personality to Property? Revisiting the Fundamentals of the Protection of Personal Data. 2018. Available online: https://www.wizdom.ai/publication/10.1007/978-3-662-576465_3/title/from_personality_to_property_revisiting_the_fundamentals_of_the_protection_of_personal_data (accessed on 17 April 2023).
103. Cole, C.L.; Sengupta, S.; Rossetti (ne'e Collins), S.; Vawdrey, D.K.; Halaas, M.; Maddox, T.M.; Gordon, G.; Dave, T.; Payne Philip, R.O.; Williams, A.E.; et al. Ten principles for data sharing and commercialization. *J. Am. Med. Inform. Assoc.* **2021**, *28*, 646–649. [CrossRef] [PubMed]
104. Richter, H. The Power Paradigm in Private Law, Towards a Holistic Regulation of Personal Data. In *Personal Data in Competition, Consumer Protection and Intellectual Property Law*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 527–577. [CrossRef]
105. Gerber, N.; Reinheimer, B.; Volkamer, M. Investigating People's Privacy Risk Perception. *Proc. Priv. Enhancing Technol.* **2019**, *3*, 267–288. [CrossRef]
106. Mitchell, V.-M. Consumer perceived risk: Conceptualizations and models. *Eur. J. Mark.* **1999**, *33*, 163–195. [CrossRef]
107. Notario, N.; Crespo, A.; Martín, Y.-S.; Jose, M.; Alamo, J.M.; Daniel Le Métayer, D.L.; Antignac, T.; Kung, A.; Kroener, I.; Wright, D. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. In *2015 IEEE CS Security and Privacy Workshops*; IEEE: Piscataway, NJ, USA, 2015; pp. 151–158. [CrossRef]
108. De Filippi, P.; Manna, M.; Reijers, W. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technol. Soc.* **2020**, *62*, 101284. [CrossRef]
109. Shariff, A.; Green, J.; Jettinghoff, W. The Privacy Mismatch: Evolved Intuitions in a Digital World. *Curr. Dir. Phycol. Sci.* **2021**, *30*, 159–166. [CrossRef] [PubMed]
110. Blobel, B.; Oemig, F.; Ruotsalainen, P.; Lopez, D.M. Transformation of Health and Social Care Systems—An Interdisciplinary Approach Toward a Foundational Architecture. *Front. Med.* **2022**, *9*, 802487. [CrossRef] [PubMed]
111. *ISO 23903:2021*; International Organisation for Standardisation. Health Informatics–Interoperability and Integration Reference Architecture–Model and Framework. ISO: Geneva, Switzerland, 2021.
112. Schneiderman, B. Bridging the Gap Between Ethics and Practice: Guidelines for Reliable, Safe, and Trustworthy Human-Centered AI Systems. *ACM Trans. Interact. Syst.* **2020**, *10*, 1–31. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.