Journal of Information Security and Applications 66 (2022) 103163

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Personal information: Perceptions, types and evolution

Rahime Belen Saglam [a], Jason R.C. Nurse [a,*], Duncan Hodges [b]

[a] School of Computing, University of Kent, Canterbury, Kent, CT2 7NF, UK
[b] Cranfield University, Defence Academy of the United Kingdom, Shrivenham, Wilts, SN6 8LA, UK

ARTICLE INFO

Keywords:
Personal information
Information sensitivity
Data protection
Regulations
Taxonomy
Cyber security

ABSTRACT

Advances in technology have made us as a society think more about cyber security and privacy, particularly how we consider and protect personal information. Such developments have introduced a temporal dimension to the definition of personal information and we have also witnessed new types of data emerging (e.g., phone sensor data, stress level measurements). These rapid technological changes introduce several challenges as legislation is often inadequate, and therefore questions regularly arise pertaining whether information should be considered personal or sensitive and thereby better protected. In this paper, therefore, we look to significantly advance research into this domain by investigating how personal information is regarded in governmental legislations/regulations, privacy policies of applications, and academic research articles. Through an assessment of how personal information has evolved and is perceived differently (e.g., in the context of sensitivity) across these key stakeholders, this work contributes to the understanding of the fundamental disconnects present and also the social implications of new technologies. Furthermore, we introduce a series of novel taxonomies of personal information which can significantly support and help guide how researchers and practitioners work with, or develop tools to protect, such information.

1. Introduction

Even though the definition of personal information might seem straightforward, recent rapid advancements in technology have made it surprisingly difficult to characterise its scope. With the increased usage of online social networks (OSNs), different types of personal information (e.g., photos or location check-ins) have emerged and are stored on OSNs in vast quantities. Information gathered from various internet-of-things (IoT) devices (e.g., sensor data, or heart-rate data from wearable devices) or from mobile apps (e.g., on health) which are currently widely employed among smartphone users, provide other examples of the evolution of personal information. All of these rapid technological changes challenge how we view personal data, and have implications for the cyber security domain regarding how this information should be protected. The changing nature of personal information due to technological developments is not limited to an increase in the amount of information that is being processed. Advances in computational power and the simplification of complex analytical problems using computational frameworks such as TensorFlow [1] mean it is now far easier to extract or infer new information by conducting analytics on data gathered from diverse sources. While such analytics can be beneficial for solving real-world problems, these can also be exploited by entities such as data brokers that collect, analyse and sell personal data to third parties [2,3] or other more maliciously motivated actors. The application of sophisticated data analytics to very large data sets makes it possible for actors to infer or derive additional personal information about individuals that may otherwise not be known from examining the underlying data.

Cloud computing plays an important role in today's data-driven society as it facilitates the efficient storage and processing of large data sets. This technology however, when combined with other emerging systems (e.g., IoT and Artificial Intelligence), challenge traditional mechanisms to protect individual's privacy [4,5]. Mehmood et al. [4] discuss the inadequacy of traditional anonymisation techniques given the availability of huge volumes of data and powerful data analytic tools. Even though several techniques such as k-anonymity, l-diversity or t-closeness have been proposed to deal with privacy issues, data breach incidents (which expose a variety of personal information) persist. These incidents are frequent and impactful [6], and often highlight a poor understanding of personal data, and thus how it should be protected.

While the developments and concerns discussed above are by no means new, one area that has received little in-depth academic analysis is how personal information has evolved and how it is perceived differently (e.g., in the context of sensitivity) due to advancements in technologies. Continuous technological developments (such as smart

[*] Corresponding author.
E-mail addresses: R.Belen-Saglam-724@kent.ac.uk (R. Belen Saglam), J.R.C.Nurse@kent.ac.uk (J.R.C. Nurse), d.hodges@cranfield.ac.uk (D. Hodges).

https://doi.org/10.1016/j.jisa.2022.103163

Available online 26 March 2022

technologies or cyber–physical systems [7]) coupled with increases in types of data and ways to extract novel insights from it also add a temporal dimension to the definition of information. By temporal dimension, we mean that the nature of data, and what is personal or sensitive, may change as time progresses. Currently when discussing sensitive data in legislations and privacy policies, the primary factor explicitly considered is the type of data. It is arguable that, as the technology evolves and the medium that the data is stored varies, the characteristics of the entire data-ecosystem will become one of the major concerns. Different sensitivity categorisations for different technologies that consider the risks levels of the platforms might also become common practice. This may in part be driven or informed by legislations discouraging processing of sensitive personal data on high risk platforms. Such discussions can already be seen in the literature where blockchain technology, as an example of an emerging technology for data storage, is not recommended for processing of sensitive personal information [8–10].

Data may also change from being anonymous to re-identifiable as more diverse data sets (e.g., aggregated from multiple sources) become collectable from the public domain [11]. Purchasing habits, which may not seem to be sensitive at first glance, may reveal highly sensitive data through data-driven inferences, for example, they may be used to reveal an unhealthy life style, location data, financial difficulties and even illegal activity when processed over time [11]. Another example is dynamic IP addresses which only started to be considered as personal information after the Case-582/14 the CJEU.[1] Furthermore, the perceptions of personal data may differ as government and legislations lag significantly behind industry (particularly new devices which interact with a range of personal data). A better understanding of such issues is important for technical research as it can form the foundation through which data is processed and protected by systems.

The contribution of this paper is twofold. First, we engage in a critical investigation of the nature of personal information as it exists in society today, and examine how it has evolved due to technological advancements. We research and analyse, in detail, the perspectives of three core stakeholders across the world: Governments, industry and academia. This assessment of the types of personal information discussed across these stakeholders, and how such information has evolved, can significantly contribute to understanding the social implications of new technologies. Observing this evolution is also critical to keeping data protection practices, including those focused on emerging security approaches, appropriate and up-to-date. This is particularly important as the variety of data sources (e.g., sensors, IoT devices, edge devices) increases and the advances in analytic capability that can fuse these diverse data sets to generate new inferences.

Our second contribution is a by product of the first and takes the form of a series of detailed taxonomies of personal information and sensitive personal information. These taxonomies have been created to define how personal information is regarded internationally across three key stakeholders (i.e., Government, industry and academia) and how the sensitivity of several sets of information are perceived. As such, they facilitated our understanding of the evolution of personal data across stakeholders. These taxonomies, do, however, contribute to the literature on their own, and represent a synthesis of a rich set of documents in each stakeholder corpus. As such, we also provide machine-readable formats of the taxonomies as supplementary materials alongside this article. To the best of our knowledge, the work and taxonomies proposed here provide the most detailed taxonomies in existing literature dedicated to personal information. These taxonomies can form the foundation for several studies supporting transparency of personal data processing and security, particularly in emerging approaches. Knowing the category of a data item, other data items under the same category and their corresponding sensitivity levels can support risk assessment of data processing activities. They also provide the perception of each stakeholder on sensitivity at a granular level which is often not considered by existing studies.

Across this work the topic of information sensitivity is important as it provides more detailed insight into how information is perceived by stakeholders. For our work, we use GDPR's description of sensitivity, which considers data that requires specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of an individual [12].

Our work examines governmental documents to understand the perspective of governments, the privacy policies associated with mobile applications (apps) to sample an industry perspective of current practice, and research articles to gather the perceptions of the academic community. Due to the pervasiveness of smartphones and the decreases in the cost of developing mobile apps, many public and private organisations have started to look for new ways to exploit the possibilities of mobile devices into their business practices. According to the Cisco Annual Internet Report, nearly 300 million mobile applications will be downloaded by 2023 [13]. Considering the difficulty of comparing and contrasting such a broad range of information sources, we have opted to synthesise a series of taxonomies of personal information. These taxonomies are created for each stakeholder group, and also allow us to observe the variation in information perceptions at a granular level across stakeholders.

Assuming the scope of personal information as defined by legislations as the first stage of the evolution (i.e., the basic way in which personal information can be perceived), our research then observes the variation in perceptions through privacy policies (i.e., the current practices employed by organisations who use personal information) and academic articles. Privacy policies are ideal as they capture and clearly identify the personal information that they use, while academic articles may define robust groupings of personal information often driven by empirical studies. We expect that this research will contribute significantly to the understanding of personal information and how it has been impacted by technology.

The remainder of this paper is structured as follows. Sections 2 and 3 reflect on the nature of personal information, how technology has impacted this, and the studies that look to characterise this type of information (e.g., in the context of taxonomies). Section 4 details and justifies the methodology applied in our research. Next, Section 5 introduces the data sources that we have made use of and explains what data has been gathered. Section 6 presents and discusses the taxonomies created for governmental documents, privacy policies and academic articles; these form the basis for our consideration of the different perspectives adopted and the evolution of how personal data is perceived. We outline and critically reflect on our findings in Section 7. Section 8 follows, and includes our limitations, before we conclude and define avenues for future work in Section 9.

2. Background

The concept of personal information has been discussed in research and practice for many years. The mainstream literature is centred on the identifiability of a person, the risk of re-identification and de-anonymisation algorithms due to technological developments [14]. Several researchers argued that absolute and irreversible anonymity is no longer possible due to the progress of data processing technologies and the amount of data available for analysis [15,16].

Governments have also been heavily involved in characterising personal information, particularly to attempt to ensure that those that process it implement adequate protective (e.g., security and privacy) measures. While there are numerous legislations across the world that focus on personal information (e.g., Privacy Act in the US [17], Data Protection Act in Estonia [18]), arguably the most significant and

[1] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016], 112/16 Luxembourg, Court of Justice of the European Union.

far-reaching of these is the EU's General Data Protection Regulation (GDPR) [12].

GDPR defines personal data as: "*Any information relating to an identified or identifiable natural person ('data subject')*", where definition of 'identifiable natural person' is given as; "*One who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" [12]. From these definitions, we can note that GDPR discerns types of personal data in terms of identifiability; this will be a key point that we will reflect on later in our analysis and discussions.

Concerns regarding the inadequacy of regulatory documents to cover the changing nature of personal information due to new technologies has been covered in the literature by several researchers. Tene [19] argued that the bi-polar approach in regulatory documents based on labelling information either 'personally identifiable' or not, is meaningless in a Big Data age. They proposed to view the identifiability of data as a continuum as opposed to the current dichotomy.

In addition to concerns regarding identifiability, researchers have also identified several other inadequacies related to personal information protection principles. For instance, the GDPR, and more generally the traditional principles of data protection, were criticised as they may be valid only in a world where data management is centralised within specific entities [20]. In this respect, those principles have been found inadequate to embrace recent technologies such as blockchain [20] or cloud technologies [21] where identifying bodies responsible for personal data is not easy.

To complement critics of personal data protection principles, literature has also highlighted issues regarding the categorisation of personal data or misalignment between the personal information types recognised by governmental documents and the variety of information emerged with the recent technologies. Wuyts et al. [22] for instance, focused on health data and explored new privacy threats to the patient's medical data, as more data becomes easily accessible via Electronic Health Record (EHR) and Personal Health Record (PHR) systems. They emphasised that the category of health data in the regulations should be divided in more concrete subcategories providing meaningful fine-grained privacy setting for online health networks. Moreover, another concern was raised in this work, i.e., the categorisation of data sensitivity in GDPR does not give a general sense of what personal data may be derived or inferred (inferences are a particular issue as highlighted in prior work [23]). For instance, individuals can never know whether assumptions are being made on their name or residential status, which are not considered sensitive in the GDPR's categorisation, to identify their ethnic origins which is regarded as sensitive.

3. Related work

To properly review how personal information has been defined and conceptualised, it is important to assess how it has been typified in existing work. In the literature, there are a limited number of studies which propose categorisations or taxonomies of personal information, in general or specific to a predefined context; see Table 1 for the complete list, which also helps to show gaps in the field. In one of these studies, Rumbold et al. proposed a schema for a granular assessment of data categories [11] which is based on the classification made by the UK Anonymisation Network (UKAN) [24].

Rumbold et al. divide personal information into five categories: Human demographics, behaviour, thoughts and opinions; Readily apparent human characteristics (unprotected); Readily apparent human characteristics (protected); Medical or health data; and Human machine interactions [11]. They give data related to motor vehicles as an example of the Human machine interactions category and emphasise that such kind of interactions can log human behaviour, like driving patterns or browsing history. This is reported as a concern since data coming from IoT devices will be a large proportion of information in the future. Especially, the privacy risks that could emerge when data from different sources are aggregated are underlined.

In their work, Rumbold et al. also emphasise the need of a more detailed classification of different types of data and more nuanced definition of personal information [11]; they argue that this could increase the utility and reduce the risks of large data aggregations. This study is important for the re-assessment of data categories which also highlight the sensitivities of data types within each category. However, the number of personal data items in their categorisation is quite limited. The two examples given for the Human machine category, which are recordings of human/machine interaction and location data, can be given as examples of this inadequacy.

In addition to generic studies that focus on categorisation of information, there are also more directed works which explore categorisation of specific types of personal information. Warken et al. proposed a new model for personal data categorisation in the context of law-enforcement cross-border access to evidence [25]. The authors examined the categorisation of data as applied in the most important current and forthcoming frameworks for law enforcement cross-border access to evidence; namely the Council of Europe's Cybercrime Convention, the US CLOUD Act and the European Investigation Order, and the EU's proposed e-evidence Directive and Regulation.

From their analysis, it was observed that these regulations divide the types of data into either two categories (metadata and content data), or three categories (subscriber data, transnational data (including traffic data and, as a further subgroup, access data) and content data) [25]. Warken et al. argue that these categories are inherited from the pre-cloud era which does not reflect the current technological developments, especially in the field of telecommunication. They propose new categorisation criterion which is claimed to be future-proof and allows coverage for all types of electronic data. This new categorisation is mainly privacy-oriented and it is made up of five main elements which are information on private life, secret data, shared confidential data, data of limited accessibility and information distributed publicly. However, they did not list the data items under categories, arguing that it will most likely have gaps and will not be future-proof.

Another specialised taxonomy has been proposed by Levalloi-Barth and Zylberberg for wellness data [26]. Researchers developed this taxonomy based on the purpose for which the data has been produced by users, which consists of three categories: Quantified self, Predictive personalisation and Health data generally. Personal data within the Quantified self category relies on sensor data such as biological parameters, physical activities and general wellness data. The Predictive personalisation category captures wellness data that is processed by companies to offer more personalised services to their customers based on the type inferred. Finally, the Health category is designed around the definition of health data given by GDPR and includes, in particular, health status, information about the provision of health services, their payments, eligibility for healthcare as well as any information about the individual collected in the course of the provision of health services. Levalloi-Barth highlights the explosion of sensors in the IoT technologies and warns about potential privacy issues for personal information generated by those technologies.

With the increased usage of OSNs, concerns regarding the sensitivity and quantity of personal information on them have emerged. A taxonomy for this specific type of information has been published by Richthammer et al. [27]. The taxonomy was developed by reviewing literature to identify possible data elements and subsequently by studying fundamental user activities on OSNs. The article divided data into two main groups as Service provider-related data and User-related data. Service provider related data refers to data that originates from the service usage such as log-in data or connection data (IP addresses), whereas user-related data models the diversity of each user's personality and their modes of interaction. This study typifies the personal data under

Table 1
Categorisation of personal information proposed in the literature.

Domain/Context	Technologies considered	Categories proposed	Study
General	Big Data	Human demographics, behaviour, thoughts and opinions; Readily apparent human characteristics (unprotected); Readily apparent human characteristics (protected); Medical or health data; and Human machine interactions	[11]
Law-enforcement cross-border access to evidence	Cloud services	Information on private life; Secret data; Shared confidential data; Data of limited accessibility; Information distributed publicly	[25]
Wellness	IoT technologies	Quantified self; Predictive personalisation; Health generally	[26]
Online Social Networks (OSNs)	None specifically	Service provider-related data; User-related data	[27]
General	None specifically	Identifiability (Identifying data; De-identified data; Anonymous data; Pseudonymous data); Sensitivity (Sensitive data; Non-sensitive data); Origin (Observed data; Derived data; Inferred data)	[28]

each category in detail however the items are limited to personal data processed by OSNs.

Cradock et al. emphasised the benefit of categorising personal data for transparency which is the key principle in European Union (EU) framework [28]. Reviewing different sources from academia, privacy experts and legislation, they have exposed how those stakeholders have different understanding, levels of granularity, and items in each category [28]. Identifying the variety in the categories and lack of low level granularity in personal data items in regulations, Cradock et al. proposed three new criteria to categorise personal data which can increase the transparency of data processing for data subjects. These are: categorising personal data in relation to identifiability, sensitivity and finally, to the manner in which the data originated. The last criterion is proposed to enable individuals to understand exactly what is being 'observed', 'derived' and 'inferred'. This is stated to support making data subjects aware of whether the personal data collected will remain in that form, or whether it will be used to create or predict other personal data via new technologies.

While existing research and practice has contributed significantly to the understanding of personal information, as can be seen from our brief review, studies often propose conceptual categorisation options or provide taxonomies dedicated to specific categories. Those taxonomies, which were built considering a single domain (e.g., wellness data) or were developed from a perspective of a single stakeholder (e.g., OSNs), do not allow to observe evolution of personal information with concrete examples. This makes those studies inadequate at exposing the impact of current technologies on personal information and highlights the urgent need of re-evaluating the concept of it to ensure appropriate protection. In this study, we aim to broaden current knowledge of the evolution of personal information with concrete examples, including a presentation of personal information taxonomies across key stakeholders (e.g., governments, industry and academia). Those taxonomies allow us to observe inconsistencies in the scope of personal information and to urge a re-think about the efficiency of current data privacy practices in the longer term.

4. Research methodology

The goal of this research study is to explore the nature of personal information as it exists in society today, and to consider how it has evolved due to technological advancements. The study is centred around three stakeholders, namely, government, industry and academia, and draws on their characterisations of personal information for our analysis; see Fig. 1 for the study's design. This assessment considers the scope of personal information as presented in governmental documents as the first stage of the evolution. Such a decision is based on the reality that these documents often lag significantly behind technology developments [25,26].

To capture the second — and therefore more progressive — stage, we review the industry perspective through an analysis of how personal information is regarded in privacy policies of mobile apps. We have reviewed privacy policies of finance and health apps which are in the list of fastest growing categories in the mobile app markets [29]. Lastly, we examine academic articles which address the topic of personal information, given that academia is often also advanced in its identification and exploitation of new types of personal information. For these articles, we also only focus on finance and health. The decision to concentrate on finance and health is because these sectors heavily process an extensive and diverse amount of items of personal information whilst also allowing us to directly compare the academic perspective with daily industrial practices. According to a data leakage report published in 2018 on global data leaks, banks were one of the most attractive and, therefore, the most vulnerable segments. On the other hand, one of the largest volume of compromised data was recorded in healthcare sectors [30]. We acknowledge that this limited scope on two sectors may, however, have an impact on our findings and therefore discuss this further when we present our limitations in Section 8.

As seen in Fig. 1, the methodology we adopt to structure our work involves four steps: Firstly, we identify and collect documents that reflect the perception of the three named stakeholders. The details of the collection process involved in each stage is given in Section 5. Once documents have been aggregated, the next step involves an analysis of each document group using content analysis [31] aiming to identify key 'themes' (information items in our context) in documents. This allows us to test theoretical issues to enhance understanding of the data. Content analysis may be used in an inductive or deductive way which is determined by the purpose of the study. An inductive approach is typically used if the former knowledge about the phenomenon is limited [32] and the themes are freely created by the researcher. Deductive content analysis is used when the structure of analysis is guided by existing theory or prior research [33]. During our analysis, we follow an approach similar to deductive content analysis and base our analysis on a manual approach where we identify data items explicitly given as personal information or sensitive personal information by the documents. Despite a large volume of documents, a manual approach was preferred due to the nuances involved in the identification, extraction and classification of personal information. This is especially

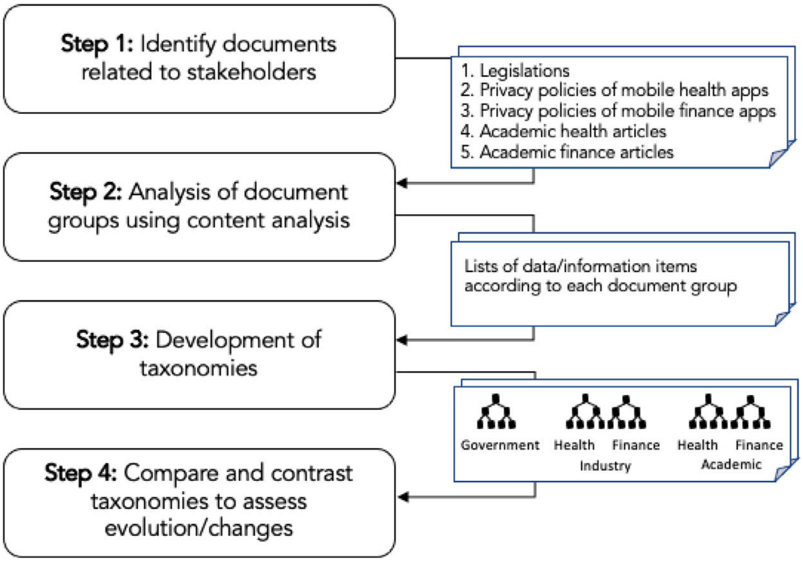
Step 1: Identify documents related to stakeholders
1. Legislations
2. Privacy policies of mobile health apps
3. Privacy policies of mobile finance apps
4. Academic health articles
5. Academic finance articles
Step 2: Analysis of document groups using content analysis
Lists of data/information items according to each document group
Step 3: Development of taxonomies
Government
Health
Finance
Industry
Health
Finance
Academic
Step 4: Compare and contrast taxonomies to assess evolution/changes

Fig. 1. Study design.

true for legislative and academic documents that often are primarily unstructured where personal information is discussed throughout the documents without explicitly mentioning each time that specific content was regarded as 'personal information'. Concerns around the accuracy of automated methods to conduct sensitivity categorisations also motivated our decision not to use such techniques. Therefore, we adopted a manual approach with coders (and second coders, or checkers), which resulted in a less-efficient process but with a likely higher accuracy.

Our manual approach can be explained with following examples. For instance, in the legislation of Spain [34], within the discussion on data with special protection, they state that "*Personal data which refer to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his explicit consent*". From this statement, we extract racial origin, health and sex life as personal information which are also labelled sensitive since they are stated to require special protection. Another example is with the privacy policy of GoogleFit [35]. In this instance, under the section "*Things you create or provide to us*" it is stated that "*When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account.*". From this explanation, we extract *name, password, phone number* and *payment information* as personal information. Two coders worked for all three (stakeholder) groups of documents. For legislations, coders analysed the documents independently then met to discuss and resolve any conflicts. A similar approach was followed for academic articles and privacy policies from apps, however, the second coder instead worked on a randomly selected sample set (20%) due to the large number of articles. Any disagreements in coding were discussed and then actioned as appropriate by the coders (e.g., refinements in coding strategy or reassessing previously coded texts). If two coders could not agree, a third coder was used as the judge (all coders were from the list of authors).

This approach allows us to obtain the perspective of each stakeholder whilst minimising our subjective judgement. The distinction between personal information and sensitive personal information is important and recognised by all of the stakeholders. This is because the protection that should be given to data differs depending on its sensitivity; sensitivity therefore links to the level of harm to an individual once that data is lost, compromised, or disclosed.

In the third step, we manually construct a series of taxonomies from governmental documents, privacy policies (as a proxy for the industry perspective) and academic articles. A taxonomy is a form of classification scheme designed to group related things together. They provide effective knowledge management by systematically and structurally organising human knowledge about things or concepts in many domains [36]. The taxonomies proposed in this study allow us to observe the variation in detail and to make a comparison of stakeholder perspectives at a more granular level.

To build each taxonomy, we first define all of the personal information items for each group, then divide the items into categories to form hierarchies of personal information. During this process, we reflect the common hierarchies given in each group in the corresponding taxonomy and seek to avoid any bias by keeping the taxonomies data driven as much as possible. We then combine smaller categorisations into a single categorisation to form the taxonomy for that stage. This process for taxonomy creation (including the use of content analysis and constructing hierarchies) has been applied in previous research [6]. It also draws inspiration from well-documented methods [36,37] which also define concepts, group them, and iterate until the taxonomy is complete.

An example of our hierarchy creation process is as follows. Working on a document (legislation, privacy policy or academic article), we identify personal data items and their classification where provided. We build an initial version of our taxonomy based on our findings on this document. We then expand this with the items extracted from other documents in the same stakeholder corpus. Once we observe a more common hierarchy different from ours, we modify the hierarchy and keep expanding the new scheme with the new personal data items. We assign a data items to a class only if the document it is mentioned does not cover any classification. Consequently, the final version of the taxonomies reflect the most common classification given in the documents investigated for each group. This process allows our taxonomies to be data driven as much as possible.

Through the aforementioned process, we create one generic taxonomy based on governmental documents, two industry taxonomies (one for healthcare and one for finance) and two academic taxonomies (similarly one for healthcare and one for finance). We intentionally do not combine health and finance taxonomies in industry and academia and refrain from proposing one personal information taxonomy. Our taxonomies are based on our data collection process which are dedicated to collect documents in health and finance sectors. Consequently, they can be thought of as branches of a much broader personal information taxonomy; though there may also be likely to overlap depending on design.

Table 2
List of legislations examined within our study.

Country/Region	Name of Legislation	Year
Austria	Datenschutzgesetz [38]	2000
Belgium	Law on Privacy Protection in relation to the Processing of Personal Data [39]	2018
Bulgaria	Law for Protection of Personal Data [40]	2019
Croatia	Act on Personal Data Protection [41]	2003
Cyprus	The Processing of Personal Data (Protection of the Individual) Law [42]	2018
Czechia	Law on Personal Data Protection [43]	2019
Denmark	Act on Processing of Personal Data [44]	2018
Estonia	Data Protection Act [18]	2008
EU	General Data Protection Regulation (GDPR) [12]	2018
Finland	Personal Data Act [45]	1999
France	Law relating to the protection of individuals against the processing of personal data [46]	2014
Germany	Federal Data Protection Act [47]	2019
Greece	Law on the Protection of individuals with regard to the processing of personal data [48]	2006
Hungary	Act on Informational Self-Determination and Freedom of Information [49]	2011
Ireland	Data Protection Act [50]	1988
Italy	Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali [51]	2003
Latvia	Law on Protection of Personal Data of Natural Persons [52]	2019
Lithuania	Law on Legal Protection of Personal Data [53]	2008
Luxembourg	Data Protection Law [54]	2018
Malta	Data Protection Act [55]	2001
Netherlands	Personal Data Protection Act [56]	2000
Poland	Act on the Protection of Personal Data [57]	1997
Portugal	Lei da proteçao de dados pessoais [58]	1991
Romania	Law on the protection of individuals with regard to the processing of personal data etc [59]	2001
Slovakia	Act on the Protection of Personal Data [60]	1992
Slovenia	Personal Data Protection Act [61]	1990
Spain	Organic Law 15/1999 on Personal Data Protection [34]	1999
Sweden	Personal Data Act [62]	1998
United Kingdom	Data Protection Act [63]	2018
United States	Privacy Act of 1974 [17]	1974

Finally, in the fourth and final step we manually compared and contrasted taxonomies to gain an idea of the evolution. Understanding personal data items at a granular level as well as the categories that they belong to allows us to make several important comparisons. There are two criteria that we use as the basis for our approach to make comparisons across taxonomies. The first focuses on the main categories of information included or excluded by the taxonomies. Identifying the main categories and their differences across taxonomies allows us to observe the diversity of personal information considered by different stakeholders and gives us a chance to explore reasons behind these expansions. The second criteria considers the general distribution of items (subcategories) within the categories common across taxonomies, and the variation between them. Exploring this provides useful insights into the extent of low-level, granular personal information items as perceived by different stakeholders; understanding such differences is particularly beneficial in tracking how personal data has evolved. In our research, we have chosen to conduct comparisons manually to avoid any items being overlooked or misrepresented.

5. Data collection

In this section, we detail the data collection process adopted to gather relevant government, industry and academic perspectives on personal information.

5.1. Government perspective

To identify the types of information which governments and legal authorities define as personal, we examined national legislations for the US, UK, European Union countries, and finally, the GDPR (which is the regulation upon which a number of relevant legislation supports). These countries and geographic areas were selected because they represent some of leading world economies and/or also host many large-scale technology companies. In order to access up-to-date legislative documents, we visited the official websites of data protection authorities and, where appropriate, accessed official translations in English.

Table 2 presents the complete list of legislations used in the study, including the respective country and the year that the legislation was last updated. The primary aim when assessing these legislations was to understand how they characterise personal information and sensitive personal information. This provides our research with the scope of personal information at the first stage of the evolution (i.e., from governments) and acts as a baseline to consider the different perspectives taken by other stakeholders (i.e., industry and academia).

There are significant differences in the ways in which individual EU member states implement the protection of privacy and personal data in national laws [64], we consider the legislations of EU member countries in addition to GDPR. This allows us to understand the coverage of personal information in each country and assess their alignment with technology on an individual basis. We extract personal information from these documents and accept an item as sensitive if it is considered sensitive in any one of the legislations. Our data collection process, which is inline with the deductive content analysis approach, involved reviewing the legislations and extracting any personal information (including any noted as sensitive or requiring extra protection) defined in the legislation. To validate the information extracted, an independent coder, who also analysed the legislations, was used. In cases where there were disagreements, these were discussed and if necessary, a judge (i.e., a third individual) was used.

5.2. Industry perspective

Industry is regularly at the forefront of the development new technologies (e.g., platforms, software and devices) and therefore is often in a position to use new and emerging types of personal information. For our work, we focus on the privacy policies of mobile apps, both Google Play Store and Apple App Store require a privacy policy to be attached to each app listing, and as such there is a requirement to list the personal information collected from individuals that use the app. Following the introduction of GDPR, organisations had to document their data handling processes, and often adjust consent forms, and privacy policies to comply with regulatory and legislative requirements [65].

Table 3
Number of apps assessed and privacy policies reviewed from the Google Play Store.

	Finance	Health	Medical	Total
Apps	250	250	250	750
Privacy policies	234	234	221	689

Table 4
Number of apps assessed and privacy policies reviewed from the Apple App Store.

	Finance	Health	Medical	Total
Apps	240	240	240	720
Privacy policies	232	230	211	673

In this study, we focused on two popular application domains where a large variety of sensitive personal data is processed; finance and health. Personal health information is a special category which is considered sensitive by the GDPR and all the legislations investigated in this study. Most mobile health apps often store and process not only health-related data but also other sensitive information such as user's location, lists of contacts or personal photographs [66]. Similarly, financial apps are also known to handle sensitive data, such as online banking credentials, investments, budgets or salaries and there is a great rise in the usage of those applications [29].

In order to collect privacy policies that relate to the these domains we searched the Apple App Store [67] and Google Play [68] Store manually in November 2019 using the categories "finance" and "medical" and "health". Those two platforms allowed the retrieval of the most popular apps for each category and also provided access to their privacy policies. We developed a tool to download privacy policies and to extract permissions listed in the web page of each application. Covering the permissions in our data set allowed us to access a complete set of personal data items accessed by the applications. A query to the Google Play Store gives a maximum of 250[2] results and the number of apps listed by the Apple Store under each category is 240.[3] Under those platform restrictions, we retrieved 1470 applications. The names of all those applications can be seen in Tables 11 to 14 in Appendix. The 108 applications that do not provide a privacy policy have been eliminated from the data set. The total number of policies analysed can be found in Tables 3 and 4. In addition to extracting privacy policies, we developed a tool to capture the permissions requested by each application. This allowed us to then manually identify and include personal information items listed in those permissions and complement findings from the privacy policies.

In summary therefore, and in line with our defined deductive content analysis approach, our data collection involved manually reviewing the apps' privacy policies and extracting any personal information that was identified (including any sensitive personal information) items listed. This information was typically found in the 'Information we collect' section of the policy. As discussed, we accepted an item as sensitive if it was considered sensitive in at least one of the privacy policies. To this, we added the findings from the analysis of permissions requested by the apps. Validation of the final set of items identified was performed using independent validation (second human content coders) similar to the process adopted for government documents. In addition to identifying self-defined personal information items, we also identified common hierarchies given in the policies to be used in the following steps.

5.3. Academic perspective

The academic community also plays a key role in understanding personal information as it tends to be a place of innovation, reflection and rigorous critique. This phase of the study aims to assess the academic literature related to personal information in the finance and health domains. As mentioned in Section 4, the process adopted was a systematic literature review, with no filter on article selection beyond its topic. This allowed us to consider any article that involved some analysis of personal information. In order to find a robust set of studies related to finance and health, we defined a set of broad keywords for each domain and searched the databases during December 2019 without time-frame restrictions. IEEE Xplore, ACM Digital Library, Springer, ScienceDirect, Web of Science and ProQuest were used as databases in which the queries were searched encompassing full text of the articles.

Table 5
Academic databases reviewed in our research.

Database	Finance	Health OR Medical
Springer	495	200
ScienceDirect	303	200
IEEE Xplore	328	200
ACM Digital Library	5	108
WoS	0	14
ProQuest	443	200
Total	1367	1014

In our initial search, we used finance or health, along with the keywords: personal data, personal information, sensitive data and sensitive information. Understandably, however, this search returned a significant number of articles, i.e., in excess of 4 million, thereby rendering that approach infeasible. To narrow the scope further (a common activity in systematic reviews [69]), we decided to include the word, taxonomy. While this would mean that potentially valuable articles (and therefore new types of information) may be overlooked, the decision would allow us to discover noteworthy categorisations of personal and sensitive information. As such we designed our search queries as follows:

> Finance: *taxonomy AND finance AND ("personal data" OR "personal information" OR "sensitive data" OR "sensitive information")*

> Health: *(taxonomy AND (medical OR health)) AND ("personal data" OR "personal information" OR "sensitive data" OR "sensitive information")*

These two queries led to more than 6000 articles in total (1367 finance articles and 4976 health articles). We reviewed 1367 finance articles but limited the health papers to 1014 articles (selected from the top 200 most relevant papers per database). The distribution of the articles reviewed can be seen at Table 5.

Following the same approach as for the legislations and privacy policies and performed a deductive content analysis on the corpus of academic articles and extracted the personal information taxonomy (including any sensitive personal information) items listed. An item was accepted as sensitive if it was considered sensitive in at least one of the articles. Validation of the final set of items identified was performed using independent checks on randomly selected articles. We also made note of common categorisations in the articles to be used in the following steps.

6. Results

This section presents the results of our assessment into how personal information is regarded, and has evolved, across the government, industry and academic domains. We structure our presentation in the context of a series of novel taxonomies of personal information derived from our analysis. Machine readable versions of all taxonomies are available in the supplementary materials.

[2] https://play.google.com/store/search?q=health&c=apps&hl=en.

[3] https://apps.apple.com/us/genre/ios-health-fitness/id6013.

6.1. Government taxonomy of personal information

Extracting personal information items from governmental documents is an important first step as it allows us to define a reference point for other stakeholder comparisons. As outlined in Section 5, to process these documents we extracted personal information explicitly defined in the legislation (including personal information identified as requiring extra control). To assist in building our taxonomy, we also made note of common categorisations in the legislations and maintained these in our work. The complete taxonomy of personal information deduced from governmental documents is presented in Table 6. In all of the taxonomies proposed in this paper we use levels and numbering to help present types of personal information (e.g., *Demographic information (1)*). Also, a second order system of numbering is used for the subcategories or information items in a category. For instance, in Table 6, *Contact information* (2.1) is a subcategory of *Personal identification information* (2); and *Phone number* (2.1.1) or *Email address* (2.1.1) are personal information items in this *Contact information* subcategory. Lastly, we present sensitive personal information in bold, as can be seen with *Racial or ethic origin* (1.1) in Table 6.

There are five main personal information categories recognised by data protection authorities: *demographic information, personal identification information, health information, financial information and judicial data*. Beyond this however, legislations do not adopt a consistent or coherent approach in their categorisations. Legislations often differ in the variety of categories they cover, there are categories, such as *judicial data*, which are handled in detail by some legislations and not explicitly identified by others. There are also differences in the level of abstraction legislations use to itemise personal information under the same top-level categories. Conversely, legislations seem to be consistent in the identification of **sensitive** personal information almost all of which list GDPR's special categories of personal information (*racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership*, and *personal data concerning sex life, personal data concerning health*) as sensitive personal information.

When considering the variety of categories covered by the legislations, *judicial data*, *personal information related to financial creditworthiness* and *social needs* are relatively uncommon categories of personal information covered by legislations. For example, *Judicial personal information* is identified in few documents (e.g., Italy [51], UK [63]), and overlooked in the majority of the legislations (e.g., Slovenia [61], Netherlands [56], Ireland [50]). The specificity within this category also differs greatly, the majority of the legislations define this type of data as personal data related to commission of an offence. However, falling victim to an offence before a public court hearing is also typified as a personal information item by the Data Protection Act of Estonia [18]. This data item is also considered sensitive as done for all judicial data. Alternatively, the UK explicitly identifies *child abuse data* [63], where Poland [57] and Portugal [58] cover wider details such as *decisions on penalty, fines and other decisions issued in court or administrative proceedings* under judicial personal information category. Portugal also mentions an abstract concept as *personal data relating to state security* which can be covered in this category. Finally, *Coercive penal procedural measures* or *administrative deprivation of liberty* are types *judicial personal data* recognised by only one country, Sweden [62].

Another uncommon personal data item, *Social welfare*, is explicitly mentioned in only three legislations: the Personal Data Act of Finland [45], the Greek Law on the Protection of individuals with regard to the processing of personal data [48] and the Italian Data Protection Act [51]. It is considered sensitive in all of those legislations. Finally, *financial creditworthiness*, is only recognised by Federal Data Protection Act of Germany [47], Personal Data Act of Finland [45] and Personal Data Act of Denmark [44].

Moving to discuss the differences in the level of abstraction of personal information items, there are inconsistencies in two main categories; *Healthcare data* and *Demographics*. *Healthcare data* is considered sensitive by the majority of legislations, however, levels of abstraction vary among the different data protection acts significantly. For instance, the legislation of Spain [34] mention health information once and it describes it as personal data relating to the health of persons. This is an example of high level abstractions which do not point to any specific health information that are collected on daily life during health care. Conversely, Italy [51] provides the most granularity for health data and address more than ten different items including *personal data related to sickness, pregnancy, child-bearing or breast-feeding, accidents, physical and mental qualifications to perform specific task*. *Addictions* is another example of uncommon, but relatively specific, personal health data which is itemised by only Poland [57] and Hungary [49]. In addition to level of abstraction, data items covered under this common category also differ, for instance, Finland [45] covers *the state of health, illness or handicap of a person* and *the treatment or other comparable measures directed at the person* whereas Lithuania [53] specifically mentions *diagnosis and prognosis*.

Another common category of data items which vary between legislation is *Demographics*. For instance in several countries such as Austria [38], Belgium [39] or Bulgaria [40], this category is limited to *name, race, colour* and *religious belief*. However another country, Italy [51], also provides personal information regarding to *education or family* within this category.

More generally, our work found that the legislations of the following countries: namely, Italy [51], Lithuania [53], US [17], Slovakia [60] and Finland [45], these tend to be far more specific in at least one of the personal information categories. This means that these list a higher number of personal data items as compared to other countries. For instance, items listed under *Online identifiers* (taxonomy item 2.3) are mainly extracted from one of those legislations, Act on the Protection of Personal Data of Slovakia [60]. The rest of the legislations limit the scope of online identifiers to IP addresses or cookies. The limitation in this category in the legislations is important considering the impact of technology specific to this category.

A key observation that can be made is with regards to re-identification. Identification is not overlooked by some legislations and *formal identifiers* (2.2) or *online identifiers* are explicitly mentioned in them. However, even in the legislations which typify several personal identification data items (e.g., Lithuania [53], or Slovakia [60]), the capacity of data items to contribute to the re-identification is not examined when they are used together. It is known that combinations of data items which are not readily recognised as identifiers have a potential to allow identification of individuals. For instance, it is reported that 87% of US residents can be identified when it is possible access their date of birth, sex and five-digit zip code [70]. Considering the increase in the amount of data available to the public, re-identification becomes a significant risk. Publicly available anonymised data have a potential to become personal again for future uses when it is possible to combine them with other data sources. Recognising those risks and providing details on the potential capacity of data items to contribute to the re-identification may help to eliminate the risk of re-identification and make the legislations more future proof.

Amongst all legislations, Italy presents the most detailed examples of sensitive personal information. For instance, *religion* which is considered sensitive by all legislations but is generally handled in an abstract way and any data that has a potential to reveal this information is not covered by the legislations. However, the Italian Data Protection Act [51] lists personal information items that can reveal the religions of a data subject and considers those items sensitive [51]. *Any information concerning leave of absence on religious holidays* or *use of canteen services* are some of the items listed in the legislation. It also presents similar details for political opinions and trade union memberships [51].

Table 6
Government taxonomy.

Level	Personal information item
1	Demographic Information
1.1	**Racial or ethnic origin**, Name, Surname, Date of birth, Title, Occupation, Native language, Education records, Duties/Status in business life, Alias, Citizenship, Signature, Date of birth, Social position, Social work data, Social work, Social position, Marital Status, Family Information
1.2	**Political Opinions**
1.2.1	**Membership of parties, Data concerning exercise of public functions and holding of political offices**
1.3	**Religious beliefs**
1.3.1	**Membership of associations or organisations with a religious or philosophical aim, Data concerning leave of absence, religious holidays, Use of canteen services, Educational purposes including the freedom to choose one's religious education**
1.4	**Social Needs**
1.4.1	**The social welfare needs, Benefits, support or other social welfare assistance received**
1.5	**Trade union membership**
1.5.1	**Associations or organisations with a political or trade-union aim, The deduction of fees due for trade-union services, Leave of absence pursuant to laws or collective agreements, Legal assistance provided by trade union-related bodies**
2	Personal Identification Information
2.1	Contact Information
2.1.1	Full Name, Address of the place of residence, Street, Number of the house, Number of the apartment, Location data, Fax number, Phone number, Email Address
2.2	Formal Identification Numbers
2.2.1	Social security number, Driver's license number, State identification card number, Insurance policy number, Passport number, Number of the identification document, Personal identification numbers
2.3	Online identifiers
2.3.1	IP Address, Log in data to online services, Identifiers provided by an application, Cookies, Log in data to online services, Radio frequency identification tags
2.4	**Physical identity/Biometric Information**
2.4.1	**Finger prints, Palm prints, Eye iris images**, Image Data, Video Data, Sound Data
2.5	Physiological identity
2.6	Genetic identity
2.7	Mental identity
2.8	Economic identity
2.9	Cultural identity
2.10	Social identity
2.11	**Genetic information**
3	**Health Information**
3.1	**Mental Health, Health of family members or co-habiters, Physical qualifications, Mental qualifications, Addictions**, Health insurance information
3.2	**State of Health**
3.2.1	**Risk factor exposure**
3.2.2	**Illness or handicap of a person**
3.2.2.1	**Disabilities, Accidents, Sick leave,**
3.3	**Provision of health care services**
3.3.1	**The treatment directed at the person,** Records of physical examination, Diagnosis, Prognosis
3.4	**Women's Health**
3.4.1	**Pregnancy status, Information related to child bearing, Information related to breast-feeding**
3.5	**Sex life, Sexual information**
4	Financial Information
4.1	Financial Conditions, Credit/creditworthiness data, Consolidated debtor files, Type and the amount of the requested and denied financial obligations, The types, the amount and the terms of performance of existing financial obligations, Data about the performance of financial obligations, Previous financial obligations and their performance, Employment status, Employment history, Bank account number, Credit card number, Debit card number
5	**Judicial Data**
5.1	**Punishment or other criminal sanction, Closed court sittings in civil matters, Decisions on penalty/fines, Criminal convictions**, Child abuse data

Given the fact that the personal information itself is amorphously defined in the legislations, and is not typified clearly, it is likely difficult for data subjects to understand when they have the right to be informed of the personal data processing. For instance, even if it is clear that the religion of a person is a sensitive personal information and it cannot be processed without a lawful basis, it is unclear if leave of absence on religious holiday should be considered sensitive as done in Italy. Or, it is not easy to know if data controllers are under obligation to keep this type of personal information with further protection. For the categories which are covered in some legislations but ignored by others (such as *social needs*), it is even more challenging to interpret how to process the information lawfully without further guidance.

6.2. Industry taxonomy of personal information

Mobile health apps can be divided into two categories: apps for consumers (i.e., patients or the general public) and apps for health professionals. Health apps for consumers form a majority of the apps in our set and include several types of applications spanning mental health, women's health, scheduling and reminders, self-monitoring and symptom checkers. Types of apps for professionals include patient health tracking, remote patient monitoring or appointments and clinical assistance. This wide variety of apps, and their respective privacy policies, allowed us to collect large range of health data and thus, to construct a comprehensive taxonomy. This variation also evidences the impact of mobile applications on the scope of personal information.

For instance, health and activity tracking apps' (e.g., Google Fit: Health and Activity Tracking [35], Health Tracker [71] or Mi Fit [72]) privacy policies provided several *body metrics* (1.4), *activity data* (1.8) and *diet information* (1.1). Further details can be viewed in the Appendix, in Table 7. On the other hand, apps dedicated to women's health provided details regarding *menstrual cycle* (1.6.1) or *pregnancy* (1.6.2). Apps developed to improve or track some other health issues such as sleep or diet allowed us to identify different types of personal information that may be otherwise overlooked. Sleep cycles, snoring episodes, calorie intake or allergies can be given as examples. Apps for professionals process personal information mainly related to access to care (1.10). The majority of the *formal identification information* and *demographics* represented in our taxonomy are also informed by the personal information captured by those applications.

The personal information processed by mobile apps are not limited to the ones that users provide directly or the ones generated through the use of services. As we discovered in our analysis, apps also collect information through automated means. *Technical device information* (6) including both *PC information* and *mobile phone information* is an example to this type of information. Apps may also access several *online identifiers* (7.1.2), *browser information* (7.1.4.4) and details related to *phone calls* (7.2) automatically. Finally, third party services also provide personal information to mobile apps. *Social media data* (7.1.3) gathered from social networks such as Twitter or Facebook are presented in the privacy policies as information processed by the apps.

For the finance app category, Credit Referencing Agencies (i.e. a third party) are often used by apps to collect personal information on users. *Credit score* and *credit reports* are obtained from those agencies on users behalf. Apps in the finance category handle extremely sensitive data, such as online banking credentials, investments, budgets, salaries or assets that its users possess. The main categories of finance information found are *income information, credit or debit account information*, and *payment information*.

Generic personal information (other than finance related ones) extracted from financial apps also differs from the health taxonomy. Differently from health apps, *criminal records* are processed in finance domain. In addition, properties or assets possessed by the users are the other types of personal information which are covered by several finance apps' privacy policies. Compared to the health taxonomy, there are also some minor differences in the demographics where *size of household* or *information related to relations of the people* are covered by those policies in more detail. The complete taxonomy can be referenced as necessary; see the Appendix, Table 8.

In summary, personal information items extracted from privacy policies constitute the largest taxonomy in this study. Similar variations observed among the legislations are also valid for personal information categorisation on privacy policies of mobile apps. Categorisation of personal information in means of sensitivity is handled differently by different privacy policies. For instance, in some of the privacy policies *body metrics* (1.4) are considered sensitive and the ones itemised in those policies are labelled as sensitive in our proposed taxonomies due to our strategy of labelling. However, in another privacy policy that collects some other body metrics, those information may not be considered sensitive which yields different sensitivity labels under the same category. As seen in Table 7, *blood pressure* is considered sensitive whereas *cholesterol* is not. In our opinion, such kind of variation does not point to the different sensitivity levels of similar metrics but it reveals different perceptions of sensitivity within industry (and specifically, for developers of apps).

6.3. Academic taxonomy of personal information

Our motivation to review academic articles is twofold; identifying existing personal information taxonomies and understanding the new types of personal information recognised by researchers in different domains. The limited number of taxonomies proposed in the literature have been covered in Section 2 which are specific to personal information in OSNs [27], wellness data [26] and law enforcement cross border access to evidence [25].

Apart from those studies, we have reviewed the articles in our data set extracting the data items considered as personal information by researchers. This approach allowed us to observe different personal information that reflects the impact of different technologies or applications. *Security data* ((8) in the Appendix, see Table 9 for further details) that covers information varying from *audio recordings* to *speed radar photographs* can be given as examples to personal information that emerge with application of new technologies.

The variety of items in *biometric information* also evidence this change in the perspective and coverage of personal information. Details of this category has been extracted from the study of Ribaric et al. [73] in which the researchers identified personal identifiers in multimedia content that should be removed to de-identify it. Ribaric et al. classified those identifiers as non-biometric, physiological and behavioural biometric, and soft biometric identifiers. In addition to traditional physiological biometrics such as *fingerprints, palm prints* or *iris shape*, researchers listed some other biometrics such as *lip motions, style of typing* or *gestures* under behavioural biometric category. The study proposes soft biometrics as vague physical, behavioural or adhered human characteristic that is not necessarily permanent or distinctive and thus does not provide a reliable personal identification, but can be used for improving the performance of recognition. *Height, weight, eye colour* or *silhouette* are given under this category ((2.3.1) in Table 9).

Working on academic articles also allowed us to observe different categorisation techniques of personal information. For instance, Kwon et al. provided Privacy Sensitivity Matrix where researchers divided personal information into four as; information whose disclosure would be regarded as unapproved, information which is already or conditionally open to the public, information which can be used in identity theft and finally information with which one can potentially point to a specific person [74]. Researchers cover *medical and health information, education* and *income records* or *log tracks of pornography websites* in the first category. Demographics such as *birthdays, birth places, gender* or *occupations* are given as information which are already or conditionally open to the public. Personally identifying numbers such as *social security numbers* is listed in the third category, those that can be used for identity theft. Finally *full name, face* and *e-mail address* are given in the fourth category via which one can potentially point to a specific person [74].

Another interesting categorisation is given based on the possible connections between "information" and "me" [75]. Jones groups the personal information into six as information owned by me; about me; directed towards me; sent or published by me; experienced by me or, relevant to me. Files on our computer's hard drive are exemplified under owned by me; Web browsing and library books checked out are given for the category about me, *Phone calls* and *web ads* for Directed towards me; *E-mail* for sent or published by me; *Web pages that remain on the Web* for experienced by me and finally *house, job* and *life-long mate* are given in the category relevant to me [75]. Those categorisations are valuable to provide insight about the scope of personal information from different perspectives.

Reviewing some articles also enabled our research to cover domain specific personal information. The study of Presser et al. enabled us to observe health data processed by care.data, an NHS England initiative to centralise patient health and social care data [76]. The study provides the details of the personal information processed by healthcare systems in the UK. Such kinds of studies facilitate an analysis of personal information that exists in society today and therefore can enrich our taxonomies accordingly. This variety of articles gives us the largest set of sensitive personal information thus far; all of which can be seen in Table 9. The potential reasons behind the academic taxonomies having the largest set of sensitive data items are discussed in Section 7.3.

The query we used to collect finance articles returned several studies regarding the dark side of the Internet which explore how financial personal information is abused via techniques such as hacking, phishing, denial of service attacks or click fraud etc. Those studies not only provided financial personal information but also highlighted their sensitivity due to their potential to be misused [77]. The list of personal data items extracted from finance articles are given in Table 10.

6.4. Differences across government, industry and academia

After investigating how personal information was regarded in governments, industry and academia, in this subsection, we highlight the main disparities across these stakeholders and provide an insight into how personal information or its sensitivity is perceived differently across them. These points were identified through a robust comparison of the taxonomies as outlined in the methodology section (step four in Section 4). Manual comparisons were particularly useful as these allowed us to accommodate for variations in levels/hierarchies of information and slightly different wordings in how information was presented. For instance, through these comparisons we could observe how a conceptual-level informational item such as Financial conditions (5.1 in Table 6) in legislations is conveyed more definitively by industry (in mobile applications) with concrete examples (including Monthly rental income, Annual personal income, Annual household income etc., 1.1.1 in Table 8). Even though it is trivial to give and compare number of nodes in taxonomies, we avoided making comparisons through them (information items) since abstraction level of each node highly differs. The contribution of nodes with generic and inclusive items such as Financial condition or Health status are highly different from the ones with concrete, measurable data items such as Bank Account Number, Balance or Blood glucose. Therefore, throughout our comparisons we present and discuss a number of subcategories and a level of abstraction for more meaningful comparisons.

To start with government and academic views of personal information, our comparison revealed several differences. For instance, from the systematic and critical review of legislation and regulation of PII from around the world, we identify that the majority, even those updated recently, provide personal information at an abstract level (Health information, online identifiers, etc.) and often exclude new personal information items that emerge due to new technologies such as a virtual currency account information or soft biometrics. This is clearly different to what was found in academia, which hint towards the progression in pieces of personal information.

The differences in the government taxonomy in a PII context as compared to academia can be observed generally in Fig. 2. In this figure, items in grey represent personal information covered by legislations; green items represent the ones covered by academic articles and the yellow items are personal information covered by both of the sources. Data items written in bold and underlined represent the personal data items considered sensitive by the researchers (sensitivity categorisations in legislation are not demonstrated in this figure to aid readability). It is important to note here that PII items (except for some biometric information such as fingerprints, palm prints, iris pattern/eye iris image) and Genetic information are not considered sensitive in legislations. All of the genetic information and the majority of the online identifiers (9 items out of 14) are also overlooked by legislative frameworks.

Additionally, Fig. 2 displays the evolution of contact data and the gap between contact data processed in today's world (as explored by research) and the ones recognised by legislations. The majority of the contact data accessible from portable devices and soft biometrics are not present in legislative frameworks. And, further to this point, two substantial categories in academic taxonomies, i.e., Communication data (7 in Table 9) and Security data (8) are also not acknowledged by them. Considering the massive amount of Online communication data (7.1) processed today and the variety of security data collected via CCTVs, speed radars or scanners at airports etc., re-evaluation of scope of personal information in legislation seems critical.

A similar scarcity in the scope of the personal information of the legislations as compared to academic taxonomies was observed regarding health information. The limited number of data items provided in legislations are related to the health status of individuals and the health care services. Fig. 3 presents the taxonomy created within the healthcare domain from international regulation and legislation; items written in bold and underlined are those that are considered sensitive within the legislations. As can be seen in the figure (Fig. 3), the items found pertaining to personal health information are typically conceptual definitions which do not specify atomic, measurable data items and thus, leave room for interpretation. However, several measurable items can be seen in academic taxonomies under the subcategory of Body metrics (1.4 in Table 9) or Diseases and Diagnosis (1.7). Details regarding the medical appointments such as data of admission to hospital or scheduled visits are also present in them in contrast to the government taxonomy. Besides, those data items are also considered sensitive by some researchers. Conceptual definitions in legislations for Women's health (1.6, Table 6), Mental Health (1.9) and Addictions (1.11) are also elaborated in academic taxonomies as can be seen in Table 9.

Differences in the level of abstraction across government and academia are also valid for financial information. For instance, conceptual definitions including Financial conditions or Creditworthiness data given in legislations are detailed into five subcategories in academic taxonomies as Income information, Credit account information, Debit account information, Payment information, and Data processed by CRA (Credential Referencing Agencies) (see 1 in Table 10).

Moving next to compare government and industry taxonomies, we found that the largest gap between the taxonomies was observed here in the scope of health and finance information. In addition to those categories which are very detailed in our industry taxonomies, generic information such as demographics or PIIs also highly differ across government and industry; i.e., a substantial extra amount of information items are present in the industry taxonomies. Information about social identity covered in the legislations such as Family information or Marital status is greatly supplemented in industry taxonomies, with additional subcategories such as Relations (3.4.2 in Table 8) or Thematic interests (3.4.3).

As stated before, mobile applications analysed in this study are typically dedicated to very specific health issues and process a variety of metrics specific to those issues. Body metrics, physical features, or activity data are heavily processed by these applications; all of which are overlooked by legislations. The variety of women health data processed by the applications also go beyond the data as perceived by current legislations. This is certainly a striking disparity, but one which again suggests legislation as either lagging behind industry progress or purely opting for more abstract views of information, potentially in a debatable attempt to future proof itself.

For comparison, we present the industry taxonomy for personal health information in Fig. 4 where items written in bold and underlined are those that are considered sensitive within this corpus.

For a more accessible visualisation of the structural differences between these taxonomies (Figs. 3 and 4), we present Fig. 5 which highlights the structure of the two taxonomies — the differences are clearly salient. In the near-term we may also expect the disconnect to only increase given the prevalence of sensors in IoT technologies, such as smart watches, clothes and shoes; with this in mind, it is reasonable to expect an increase in both the volume and diversity of PII being processed.

Similar problems are also apparent in the finance domain. In the taxonomy derived from regulation, Credit Card Number is present, however, other details that are used by the applications to authenticate users or to secure their information are ignored, information such as CVC, Expiry date or security code are all missing. Virtual wallets

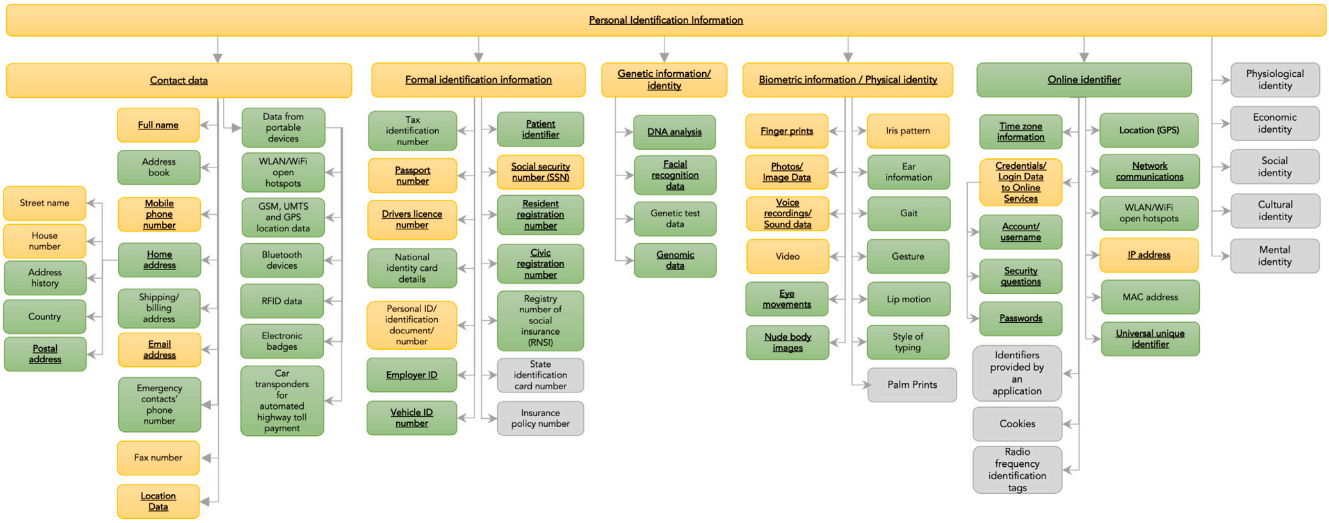

Fig. 2. Personal Identification Information in the Government and Academic Taxonomies.

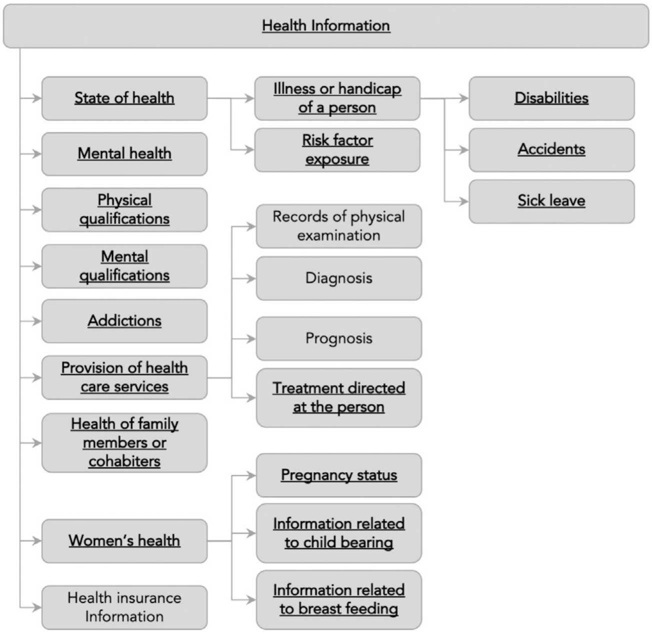
Health Information
State of health
Mental health
Physical qualifications
Mental qualifications
Addictions
Provision of health care services
Health of family members or cohabiters
Women's health
Health insurance Information
Illness or handicap of a person
Risk factor exposure
Records of physical examination
Diagnosis
Prognosis
Treatment directed at the person
Pregnancy status
Information related to child bearing
Information related to breast feeding
Disabilities
Accidents
Sick leave

Fig. 3. Personal Health Information in the Government Taxonomy.

which are becoming one of the most important forms of money transfer mechanisms [78] introduce a new personal data-item (1.5 in Table 8) which are not directly accounted for in legislations. As the finance sector continues to innovate and seeks to find new mechanisms for supporting an increasingly digitised society, it is possible to argue that industry taxonomy will further expand with new personal data items to support this innovation and challenge current regulations.

Final comparisons can be made between academia and the industry taxonomies. The items recognised by researchers but not by the industry taxonomies are especially important since they hint the new types of personal information that has emerged (or will emerge) due to new innovations; such innovations will potentially involve data being processed by applications in the near future. Soft-biometrics (2.3.1 in Table 9) can be given as a good example since, similar to government taxonomy, they are not present in the industry taxonomies. Contact data from portable devices (2.6.3 in Table 9) are also only noted by academic articles. As IoT devices become increasingly popular, it may be reasonable to expect more mobile applications to process data coming from those devices. Derived data present in the academic taxonomies such as Behavioural analysis using GSM (3.3.1 in Table 9) or Spending patterns (1.4.1 in Table 8) are given as relevant examples. Such kinds of data inferred from other data collected from individuals may inevitably processed by applications, even though we did not find any of them explicitly mentioned in the privacy policies.

As may be expected, industry taxonomies can also include some detailed, and more measurable health information compared to academic taxonomies. It is the same for financial information. It is especially noteworthy to view a large amount of financial information processed by CRAs such as Credit scores or Insolvency related events in industry taxonomies. Those highly confidential information are accessible via several mobile applications. The lack of these details in academic articles may be interpreted as a hint to an under-researched area in data privacy studies that needs more attention.

7. Discussion and implications

This paper has sought to conduct a critical investigation into personal information as understood in society today, and consider how it has evolved due to technological advancements. We are particularly interested in how this type of information is regarded across government, industry and academic stakeholders, and how the sensitivity of several specific sets of information are perceived. We will discuss the specific findings in this section.

7.1. The challenge of providing future-proof legislations

As presented in Section 6.4, legislations tend to provide personal information at an abstract level. Two explanations can be proposed for this finding, the first, that the legal frameworks' adoption to new technical standards takes much longer than technical development is already identified within the literature [25]. However, it is also possible to argue that fine-grained personal data items are not explicitly covered by legislation or regulation intentionally and instead, personal information is covered conceptually with the aim of enabling legislations to sustain their value into the future.

In any case, the abstract level (i.e., with less granularity) of personal information listed in the legislations leads to a significant discontinuity (as measured by the criteria outlined in Section 4) between the government taxonomy and the taxonomies generated from industrial practice and academia. There are subcategories which are not covered

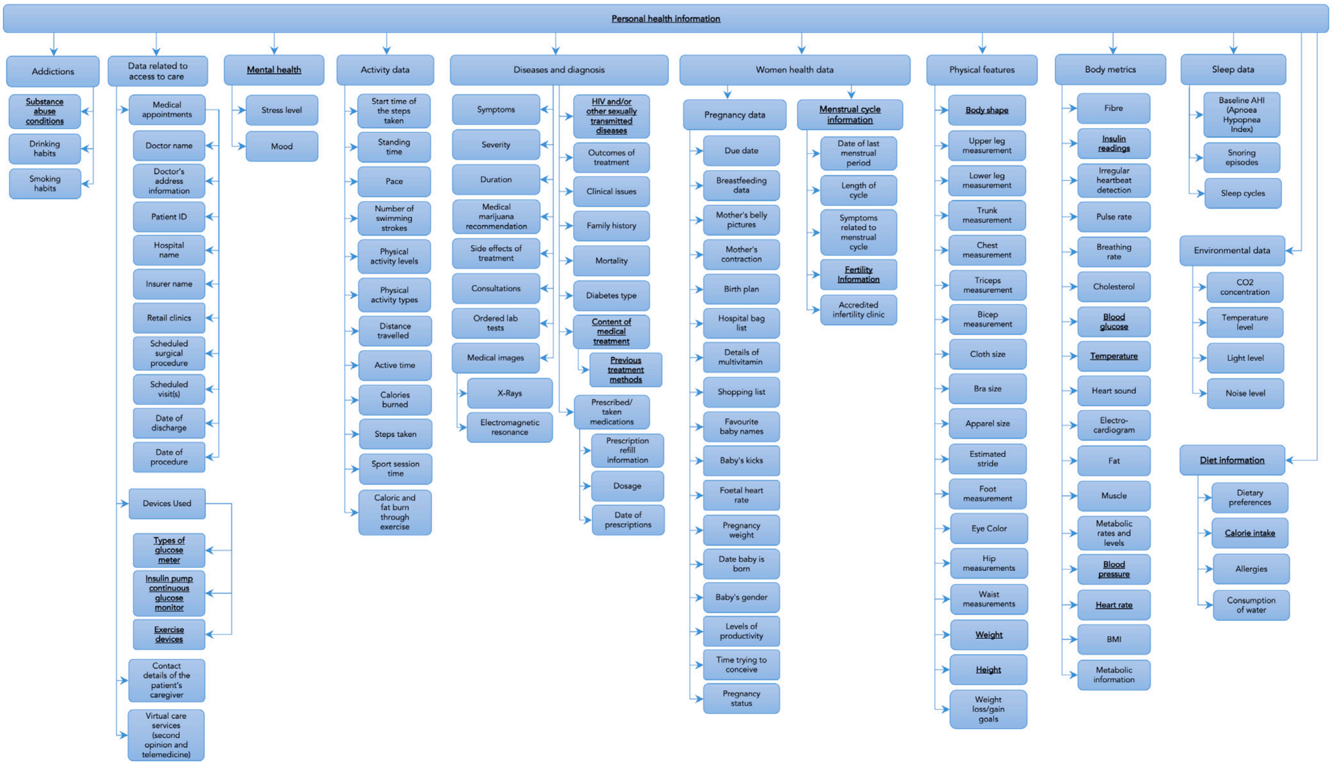

Fig. 4. Personal Health Information in the Industry Taxonomy.

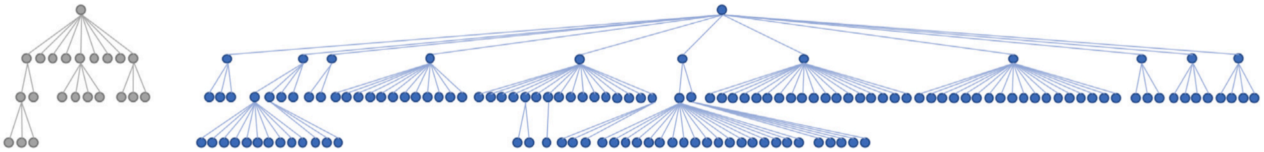

Fig. 5. A Structural Comparison of Personal Health Information in the Government Taxonomy (left, grey nodes) and the Industry Taxonomy (right, blue nodes). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

by the legislations and a number of data items under common categories highly differ. This reveals the fundamental disconnect between the personal information considered in the legislations and the ones processed in practice.

One of the top-level goals of legislation and regulation is to guide and support industrial practice, this disconnect between high-level abstract understanding of PII and low-level granularity required in practice compromises this goal. In essence, Industry, in our case mobile App developers, need to collect measurable, atomic, low-level elements of PII, this is currently poorly supported by the abstract high-level understanding of PII within the regulatory and legislative guidance.

Similar problems are also valid for personal health information collected via apps or IoT devices. Levallois-Barth and Zylberberg [26] claim that it will be possible to infer the prevalence of certain pathologies using information in the 'near future'. Consequently, even though those data items are potentially not sensitive when considered in isolation, in the 'near future' they might combine to create very real privacy concerns. In this context, another fundamental conflict arises for legislations; not only does recognising fine grained personal data items prohibit the building of future-proof regulation, **not** capturing the implications of analytically combining an increasingly diverse set of data types risks leaving the threat of both re-identification, or the inference of sensitive information, with no legislative or regulatory control.

The finance domain provides another good example, this domain saw the greatest increase in downloads across key markets, with an average increase of 27.8% in 2019 [29]. Finance mobile apps process diverse ranges of information to provide a wide range of services. As mentioned in Section 6.4, innovations in this sector will lead several new types of personal information to be processed and challenge policy makers to keep pace with the rate and scope of change.

In conclusion, current regulatory and legislative practice faces a significant problem. There is currently a fundamental disconnect between the abstract level of regulation and the discrete, low-level requirements of industrial practice. This results in a lack of regulatory guidance and support for those building and shaping the applications that we use on a daily basis. This disconnect is only likely to increase, the fastest growing areas in mobile technology include finance and healthcare — two of the areas where there are significant volumes of PII and domains where the unintended disclosure or inappropriate use of can have significant consequences. If regulatory and legislative bodies seek to close this gap by making the regulation very specific they risk becoming outdated quickly and unable to iterate new versions of guidance to support industry and research at the bleeding-edge.

7.2. The benefits of personal information categorisation

Even though the main motivation in this study is to observe the evolution of personal information, the taxonomies built for this purpose are also valuable on their own. The details that we present in our taxonomies contribute to the novelty of the research given that existing studies only focus on personal information in specific domains such as social network data [27] or propose conceptual categorisation options [75].

The most similar paper can be given as the one proposed by Levallois-Barth and Zyllberberg which proposes a taxonomy for wellness data [26]. The researchers categorised this data into three as; Quantified Self, Predictive Personalisation and Health Data. Their itemisation under Health data is limited to conceptual definitions such as health status, information about the provision of health services, their payments, eligibility for healthcare and information about the individuals collected in the course of the provision of health services. Considering the number of items covered under this category, our taxonomy provides a much more comprehensive and detailed information. Several categories proposed in this study such as Addiction, Women Health, Body Metrics or Sleep Data are overlooked by Levallois-Barth and Zyllberberg. We hope the variety of our taxonomies to allow to address data privacy problems regarding personal health data much better which is not very possible when we do not know the scope of it well.

For instance, the health data extracted from privacy policies (see Fig. 4) reveal that a significantly higher number personal health information have been collected via mobile applications than it is processed by healthcare systems in UK [76]. With the explosion of sensors in the IoT, such data collection is becoming more ubiquitous and raise new privacy concerns. For instance, prospective use cases may cover sharing those data with health professionals or even insurance companies [26]. Despite their benefits on monitoring one's health and accessing more personalised medicine and more effective treatments, this will raise several privacy concerns increasing the risk of discrimination, especially for people suffering from rare diseases or people with behaviours that are considered as unhealthy (drinking alcohol, smoking, low active hours) [26]. Our taxonomies enable to observe the explosion of personal information processing and have a potential to feed into several privacy studies.

In brief, based on a literature survey and on reviewing privacy policies and several legislations, we identify various types of personal information and create a taxonomy of personal information. To the best of our knowledge, this is the first study that provides taxonomies dedicated to personal information in general with low level itemisation for each category. Simply knowing the class of a personal data item that is being processed and its sensitivity will support the transparency enabling the assessment of the risk involved in the processing. Categorising data in relation to the degree of identifiability also allows to check whether the security obligations have been complied with. Our categorisation in academic taxonomies also allow to observe new types of PIIs processed by cutting edge technologies. Soft biometrics such as lip motions or style of typing or contact data retrieved from portable devices (such as RFID data) can be given as examples to personal information that are provided only by academic articles. Considering the risk of security breaches and data leaks, especially when these devices are used by people unaware of their vulnerabilities, it is important to keep those data items under this category to support ensuring appropriate safeguards for them.

Finally, classifications proposed in this study can help researchers identify areas that could be standardised such as demographics or biometrics. This may be further supported through the machine-readable taxonomies (which implicitly contain classifications, hierarchies and extensive lists of information items) that we have contributed as an output of this article's research.

7.3. Impact of environment where personal information is held

The impact of technological developments on personal information is not limited to the increase in volume or variety of data items. The increase in the variety of environments where personal information is stored and processed also introduces a series of new privacy and security concerns. For example cloud technologies or distributed ledgers all challenge the traditional storage and analytic paradigms which privacy regulation and legislation were designed to support. These fundamental changes in storage and analytic capability adds challenges which, at present, legislation is unable to support. At a practical level there are challenges around the management and location of data when using distributed systems, indeed some technologies are fundamentally challenged by 'deleting' data. For example, would an individual enacting their 'right to be forgotten' under GDPR be content for their data to continue to exist in a database but with an index entry deleted so the data could not be found? Would that same individual accept that a file deleted on a disk-based file system effectively follows the same process? These are complexities which those using modern distributed storage mechanisms require regulatory guidance.

Going beyond the more simple mechanistic data management issues there are many emergent analytic platforms which provide industry and individuals (whether with malicious or non-malicious intent) very powerful computational capability. This results in enabling a re-identification and inference risk beyond anything that existed previously, traditional anonymity approaches may function acceptably within a static information environment. However, we clearly do not exist in a static information environment, new data is continually being generated and either intentionally or unintentionally this data is released providing an increasingly diverse set of PII. The ability to combine these diverse data sets to infer potentially sensitive information from information that is not sensitive provides a significant risk that current legislation is not designed to protect.

As discussed previously in Section 6.3, the taxonomies of PII generated from academia provide the largest set of sensitive personal information in this study. Outside of PII, researchers also consider information on education, occupation and even thematic interests sensitive. There are two main reasons behind the high number of personal information considered to be sensitive in academic taxonomies. The first is that research focusing on privacy in cloud technologies tends to consider personal information as sensitive because it may be at greater risk of exposure. And secondly, within the large-scale data research domain personal data items which are non-sensitive in isolation are considered sensitive when combined with other data items.

This variation in sensitivity of information can be seen to map to a temporal dimension where a given data set may become more sensitive once it is stored in a different environment alongside other data sets. We posit that even though the current legislative frameworks define sensitivity based on the data-type, the environment in which the data is stored, the possibility of it being combined with other data items should be considered while developing the categorisations going forward. In the future, legislation may encourage different categorisations for different technology platforms encapsulating those technologies at appropriate risk levels. For instance, PII stored on cloud services may be more prone to become more sensitive personal information than the ones stored on centralised (or in-house) databases.

8. Limitations

In our study, we have followed a data-driven approach and built our taxonomies based on documents we collected. Due to language restrictions, we could not cover context specific laws in health and finance domains. Since identifying those specific laws for each country and finding official English translations are not trivial, we limited our study to the general legislations provided on the website of the national data protection authorities.

Another limitation is in the scope of privacy policies reviewed. Limiting the privacy policies to the ones that belong to health and finance apps allowed us to focus on those major personal information categories, particularly those that may be sensitive. However, this decision means that other domains such as games, lifestyle or business were not addressed. The implication of this decision is that some personal information areas may not have being covered or other areas may have been over-represented, thus introducing bias into the study. We accept this as a practical limitation of our work, and recommend that readers interpret our findings with this scope in mind.

The main limitation of our systematic literature review process is eventual omission of papers and bias in our search queries. We may have missed relevant papers due to the possible existence of relevant papers that do not mention the keywords we specified explicitly. It may be possible to enrich taxonomies through more generic queries without narrowing down the results with the word taxonomy such as *"personal data" OR "personal information" OR "sensitive data" OR "sensitive information"*. However, we would suggest that any significant synthesis activity is likely to result in an taxonomy being constructed and our search will identify such papers.

Due to our strategy of labelling personal data items as sensitive, we accepted an item sensitive if it is considered sensitive in at least one of the documents in the corresponding data source. A more nuanced approach may have identified some variations but it is unlikely to structurally affect the resulting taxonomies or insight. Finally, we have considered all three domains to be static 'snapshots' of their relevant domain/stakeholder and there may be small temporal anomalies due to e.g. differences in the publication dates of particular legislations, however since we are synthesising over a large corpus we anticipate some of this variation is removed.

9. Conclusion and future work

As technology continues to advance, sharing personal information will be indispensable to participation in modern society. In addition to the increase in the amount of personal information processed online, new types of personal information or even new categories will appear as new technologies are both created, shaped and adopted by society. These rapid changes in technology introduce several challenges for society, particularly for data protection authorities in developing forward-looking legislations adequate to address the changing nature of personal information.

In this study, in order to highlight the issues pertaining to how personal information is regarded, we developed a series of personal information taxonomies from three key stakeholders: Government legislations, App privacy policies (representing current practices) and academic articles. These taxonomies allowed us to observe the variation of personal information at a granular level. Our findings reveal how the personal information in several categories such as health, finance, demographics or personal identifying information have expanded due to increased engagement with technology for several purposes and to emergence of new personal data items with new technological improvements such as virtual wallets. It also highlights fundamental disconnects between the abstract description of classes of PII by legislation and the discrete, atomic nature of the data points collected in practice.

Even though the motivation behind building these taxonomies was to observe the variation in the personal information scope, our taxonomies are also valuable on their own. The categorisation of personal information at such a granular level has not been done within academia, and it can form the basis for better data understanding and protection. Furthermore, it can increase the transparency of personal data interaction both for industry and individuals, i.e. the processors and users generating information.

A primary avenue of future work is on the further development of these taxonomies to improve their accuracy in sensitivity labels. It is known that the perceived sensitivity of a particular type of information varies widely both between societies and ethnic groups, and that an information type might be considered sensitive in one context and non-sensitive in another [11]. Through conducting user studies, we aim to assess impact of cultural differences on perceived sensitivity which will also enable us to gather sensitivity levels in a spectrum. This approach will enable us to, for example, differentiate the sensitivity levels of name and HIV status both of which are considered sensitive in our taxonomies, but we would hypothesise exhibit different 'degrees' of sensitivity.

We are also considering improving our academic taxonomies by fine tuning our search queries according to our findings in this study. Since the evolution of personal information has been observed to be around the improvements in Big Data, IoT or OSNs, we could review the studies in those domains and to identify personal information covered in those specific technological improvements.

In summary, the evidence from this study suggests that the categorisation of personal information requires a critical re-evaluation in today's data-driven world. Those emerging techniques create enormous value for the global economy, driving innovation, productivity, and efficiency in several sectors. However, they also raise several privacy concerns. In order to craft a better balance between these benefits and the protection of individuals privacy, policymakers must develop more timely and apt approaches to address the concerns raised by such technologies. This is critical to ensure appropriate protection for personal data since amorphously defined personal information in the legislations leave room for interpretation for technology developers and challenge lawful processing. We call for more research into the interfaces between data protection law and the technology developers to overcome outdated conceptualisations resulting in poor legal frameworks. We hope that our taxonomies, which provide key perspectives of different stakeholders, can act as a valuable foundation for those discussions.

CRediT authorship contribution statement

Rahime Belen Saglam: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing. **Jason R.C. Nurse:** Conceptualization, Methodology, Investigation, Writing – review & editing, Validation, Supervision. **Duncan Hodges:** Conceptualization, Methodology, Investigation, Writing – review & editing, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was conducted as a part of a UK EPSRC-funded project, A Platform for Responsive Conversational Agents to Enhance Engagement and Disclosure (PRoCEED) (Grant number: EP/S027297/1 and EP/S027211/1).

Appendix

See Tables 7–14.

Appendix B. Supplementary data

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.jisa.2022.103163.

Table 7
Industry taxonomy: Health.

Level	Personal information item
1	Health Information
1.1	Diet Information
1.1.1	**Calorie intake**, Dietary Preferences, Allergies, Consumption of water
1.2	Environmental Data
1.2.1	CO2 concentration, Temperature level, Light level, Noise level
1.3	Sleep Data
1.3.1	Baseline AHI (Apnoea Hypopnea Index), Snoring Episodes, Sleep cycles
1.4	Body Metrics
1.4.1	**Insulin readings, Blood glucose, Temperature, Blood pressure, Heart rate**, Fibre, Irregular heart beat detection, Pulse rate, Breathing rate, Cholesterol, Heart sound, Electrocardiogram, Water percentage, Fat, Muscle, Metabolic rates and levels,Body mass index (BMI),Metabolic information
1.5	Physical Features
1.5.1	**Body shape, Weight, Height**, Upper leg measurement, Lower leg measurement, Trunk measurement, Chest measurement, Triceps measurement, Bicep measurement, Cloth size, Bra size, Apparel size, Estimated stride, Foot measurement, Eye Colour, Hip measurements, Waist Measurements, Health/ weight loss/gain Goals
1.6	Women Health Data
1.6.1	**Menstrual cycle information**
1.6.1.1	**Fertility information**, Date of last menstrual period, Length of cycle, Symptoms related to menstrual cycle, Accredited infertility clinic
1.6.2	Pregnancy Data
1.6.2.1	Pregnancy status, Due date, Breastfeeding data, Mother's belly pictures, Mother's contraction, Birth plan, Hospital bag list, Details of multivitamin, Shopping list, Favourite baby names, Baby's kicks, Fetal heart rate, Pregnancy weight, Date baby is born, Baby's gender, Time trying to conceive, Levels of productivity
1.7	Diseases and Diagnosis
1.7.1	**HIV and/or other sexually transmitted diseases**, Symptoms, Severity, Duration, Medical marijuana recommendation, Side effects of treatment, Consultations, Ordered lab tests, Outcomes of treatment, Clinical issues, Family history, Mortality, Diabetes type
1.7.2	**Content of Medical Treatment**
1.7.2.1	**Previous treatment methods**
1.7.3	Prescribed/taken medications
1.7.3.1	Prescription refill information, Dosage, Date of prescriptions
1.7.4	Medical Images
1.7.4.1	X-rays, Electromagnetic resonance
1.8	Activity data
1.8.1	Physical activity levels, Physical activity types, Active time, Calories burned, Start time of the steps taken, Standing time, Pace, Number of swimming strokes, Distance travelled, Steps taken, Sport session time, Caloric and fat burn through exercise
1.9	**Mental Health**
1.9.1	Stress level, Mood
1.10	Data related to access to care
1.10.1	Virtual care services (second opinion and telemedicine), contact details of the patient's caregiver
1.10.2	Medical appointments
1.10.2.1	Doctor name, Patient ID, Hospital name, Doctor's address information, Insurer name, Retail Clinics, Scheduled surgical procedure, Scheduled visit(s), Date of discharge, Date of procedure
1.10.3	Devices used
1.10.3.1	Types of glucose metre, Insulin pump continuous glucose monitor, Exercise devices
1.11	Addictions
1.11.1	**Substance abuse conditions**, Drinking habits, Smoking habits
2	Personal identification information
2.1	Formal Identification Information
2.1.1	**SSN, Passport number, Drivers licence number, Personal ID/ Identification document**, Tax identification number, National identity card details, Medical record number, Health record number, National provider identification ("NPI") numbers
2.2	Genetic Information
2.2.1	DNA analysis, Facial recognition data
2.3	Biometric information/Physical identity
2.3.1	Finger prints, Photos, Voice recordings, Video
3	Demographic Information
3.1	**First Name, Family Name, Gender, Signature, Date of birth, Age, Marital/Relationship status, Religious beliefs, Political opinions, Trade union membership**, Nick name, Title, Mother's maiden name, Driving Licence Details
3.2	Information on education
3.2.1	Attended schools and universities, Qualifications
3.3	**Contact Data**
3.3.1	**Full Name, Home address, Mobile phone number,Email address**, Home Phone Number, Fax Number, Shipping/Billing address, Emergency contacts' phone number, Security phone number, Security email address, Work email address, Postal address
3.4	Social Identity
3.4.1	Family history, Living with a partner/spouse
3.4.2	Relations
3.4.2.1	Children, Spouse, Friends

(*continued on next page*)

Table 7 (*continued*).

Level	Personal information item
3.4.3	Thematic interests/ preferences
3.4.3.1	Hobbies, Leisure activities, Favourite scent, Having pet
3.4.3.2	Content Consumption
3.4.3.2.1	Movies watched, TV Shows watched, Marketing preferences, Apps/Games, Engagement with advertisements
3.5	Racial or Ethnic Origin
3.5.1	Nationality, Place of Birth, Citizenships, Preferred Language, Visa Information
3.6	Occupation
3.6.1	**Employment status**, Job title, Company address, Past occupations, Company name, Description of role
4	**Criminal records/ Court judgements**
5	**Sex life, Sexual orientation**
6	Technical device information
6.1	PC information
6.1.1	**IP Address**, Operating system, Universal unique identifier (UDID), MAC address, Internet service provider, Cookie information, Language settings, Device settings, ROM version, Hardware version, Files on the device, Screen resolution, Type of device, Web beacon data
6.2	Mobile phone information
6.2.1	IMSI, ICC-ID, IMEI, Files, Media, Operating system, Time zone settings, Mobile network information, Calendar entries, Bookmarks, Notes, Alarm clocks, Model, Battery level, Mobile service provider
7	Communication data
7.1	Online communication data
7.1.1	Emails, Error reports, Online meeting requests, Online chats, Search queries, Web beacon data
7.1.2	Online identifiers
7.1.2.1	Cell towers, Location (GPS), Google Advertiser ID, Wifi Connections
7.1.2.2	Credentials
7.1.2.2.1	**Passwords**, Security question, Password hints,
7.1.3	Social media
7.1.3.1	Generated contents(tweets' photos etc.), Contacts (Followers, Followees, Friends, Their gender etc.), Likes, Group membership, Biography
7.1.4	Application usage information
7.1.4.1	Online chats, Search queries
7.1.4.2	Credentials
7.1.4.2.1	Passwords, QR code login information, Account/User name
7.1.4.3	Service Usage
7.1.4.3.1	Registration Logs, Login Logout logs, Time stamp of usage activities, Account modification metrics, Account authentication metrics
7.1.4.4	Browser information
7.1.4.4.1	Browser type, Browser version, Browser plugins, Browsing history, Language settings, Links clicked, Average time spent on websites
7.2	Phone Calls
7.2.1	Duration of Call, Time of communication, SMS Logs, Contacts, Receiving-party number, Calling-party number

Table 8
Industry taxonomy: Finance.

Level	Personal information item
1	Finance Information
1.1	**Income Information**
1.1.1	Monthly rental income, Annual Personal Income, Annual Household Income, Income Source, Stock and Fund Information
1.2	Credit Account Information
1.2.1	**Bank Account Number, Balance**, Account Name, Bank Routing Number, Type of Account, Currency, IBAN, Sort Code
1.2.2	Bank Card Information
1.2.2.1	CVC, CVV, CVV2, Expiry Date, login credentials, Bank Name, Name of the holder, Security Code, Card Number
1.2.3	Transaction History Information
1.2.3.1	Amount, Date/ timestamp, Currency, Supplier, Exchange Rate, Beneficiary Details, IP Address of Receiver, IP Address of Sender, Payment Reason, details of the merchant or ATMs associated with the transaction
1.3	Debit Account Information
1.3.1	**Bank Account Number, Balance**, Account Name, Bank Routing Number, Type of Account, Currency, IBAN, Sort Code
1.3.2	Bank Card Information
1.3.2.1	CVC, CVV, CVV2, Expiry Date, login credentials, Bank Name, Name of the holder, Security Code, Card Number
1.3.3	Transaction History Information
1.3.3.1	Amount, Date/ timestamp, Currency, Supplier, Exchange Rate, Beneficiary Details, IP Address of Receiver, IP Address of Sender, Payment Reason, details of the merchant or ATMs associated with the transaction

(*continued on next page*)

Table 8 (*continued*).

Level	Personal information item
1.4	Payments Information
1.4.1	Accommodation Related Payments
1.4.1.1	Energy and Gas Tariff details, Residential details, Utility Bill Details/Billing Information
1.4.2	Tax information
1.4.2.1	tax filing status, Withholding allowances
1.5	Virtual Currency Account Information
1.5.1	Wallet Address, Transaction Data
1.6	Financial associations and linked people
1.7	Investment Preferences
1.8	Data processed by CRA (Credential Referencing Agencies)
1.8.1	Credit Report, Credit Scores/ Creditworthiness, Affordability Score, Mortgage Accounts, Late Payments, Missing Payments, Gone Away Information Network (GAIN), Search footprints
1.8.2	Insolvency Related events
1.8.2.1	Start Date, End Date, Insolvency Score, bankruptcies, Individual Voluntary Arrangement (IVAs), debt relief orders, sequestrations, trust deeds, debt arrangement schemes, foreclosures
2	Personal identification information
2.1	Formal Identification Information
2.1.1	**SSN, Personal ID/ Identification document, KYC Status, PAN Document**, Passport number, Drivers licence number, Tax identification number, National identity card details, Electoral Register, Licence Plate Number, Vehicle Serial Number
2.2	Genetic Information
2.2.1	Facial recognition data
2.3	Biometric information/Physical identity
2.3.1	Finger prints, Photos, Voice recordings, Video
3	Demographic Information
3.1	**First Name, Family Name, Gender, Signature, Date of birth, Age, Marital/Relationship status, Religious beliefs, Trade union membership**, Nick name, Title, Mother's maiden name, Driving Licence Details
3.2	Information on education
3.2.1	Attended schools and universities, Qualifications
3.3	**Contact Data**
3.3.1	**Full Name, Home address, Mobile phone number, Email address**, Home Phone Number, Fax Number, Shipping/Billing address, Security phone number, Security email address, Work email address, Postal address
3.4	Social Identity
3.4.1	Family history, Living with a partner/spouse, Size of Household
3.4.2	Relations
3.4.2.1	Spouse, Friends, Relatives, Colleagues
3.4.2.2	Children
3.4.2.2.1	Number of Children, Names of Children, Gender of children, Nationality of children, Country of children
3.4.3	Thematic interests/ preferences
3.4.3.1	Hobbies, Leisure activities
3.4.3.2	Content Consumption
3.4.3.2.1	Musical Style, Movies watched, TV Shows watched, Marketing preferences, Apps/Games, Engagement with advertisements, Books read, Followed sports team
3.5	Racial or Ethnic Origin
3.5.1	Nationality, Place of Birth, Citizenships, Preferred Language, Visa Information
3.6	Occupation
3.6.1	Employment status, Job title, Company address, Company website, Department, Past occupations, Company name, Description of role, Salary, CV
3.7	**Political opinions**
3.7.1	payment for a membership to a particular political party
4	**Criminal records/ Court judgements**
4.1	**Criminal records of convictions and offences, Allegations of criminal offences**, Claims History, CCJs, the nature of the judgment, Name of the court, money owed
5	**Sex life, Sexual orientation**
6	Property/ Assets Information
6.1	Vehicles
6.1.1	Brand, Year Bought, motor vehicle reports, Vehicle changes, Year of manufacture
6.2	Technical Device Information
6.2.1	PC Information
6.2.1.1	**IP Address**, Operating System, Universal Unique Identifier/ UDID, MAC Address, Internet Service Provider, Cookie Information, Name of Device, Device Settings, Accounts on Device, Hardware version, Screen Size
6.2.2	Mobile Phone Information
6.2.2.1	IMSI, ICC-ID, IMEI, Files, Media, Operating System, Time Zone Settings, Mobile Network Information
7	Communication data
7.1	Online communication data
7.1.1	Emails, Error reports, Online meeting requests, Online chats, Search queries, Web beacon data
7.1.2	Online identifiers
7.1.2.1	Location (GPS), Google Advertiser ID, Wifi Connections

(*continued on next page*)

Table 8 (*continued*).

Level	Personal information item
7.1.2.2	Credentials
7.1.2.2.1	**Passwords**, Security question, Password hints,
7.1.3	Social media
7.1.3.1	Generated contents(tweets' photos etc.), Contacts (Followers, Followees, Friends, Their gender etc.), Likes, Group membership, Biography
7.1.4	Application usage information
7.1.4.1	Online chats, Search queries
7.1.4.2	Credentials
7.1.4.2.1	Passwords, QR code login information, Account/User name
7.1.4.3	Service Usage
7.1.4.3.1	Registration Logs, Login Logout logs, Time stamp of usage activities, Account modification metrics, Account authentication metrics
7.1.4.4	Browser information
7.1.4.4.1	Browser type, Browser version, Browser plugins, Browsing history, Language settings, Links clicked, Average time spent on websites
7.2	Phone Calls
7.2.1	Duration of Call, Time of communication, SMS Logs, Contacts, Receiving-party number, Calling-party number

Table 9
Academic taxonomy: Health.

Level	Personal information item
1	Health Information
1.1	**Diet Information**
1.1.1	**Dietary Preferences/Pattern of Consumption, calorie intake, allergies**, Intolerances
1.2	Environmental Data
1.2.1	Time spent commuting in traffic
1.3	Sleep Data
1.4	Body Metrics
1.4.1	**Blood glucose**, Cholesterol, Temperature, Blood type, Blood pressure, Heart Rate, BMI
1.5	Physical Features
1.5.1	Silhouette, Tattoos, Birth marks, Scars, Eye colour, Weight, Height
1.6	Women Health Data
1.6.2	**Pregnancy Data**
1.6.2.1	**Pregnancy status, levels of productivity,, pregnancy termination, IVF treatment**
1.7	**Diseases and Diagnosis**
1.7.1	**Individual History, Autopsy results, Content of Medical Treatment, HIV and/or other sexually transmitted diseases, Family Medical History, mortality, Therapy, risk of getting a certain disease, value for Icd code, Cpt rate and value, Progress Notes**, Vital Signs, Medical Images (X-rays, Electromagnetic resonance)
1.7.2	**Cancer related Information**
1.7.2.1	**Tumor location, Histology, Stage**
1.8	Activity data
1.8.1	Distance in metres of the steps taken, Floors Climbed, active time, calories burned, Daily Movements
1.9	**Mental Health**
1.9.1	**Stress level, Mood/Emotional state, psychiatric care, psychotherapy notes**
1.10	Data related to access to care
1.10.1	**Prescribed/Taken Medications, reports and drawings from surgeons or clinicians**, Vaccination, Referrals, purchase of health care services or products
1.10.2	Medical appointments
1.10.2.1	**Date of admission to the hospital, Frequency of hospital visits, Frequency of treatments, scheduled visit(s)**, Doctor name, Doctor's address information
1.11	Addictions
1.11.1	**Alcohol Consumption**, Drinking habits, Smoking habits, Drug Testing, Desire to quit smoking
2	**Personal identification information**
2.1	**Formal Identification Information**
2.1.1	**SSN, Passport number, Drivers licence number, Employer ID, Vehicle ID number, Patient identifier, Resident registration number, Civic registration number**, URLs, Registry number of social insurance (RNSI)
2.2	**Genetic Information**
2.2.1	**DNA analysis, Facial recognition data, Genomic data**, Genetic test data
2.3	**Biometric information/Physical identity**
2.3.1	**Finger prints, Photos, Voice recordings, Eye Movements, Nude Body Images**, Iris Pattern, Video, Ear Information, Gait, Gesture, Lip Motion, Style of typing
2.4	**Online identifiers**
2.4.1	**IP Address, Network Communications, Location (GPS), Wifi Connections, Time Zone Information**, MAC Address, WLAN/WiFi open hot-spots
2.4.2	**Credentials**
2.4.2.1	**Passwords, Security question, Account/User Name**

(*continued on next page*)

Table 9 (*continued*).

Level	Personal information item
2.6	**Contact Data**
2.6.1	**Full Name, Home address, Mobile phone number,Email address**,Fax Number, Shipping/Billing address
2.6.2	**Home Address**
2.6.2.1	**Postal address**, Street name, House Number, Address History, Country
2.6.3	Data from portable devices
2.6.3.1	GSM, UMTS, and GPS location data, WLAN/WiFi open hot-spots, Bluetooth devices, RFID data, Car transponders for automated highway toll payment systems, Electronic badges
3	Demographic Information
3.1	**Gender, Date of birth, Age, Marital/Relationship status, Trade union membership**, First Name, Family Name, Languages Spoken, Age Range
3.2	**Information on education**
3.2.1	**Attended schools and universities, Qualifications**
3.3	Social Identity
3.3.1	**Social Class, Family Honour, surveillance camera images in public places**, behavioural analyses using GSM, UMTS, and GPS location data
3.3.2	Relations
3.3.2.1	**Children**, Contact details of relatives, Number of dependents, Membership Data, Religious organisations, professional associations, political parties
3.3.3	**Thematic interests/ preferences**
3.3.3.1	**Life Style Choices, Living Habits, Voter Registration Information, Adults sites visited**, Favourite Colour, Musical Tastes, Leisure Activities, Consumer Habits, Dressing Style, Hair Style, Favourite Restaurants
3.3.3.2	Contents Generated
3.3.3.2.1	**Letters, Diaries, blogosphere data (forums, blogs, chats, etc.), in-home recorded videos**,
3.3.3.3	**Travel Records**
3.3.3.3.1	business travel, Direction of Travel, flight information
3.4	**Racial or Ethnic Origin**
3.4.1	**Place of Birth**
3.5	**Occupation**
3.5.1	**Employment status, Job Evaluation Records, Company address,Past occupations, Job performance information**
3.6	**Religious beliefs**
3.6.1	**Religious Confessions**
3.7	**Political opinions**
3.7.1	**E-voting**
4	**Criminal records/ Court judgements**
4.1	**Convictions, Abuse Data, Administrative Sanctions**, Cavit Search Data
5	**Sex life, Sexual orientation**
5.1	**Transgender Status**
6	Technical device information
6.1	PC information
6.1.1	**IP Address, Universal Unique Identifier/ UDID**, MAC address
6.2	Mobile phone information
6.2.1	**Unlock pattern, PIN Code, IMEI, Time Zone Settings, Mobile Network Information, Model, Camera, Bluetooth** Operating system, Calendar entries, Notes
7	Communication data
7.1	Online communication data
7.1.1	**Emails**
7.1.3	Social media
7.1.3.1	Generated contents(tweets' photos etc.), Contacts (Followers, Followees, Friends, Their gender etc.), pictures, and comments with their friends
7.1.3.2	**Facebook stream**
7.1.3.2.1	Attendance at Events, Pages Liked, Group Membership
7.1.4	Application usage information
7.1.4.1	**Service Usage, Encryption Key, Tokens, Access Keys** Online chats, Search queries
7.1.4.2	Credentials
7.1.4.2.1	Passwords, Account/User name
7.1.4.3	Browser information
7.1.4.4.1	**Browsing history, Links clicked** Browser type, Browser Cache, Average time spent on websites, Cookie Information
7.2	**Phone Calls**
7.2.1	**SMS Logs**, Contacts, MMS
8	Security Data
8.1	video surveillance (CCTV), Face recognition data, biometric data, audio recordings, directional microphone observations, phone call surveillance, Speed radar photographs, scanned items and body scans at airports, security forms that must be filled in

Table 10
Academic taxonomy: Finance.

Level	Personal information item
1	Finance Information
1.1	**Income Information**
1.1.1	Annual Personal Income, data about compensation and benefits
1.2	**Credit Account Information**
1.2.1	**Bank Account Number, Transaction History Information, Balance**, Account Name, Bank Routing Number, Type of Account, Currency, IBAN, Sort Code
1.2.2	**Bank Card Information**
1.2.2.1	**CVC, CVV, CVV2, Expiry Date, login credentials**
1.3	Debit Account Information
1.3.1	**Bank Account Number, Balance**, Account Name, Bank Routing Number, Type of Account, Currency, IBAN, Sort Code
1.3.2	**Bank Card Information**
1.3.2.1	**CVC, CVV, CVV2, Expiry Date, login credentials**
1.4	Payments Information
1.4.1	**Bank Loans, Personal Loans** Tax information, Spending Patterns
1.4.2	Accommodation Related Payments
1.4.2.1	Energy and Gas Tariff details, Residential details, Utility Bill Details/Billing Information
1.4.3	Purchase Orders
1.4.3.1	Airline Ticket Purchase
1.5	Data processed by CRA (Credential Referencing Agencies)
2	**Personal identification information**
2.1	**Formal Identification Information**
2.1.1	**SSN, personal identification numbers (PINs), Drivers licence number**, Passport number, Tax identification number, National identity number, Electoral Register, Personal ID, birth certificate numbers, resident registration numbers
2.2	**Genetic Information**
2.2.1	**Facial recognition data**
2.3	**Biometric information/Physical identity**
2.3.1	**Finger prints, Photos, Voice recordings, Biological traits/markers**, Video
3	Demographic Information
3.1	**First Name, Family Name, Gender, Date of birth, Age, Driving Licence Details, Political opinions, Trade union membership**, Voter registration data, Marital/ Relationship Status, Immigration records/status, Mother's maiden name
3.2	Information on education
3.2.1	Attended schools and universities, Major subject of study, Number of years studying a subject
3.3	**Contact Data**
3.3.1	**Full Name, Mobile phone number,Email address, Home Phone Number,Fax Number,** , Shipping/Billing address, Security phone number, Security email address, Work email address
3.3.2	**Home address**
3.3.2.1	**Street Address, City, Country, Postal address**
3.4	Social Identity
3.4.1	**Intellectual Property, Lifestyle choices**, Habits, Thoughts, emotions/feelings, Technology and market skills, strategic plans, competitive intelligence
3.4.2	Relations
3.4.2.1	Size of Household/Household Data, Number of dependents, Life long mate
3.4.3	Thematic interests/ Preferences
3.4.3.1	**Lifestyle choices, Intellectual Property**, Competitive intelligence
3.4.3.2	Hobbies/Likes
3.4.3.2.1	Favourite Actor/Actresses, Favourite Pet
3.4.3.3	Leisure Activities
3.4.3.3.1	Campaign finance donations, membership data
3.4.3.3.2	Travel records
3.4.3.3.2.1	**Vacation plans**, Flights, Hotel Bookings
3.4.3.3.3	Shopping Behaviours
3.4.3.3.1	purchase history
3.4.3.4	Content Consumption
3.4.3.4.1	**Apps/Games**, TV Shows watched, Radio programs, library books checked out, Internet Habits
3.5	**Racial or Ethnic Origin**
3.5.1	**Nationality, Citizenships**, Place of Birth, Preferred Language, Skin colour
3.6	Occupation
3.6.1	**Salary**, Profession, Job title, Description of role, Years of experience, Sector, Projects, business relationship information, Company Name/Organisation
3.7	**Religious beliefs**
3.7.1	**Church Attendance**
4	**Criminal records/ Court judgements**
4.1	**Criminal records of convictions and offences**
5	**Sex life, Sexual orientation**
6	**Property/ Assets Information**
6.1	Vehicles
6.1.1	**Vehicle Identifiers, Serial Number**
6.2	Technical Device Information
6.2.1	PC Information

(*continued on next page*)

Table 10 (*continued*).

Level	Personal information item
6.2.1.1	**IP Address, Cookie Information/Log contained in cookie, Serial Number, Device Identifiers**, Files, on PC
6.2.2	Mobile Phone Information
6.2.2.1	**IMSI, ICC-ID, IMEI, Mobile Network Information**, Files, Media, Notes
6.2.3	**e-cash, bitcoin, Misuse of credit cards**
7	Communication data
7.1	Online communication data
7.1.1	Emails, voice mail, RSS/Atom feeds, Alerts, personal website, published reports and articles
7.1.2	Online identifiers
7.1.2.1	**Location (GPS)**, Location History
7.1.2.2	Credentials
7.1.2.2.1	**Passwords, Encryption keys**, key tokens
7.1.3	Social media
7.1.3.1	Generated contents (tweets' photos etc.), photos about peoples life, Holiday Photos, photos about their children, Birthday Party Photos, interactions in social networks
7.1.4	Application usage information
7.1.4.1	Browser information
7.1.4.1.1	Browsing habits, click-stream data, Links clicked, search activities
7.2	Phone Calls
7.2.1	**SMS Logs**, Contacts
7.3	Fax communications

Table 11
List of mobile health applications assessed from the Google Play Store.

Samsung Health	Huawei Health	Google Fit: Health and Activity Tracking	Pedometer - Step Counter, Weight & Calorie Tracker
Health & Fitness Tracker with Calorie Counter	Health Mate - Total Health Tracking	Health Tracker	LG Health
Health Pal - Fitness, Weight loss coach, Pedometer	Calorie Counter - MyFitnessPal	Ada – your health companion	Youper - Emotional Health
Step Counter - Walking, Lose Weight, Health, Sport	Natural Remedies: healthy life, beauty and recipes	Step Counter - Pedometer Free & Calorie Counter	What's Up? - A Mental Health App
Student Health App	Sanitas HealthCoach	Mental Health Tests	Pedometer - Step Counter Free & Calorie Burner
Lifelog	HealthifyMe: Get Diet Plan, Nutritionists, Coaches	Pedometer for walking - Step Counter	Health Sync
Health Diet Foods Fitness Help	Step counter & Calorie counter	Health e-Hub	Fitbit
Period Tracker Flo, Ovulation Calendar & Pregnancy	Noom: Health & Weight	Healthy Spine & Straight Posture - Back exercises	Medical ID (Free): In Case of Emergency
Health Mate - Calorie Counter & Weight Loss App	Health and Nutrition Guide	Mi Fit	Fabulous: Daily Motivation
30 Day Fitness Challenge - Workout at Home	Babylon: Doctor Appointments, Healthcare & more	Feelfit-Health Fitness Tool	Lefun Health
Cigna Virtual Health	One You Couch to 5K	HeadUp – Health & Fitness	Health Log
Yolanda-Health Fitness Tool	Garmin Connect™	Jiff - Health Benefits	Period Tracker - Period Calendar Ovulation Tracker
Instant Heart Rate: HR Monitor & Pulse Checker	Lifesum - Diet Plan, Macro Calculator & Food Diary	Make me Healthy Fitness & Healthy Lifestyle app	Your.MD: Symptom Checker & Health Tracker
IEatWell:Food Diary&Journal Healthy Eating Tracker	Wellington Health & Fitness	MedM Health	Health Tips
Allianz MyHealth	Zeroner Health Pro	Dog Health	Beurer HealthManager
Health Connect 24 × 7	Men's Health Fitness Trainer - Workout & Training	Keep Trainer - Workout Trainer & Fitness Coach	Dream Hospital - Health Care Manager Simulator
23andMe - DNA Testing: Health & Ancestry	FEMM Health Period and Ovulation Tracker	Health News, Videos, & Social Media	Lifetrons Health
1byone Health	Daily Mudras (Yoga) - for health	Qardio Heart Health	Healthy Diet - Best Diet Plan, Calorie Counter

(*continued on next page*)

Table 11 (*continued*).

Samsung Health	Huawei Health	Google Fit: Health and Activity Tracking	Pedometer - Step Counter, Weight & Calorie Tracker
Updoc: Health diary	Gluten free Recipes: Healthy Cookbook	M-Health	Women's Health Diary
Health Articles, Info & Motivation - LetsHealthify	Health Calculator	UP – Smart Coach for Health	Microlife Connected Health
Koogeek - Smart Health	Healthy Food	Herbal Health Care	The Healthy Mummy
Changing Health	ContinuousCare Health App	Acıbadem Health Point	Transtek Health
Daily Health Tips	Health & Weight Loss Coach	Player's Health	Health Heroes
Backpack Health	Gini: DNA Based Health & Nutrition	Philips HealthSuite Health app	CDC Health IQ
My Health Guide	HealthMax - Health Calculator	Health Equals Wealth	Sano Health
CircleCare - Live Healthy. Earn Rewards.	Health Calculator - BMI & WTH	Health.Me2	UK Health Radio™
Health Atlas by IHME	ADHD Health Storylines	Cigna Health Benefits	LCARE - Health
The health Podcast (The health code)	Health & Fitness Tips Hindi-English	Now Health International	LinkTo Health
Baby + – your baby tracker	Synergy Health	The Ultimate Health Podcast	Health Journeys - Guided Imagery & Meditation
Health First — blood test explains diseases	Health Solutions	Medel Health Check	Your Health-Key: Online Doctor Consultation App
Braun Healthy Heart	Womens Health Personal Trainer- Workout & Training	Pregnancy +	HealthWatch 360
Headspace: Meditation & Sleep	Vita Health	MyPlate Calorie Tracker	cure.fit Healthy food, Fitness, Yoga, Meditation
Fitonomy - Workouts, Weight Loss & Meal Planner	Modus Health Card	Weight Loss Formula: Best Health Recipes	Fruits For Health
Center Health — The Diabetes App	FaceYoga - Facial Health & Fitness	Daytoday Health: Patient care management platform	Vitamins Academy Power Health
SuperFood - Healthy Recipes	Webteb Health News	Period Tracker Clue - Ovulation and Cycle Calendar	Happy Food - Healthy Food
Nudge Health	Magic Health Counter	e-Health	Health E-Chat
iTooch 6th Grade Health	Health	Dentacare - Health Training	Roko Health Clubs
ABC OF BREAST HEALTH	Daily Challenge - MeYou Health	Healthy Weight: tracker & BMI	Health Online
Praktice Health	Actofit Health & Workouts	Wim Hof Method -Making you strong, healthy & happy	Noom Walk Pedometer
Accurate Heart Rate Monitor	dacadoo - Health Score	Water Drink Reminder	PSY - mental health help. Support groups.
Bannatyne Health Club	Female Fitness - Women Workout	Healthy U	My TANITA – Healthcare App
Ovia Pregnancy Tracker: Baby Due Date Countdown	Pill Reminder & Medication Tracker - Medisafe	Health Guide	Health Benefits of Moringa Leaves
Lose Belly Fat in 30 Days - Flat Stomach	7 Minute Workout	Fruit Health Benefits	Yoga For Health & Fitness
Period Tracker MIA Fem: Ovulation Calculator	SWEAT: Kayla Itsines Fitness	Sadhguru - Yoga, Meditation & Spirituality	BMI Calculator
Wellness Coach - Health	Ovia Fertility: Ovulation & Cycle Tracker	Health Help Now	Spices For Health
8fit Workouts & Meal Planner	Health Tips 1000	iHealth MyVitals	Eye Exercises & Eye Training Plans - Eye Care Plus
My Diet Coach - Weight Loss Motivation & Tracker	Argus Calorie Counter Diet, Activity, Step Tracker	Muthoot Health Connect	WebMD: Check Symptoms, Find Doctors, & Rx Savings
Beauty and Health Tips	Best Ayurvedic Beauty and Health Tips	Symptomate – Symptom checker	Be Fit Be Healthy

(*continued on next page*)

Table 11 (*continued*).

Samsung Health	Huawei Health	Google Fit: Health and Activity Tracking	Pedometer - Step Counter, Weight & Calorie Tracker
EHR/EMR Health records	Westfield Health Claims	Lose It! - Calorie Counter	Lifesense
Medocity Home Health: Patient Virtual Care	Huawei Wear	Men’s Health Magazine	Health and Fitness Pro
Endomondo - Running & Walking	Bellabee Health	Weight Loss Recipes	Heart Rate Monitor
Health Tips Hindi Collection	Pedometer: GStep Counter And Running Tracker App	Virgin Pulse	Ovia Parenting: Baby Tracker, Breastfeeding Timer
Booster Buddy	Gmate® Healthcare	Mosby’s Drug Reference for Health Professions	Walk with Map My Walk
Pedometer - Step Counter	Water Time Pro Drink Tracker & Reminder	10 Best Foods for You	Cat’s Health – feline BMI
Evergreen Life PHR	Nike Run Club	BMI Calculator	Healthy Digestion Foods Metabolism Nutrition Diet
eHealthSystem	AHRQ ePSS	Men’s Health: Sexuality and Fertility Medicine	Keep Yoga - Yoga & Meditation, Yoga Daily Fitness
FitCalc+ Fitness & Health Calculator - Gym Tools	OHS Assist - No. 1 Health & Safety Application	Peak Health	One You Easy Meals
MINDBODY: Fitness, Salon & Spa	mySymptoms Food Diary & Symptom Tracker (Lite)	My Possible Self: The Anxiety & Mental Health App	InnerHour: Calm, Sleep, Depression & Anxiety Therapy
Drink Water Reminder - Hydration and Water Tracker	Period tracker & Ovulation calendar by PinkBird	104 Law of Attraction Health Affirmations	Eve Period Tracker - Love, Sex & Relationships App
Health Benefits of Honey	World of Health Care	HealthPass – Doctors & Health Checkups	My Eyes Protection
GymRun Workout Log & Fitness Tracker	Health Jobs	Glow: Fertility Calculator and Ovulation Tracker	Weight Loss Bet by HealthyWage
Yuka - food & cosmetics scan	Heart Rate Monitor – Simple Heartbeat Tracking	One You Active 10 Walking Tracker	Run with Map My Run
Lose Weight in 30 Days	IRIS Health Services		

Table 12
List of mobile health applications assessed from the Apple App Store.

MyFitnessPal	Fitbit	Lose It! – Calorie Counter	Calm
Nike Run Club	Headspace: Meditation & Sleep	Map My Run by Under Armour	WW (Weight Watchers)
Sweatcoin	Flo Period & Ovulation Tracker	Period Tracker by GP Apps	Runkeeper—GPS Running Tracker
Nike Training Club	Relax Melodies: Sleep Sounds	AllTrails: Hike, Bike & Run	Weight Loss Running by Verv
BetterMe: Weight Loss Workouts	Sworkit Fitness & Workout App	Pregnancy Tracker - BabyCenter	Clue Period & Cycle Tracker
White Noise Lite	Pregnancy & Baby Tracker	MyPlate Calorie Counter	Lifesum: Diet & Macro Tracker
SWEAT: Kayla Itsines Fitness	Instant Heart Rate: HR Monitor	Sleep Cycle: smart alarm clock	Sleep Sounds by Sleep Pillow
MINDBODY: Fitness, Salon & Spa	30 Day Fitness	Strava: Run, Ride, Swim	8fit Workouts & Meal Planner
Pacer Pedometer & Step Tracker	adidas Running by Runtastic	Garmin Connect™	Aaptiv: #1 Audio Fitness App
Weight Loss Fitness by Verv	Fitness Buddy: Gym Workout Log	Weight Loss Walking by Verv	Bellabeat Period Diary
Pillow Automatic Sleep Tracker	LA Fitness Mobile	Fooducate Diet & Nutrition	Planet Fitness
Seven - 7 Minute Workout	C25K® 5K Trainer	Daily Workouts Fitness Trainer	Workout for Women: Fitness App
Fitbit Coach	Breethe: Meditation & Sleep	Pedometer++	Rain Rain Sleep Sounds

(*continued on next page*)

Table 12 (*continued*).

MyFitnessPal	Fitbit	Lose It! – Calorie Counter	Calm
Carb Manager: Keto Diet App	My Diet Coach - Weight Loss	BetterMen: Workout Trainer	Period Tracker - Eve
Life - Period Tracker Calendar	Map My Ride by Under Armour	Steps - Activity Tracker	Kaiser Permanente
Beachbody® On Demand	Insight Timer - Meditation App	Period Tracker Period Calendar	Glow Period, Fertility Tracker
Freeletics - Workout & Fitness	Interval Timer - HIIT Workouts	Noom	Plant Nanny
Reflectly	Motivation Quotes -Daily Quote	Daily Ab Workout - Abs Trainer	adidas Training by Runtastic
Simple Habit Daily Meditation	The Bump - Pregnancy Countdown	Workout: Gym routines planner	Health4Me
My Fitness Workout by GetFit	Daily Yoga - Workout & Fitness	Calorie Counter - MyNetDiary	Sleepzy - Sleep Cycle Tracker
Record by Under Armour	Workout Trainer: fitness coach	iHoroscope - Daily Horoscope	BetterMe: Walking & Weightloss
5K Runner: Couch to 5K Trainer	Fitbod Weight Lifting Workout	myCigna	Quotes” Inspirational Sayings
Asana Rebel	Withings Health Mate	JEFIT Workout Planner Gym Log	Map My Fitness by Under Armour
7 Minute Workout	Ab & Core Workouts	Bed Time Fan White Noise Sound	iPeriod Lite Period Tracker
Moment - Screen Time Control	BodySpace - Social Fitness App	Men’s Health Magazine	7 Minute Workout Challenge
Period Tracker Health Calendar	Seconds Interval Timer	Peloton — Guided Workouts	10% Happier: Meditation
Aura: Sleep & Mindfulness	Fabulous - Daily Motivation	Keto.app - Keto Diet Tracker	Argus: Calorie Counter & Step
Think Dirty – Shop Clean	Daily Butt Workout - Trainer	Aetna Mobile	Period Tracker: Monthly Cycles
My Water Balance	Life Advisor: Personal Test	Simply Yoga - Fitness Trainer	TeasEar - ASMR Slime Triggers
Stop, Breathe & Think	Sleep++	Zero - Fasting Tracker	White Noise Deep Sleep Sounds
iMassage U Vibrating Massager	First Aid: American Red Cross	Happify: for Stress & Worry	Sleep Watch by Bodymatter
Stepz - Step Counter & Tracker	Express Scripts	Calorie Counter by FatSecret	Sleep Time: Cycle Alarm Timer
Cardiogram: Heart Rate Monitor	ShopWell - Better Food Choices	Strong Workout Tracker Gym Log	23andMe - DNA Testing
Atkins® Carb & Meal Tracker	Waterlogged — Drink More Water	ClassPass	Fertility Friend FF App
Endomondo	Baby Names	21 Day Fix® Tracker – Official	At Home Workouts by Daily Burn
Orangetheory Fitness Booking	Qardio heart health	Sanvello:Stress & Anxiety Help	Fit Radio: Train Inspired
Zombies, Run!	Daily Water - Drink Reminder	FitOn: Fitness Workout Plans	Abs Workout - Daily Fitness
Muscle Booster Workout Tracker	CalorieKing Food Search	Virgin Pulse	Relax Meditation: Guided Mind
Disney Magic Timer by Oral-B	J&J Official 7 Minute Workout	Achievement - Reward Health	Happy Scale
Sprout Pregnancy	VeryFitPro	Drink Water Reminder N Tracker	SparkPeople Calorie Tracker
WebMD Pregnancy	Full Fitness: Exercise Workout Trainer	Daily Cardio Workout - Trainer	Cardiio: Heart Rate Monitor
Charity Miles	Female Fitness Women Workout	iVibe: Vibrating Massager	Your Texas Benefits
Fitonomy: Weight Loss Workout	Fitplan: Gym & Home Workouts	Sleep	My Challenge Tracker
Oral-B	Menstrual Period Tracker	StrongLifts 5 × 5 Weight Lifting	Abide - Christian Meditation

(*continued on next page*)

Table 12 (*continued*).

MyFitnessPal	Fitbit	Lose It! – Calorie Counter	Calm
Yoga Studio: Mind & Body	Free Relaxing Nature Sounds and SPA Music	Running Distance Tracker Pro	Fitness Buddy+ Gym Workout Log
The Wonder Weeks	Spot On Period Tracker	SleepIQ	Meditation Studio
StepsApp Pedometer	RockMyRun - Workout Music	Baby Names	Life Time Member App
Lose Weight Hypnosis	Home Workout - No Equipments	Rally Health®	White Noise Ambience Lite
White Noise	YAZIO — Diet & Food Tracker	Sanity & Self: Self-Care Guide	Mi Fit
Talkspace Online Therapy	Walkmeter Walking & Hiking GPS	Couch to 5K® - Run training	Sound Sleeper: White Noise
UnitedHealthcare	30 Day - Ab Challenge	Find Me Gluten Free	Centr, by Chris Hemsworth
7 Minute Workout: Fitness App	BetterMe: Sleep & Meditation	Butt Workout and Fitness App	Daily Leg Workout - Trainer
BetterHelp - Online Counselling	Relaxing Sounds, Sleep Easy	Sports Tracker for All Sports	Volt: #1 AI Workout App
Life Cycle - Track Your Time	Yoga — Down Dog	Wodify	Smoke Free - Quit Smoking Now
Zova: Health & Fitness Coach	Slumber: Fall Asleep, Insomnia	Misfit	WebMD Baby
MyHumana	Period Tracker Deluxe	iHerb	Meditation & Relaxation Music
Glo - Yoga and Meditation	RENPHO	21-Day Meditation Experience	Equinox
Tabata Stopwatch Pro	AutoSleep Tracker for Watch	Jillian Michaels Fitness App	TrailLink: Bike, Run & Walk
Weight Gurus	Cyclemeter Cycling Running GPS	30 Day - Squat Challenge	Monitor Your Weight
Lark - 24/7 Health Coach	Lasting: Marriage Health App	Human - Activity Tracker	Bose® Hear

Table 13
List of mobile finance applications assessed from the Google Play Store.

Yahoo Finance: Real-Time Stocks & Investing News	Wallet - Finance Tracker and Budget Planner	Easy Home Finance	MSN Money- Stock Quotes & News
Investing.com: Stocks, Finance, Markets & News	Money Manager: Expense Tracker, Free Budgeting App	Bloomberg: Market & Financial News	Monthly Budget Planner & Daily Expense Tracker
Money Manager Expense & Budget	Financial Times	Money Lover: Money Manager, Budget Expense Tracker	Emma - Budget Planner and Money Management
Mobills Budget	Monefy - Money Manager	Oxford Dictionary of Finance and Banking	Fast Budget - Expense & Money Manager
ClearScore - Track Your Credit Score & Finances	CNBC: Breaking Business News & Live Market Data	My Finances	Financial Dictionary by Farlex
CityFALCON - Financial News	MarketWatch	Best Brokers: Stock Simulator	Financial Calculators
Yolt - The Smart Money Manager	Bluecoins Finance: Budget, Money & Expense Manager	Toshl Finance - Personal Budget & Expense Tracker	Single Expense - Financial Planner
Invstr: Investing for Everyone	Honeydue: Budget, Bills & Money for Couples	Spendee - Budget and Expense Tracker & Planner	EasyBudget
My Stocks Portfolio & Widget	Financisto - Personal Finance Tracker	My Expenses	Squirrel - Saving, Budgeting & Money Management
eToro	Spending Tracker	Money Manager: Track expense & budget bookkeeping	Goodbudget: Budget & Finance
Daily Expenses 3: Personal finance	Daily Expenses 2: Personal finance	PayPal Mobile Cash: Send and Request Money Fast	Finance Manager
Expense Manager	Barchart Stocks & Futures	HMRC	Family Budget Finance Tracking

(*continued on next page*)

Table 13 (*continued*).

Monese - Mobile Money Account & Finance Management	Splid – Split group bills	Account Book - Money Management	Splitwise
Fortune City - A Finance App	Wallets: expense tracker, money manager	Day-to-day Expenses	Dollarbird - Personal finance calendar
MoneySuperMarket: Credit Monitor	Accounts and Finance App	AndroMoney (Expense Track)	Vault - Budget Planner
Dave Ramsey Show: Financial Advice Anytime	1Money - Expense Tracker, Money Manager, Budget	Finance Manager	Exchange Rates - Currency Converter
Cindicator: become a financial analyst	Revolut - A Radically Better Account	Alzex Finance: Family budget with cloud sync	Personal Finance Cost accounting Family budget
CoinKeeper: spending tracker	Capital One UK	UOL Cotações	Home Bookkeeping Lite
Change Invest: Buy & Sell Bitcoin Commission-free	DAILY POCKET - Budget Manager	Webull: Trade Stocks & ETFs	Google Pay: Pay with your phone and send cash
NYSE Live Stock Market	Economy and Finance	My Argos Card	Supermon Free Finance Manager
BankTree Personal Finance	Money Pro - Personal Finance & Expense Tracker	Money Dashboard Budget Planner	FinWiz-Stocks, News, Investing,Portfolio & Markets
Income vs Expenses - budget & finance manager	Loan Calculator	Expense IQ Money Manager	USA Stocks
Moneycontrol – Stocks, Sensex, Mutual Funds, IPO	My Budget Organizer - Budget Planner with Sync	Halifax: the banking app that gives you extra	GnuCash
Basic Finance	Paymaster: Budget Manager & Spend Tracker	Bills Reminder, Budget & Expense Manager App	MoneyWiz 3 - Personal Finance
Moneon — personal budget planner, finance tracker	MetaTrader 4 Forex Trading	Money Management, Expense & Budget App Spendless	Expense Manager - Tracker
Expense Manager	My Money Tracker	Tradays — forex economic calendar	Money Keeper: Expense Tracker, Note, Budget
Settle Up - Group Expenses	Financial Monitor - personal finance manager	ET Markets: NSE & BSE India	N26
Financial Calculator	Bitcoin Wallet by SpectroCoin	Lloyds Bank Mobile Banking: by your side	TransferWise Money Transfer
NetDania Stock & Forex Trader	MetaTrader 5	Monzo Bank	Cash App
Percentage Calculator	Metro Bank	BBVA Spain	Santander
Financial Calculators	first direct	Home Budget Manager Lite With Sync	Smart Receipts
Financial Calculator Pro EF	Tricount - Split bills & manage group expenses	EO.Finance: Buy and Sell Bitcoin. Crypto Wallet	Amigo Loans
Learn: how to invest in stocks	gohenry - the allowance app for young people	Barclays	Money Manager: Spending Tracker, Budget Planner
NDTV Profit	Stocks - London Stock Quotes	Easy Bills Reminder	Expenses Manager
E*TRADE: Invest. Trade. Save.	US Stock Market	Poloniex Crypto Exchange	Stocks: Realtime Quotes Charts & Investor News
Plutos: Receipt & Finance Scanner	Bitcoin Trading: Investment App for Beginners	Investmate - Learn to trade shares and derivatives	Kite by Zerodha
Income Expense	GTBank	Santander Mobile Banking	FXhours: Forex Trading, Charts, finance & news
WebMoney Keeper	IndusMobile	Fudget: Budget and expense tracking app	Forex Calendar, Market & News
Barclaycard	Cleo	Toman	Expense Manager
YNAB — Budget, Personal Finance	Seeking Alpha: Stock Market News & Analysis	Finance - your stock profolio	NetBenefits
TVM Financial Calculator	Financial markets	Investing Game - Learn How to invest in trading	Bloomberg Professional
ExpertOption - Mobile Trading	Debt Manager and Tracker	ProCoins debt tracker, spending tracker, budgeting	Stock Market Tracker

(*continued on next page*)

Table 13 (*continued*).

TradingView - Charts, Quotes, Traders & Investors	Our Budget Book	Markets Mojo	My Wallet - Expense Manager
Timesheet - Track Time Hours and Salary Timecard	Monific - Budget and Expense Planner	DR LOCUST FINANCE	Loan Calculator IQ
mBank PL	ANNA Money: the business account for startups	IG Academy: Trading Courses – Learn How to Trade	Coin by Zerodha
Small World Money Transfer	iMobile by ICICI Bank	International Finance	All bank Money Manager, Track Bank balance & Cards
BSEIndia on Mobile	My Money Manager	CommBank	Thriv - Savings Goal
FinArt: Family Expense Tracker	Tesco Bank Mobile Banking	Stock Trainer: Virtual Trading (Stock Markets)	Stocktwits - Stock Market Chat
Learn to Invest in Stocks - Trade Brains	Financial regulatory alerts	Daily Expenses: Personal finance	Efics - expense tracker & money management app
Sprouts: Money Manager , Expense and Budget	Loan Calculator	Citibank IN	FirstMobile
Tarot of Money & Finance - Free Tarot Card Reading	52 Weeks Money Challenge	Penny Stocks	Loan Calculators
IIFL Markets - NSE BSE Mobile Stock Trading	Deposit & Savings Calculator	Plus500: CFD Online Trading on Forex and Stocks	Bitcoin, Ethereum, IOTA Ripple Price & Crypto News
ERAMET Finance	Wealth eOffice	BHEX	Investec
JStock - Stock Market, Watchlist, Portfolio & News	Easy Currency Converter	Currency Converter free	AxisDirect Mobile
The Economic Times: Sensex, Market & Business News	Homeasy - Bills calendar	Zacks Stock Research	Finance Simulator: Loans & Interests Calculator
Jojo Personal Finance	aqua card	52 Weeks Money Challenge - Free	Currency Financial News
Vernimmen Finance d'Entreprise	Guide to Make Money	Barron's: Stock Markets & Financial News	Simple Loan Calculator
Karl's Mortgage Calculator	Experian – Your Free Credit Score Check	Trading 212 - Stocks, Forex, Crypto, Gold	NJ Client Desk
Stocks Widget	KarvyOnline - Mobile Trading App	FXStreet - Forex News, Economic Calendar & Rates	Easy Loan Calculator
HDFC securities MobileTrading	Loan Calculator	Loan & Interest Calculator	Moje Finance
FundzBazar	Market Trends - Forex signals & traders community	Monthly Expenses	Parmis Accounting
Forex – Trading strategies	MoneyWiz 2 - Personal Finance	Walter Finance	Forex Course
Mo Investor: Mutual Fund & Stock Investment App	Finance View		

Table 14
List of mobile finance applications assessed from the Apple App Store.

Venmo Send & Receive Money	PayPal: Mobile Cash	Cash App	Chase Mobile
Bank of America Mobile Banking	Capital One Mobile	Credit Karma	Wells Fargo Mobile
Mint: Personal Finance & Money	Citi Mobile	GEICO Mobile - Car Insurance	Discover Mobile
Amex	Zelle	Robinhood: Invest. Save. Earn.	Acorns: Invest Spare Change
Progressive	USAA Mobile	TurboTax Tax Return App	IRS2Go
WesternUnion US Money Transfer	Stash: Invest. Bank. Save	Coinbase – Buy & sell Bitcoin	U.S. Bank
State Farm	Yahoo Finance	Google Pay	PNC Mobile Banking
TD Bank (US)	Earnin - Get paid today	Navy Federal Credit Union	Fidelity Investments
Allstate® Mobile	MileIQ: Mileage Tracker & Log	Digit: Save Money Effortlessly	EveryDollar Easy Budgeting App

(*continued on next page*)

Table 14 (*continued*).

Venmo Send & Receive Money	PayPal: Mobile Cash	Cash App	Chase Mobile
Experian Credit Report	Credit One Bank Mobile	Barclays US	Capital One CreditWise
E*TRADE: Invest. Trade. Save.	Dave - Banking For Humans	QuickBooks Self-Employed	Goodbudget Budget Planner
Clarity Money - Budget Manager	Xoom Money Transfer	Credit Sesame	Money Network Mobile App
Splitwise	Regions Mobile	JPay	Chime - Mobile Banking
TD Ameritrade Mobile	SunTrust Mobile App	Albert: Save and Spend Smarter	U by BB&T
Fifth Third Mobile Banking	NetBenefits	Spending Tracker	Mortgage by Zillow
Schwab Mobile	PNC Virtual Wallet	TaxCaster: Tax Calculator	Green Dot - Mobile Banking
Fresh EBT - Food Stamp Balance	CareCredit Mobile App	Netspend	Vanguard
Citizens Bank Mobile Banking	Stocks Tracker:Real-time stock	MoneyGram	Qapital: Save. Invest. Spend.
Huntington Mobile	LifeLock ID Theft Protection	Chase Pay® — Earn, Save, Order	Personal Capital
My Block	Ally Mobile	Blockchain Wallet: Bitcoin	iSpreadsheet™: Office Sheets
Daily Budget Original	MySynchrony	Walmart MoneyCard	MarketWatch - News & Data
Truebill Budget & Bill Tracker	Seeking Alpha: News & Analysis	KeyBank Mobile	TD Ameritrade: Mobile Trader
MoneyLion: Mobile Banking	BankMobile App	Root: Affordable car insurance	Pocket Expense 6
FedLoan Student Loans	Ally Auto Mobile Pay	Santander Bank US	myTFS - Toyota Financial
YNAB (You Need A Budget)	Great Lakes Mobile	Brigit: Get $250. When Needed.	Paribus: Money Back Shopping
M&T Mobile Banking	BBVA United States	PREMIER Credit Card	Quicken
Serve	myFICO - Official FICO Scores	MetaTrader 4 Forex Trading	Fudget: Budget Planner Tracker
Varo: No Fee Mobile Banking	Earny: Money Back Savings App	Cleo	Mi Banco Mobile
Bluebird by American Express	Tally — Pay Off Debt Faster	Current - Bank for Modern Life	Even App
Stock Master: realtime stocks	EZ Financial Calculators	ATH Móvil	Prism Pay Bills, Bill Reminder
Woodforest Mobile Banking	Twine: Easy Saving & Investing	ConnectNetwork	thinkorswim: Buy. Sell. Trade.
AutoGravity - Car Loan & Lease	H&R Block Tax Prep and File	Remitly: Transfer Money Abroad	Betterment: Invest and Save
GoBank - Mobile Banking	Everlance: Mileage & Expenses	myStudentAid	Merrick Bank Mobile
Checkbook - Account Tracker	Rocket Mortgage	TouchBanking	Farmers Insurance Inc.
HSBC Mobile Banking	Mortgage Calculator by QL	Best Brokers Stock Market Game	MyMerrill
Nationwide Mobile	Bitcoin Wallet By Bitcoin.com	NerdWallet	TransferWise
Greenlight Debit Card for Kids	Snapshot® Mobile	Fox Business: Invested In You	Possible Finance - Fast Loans
FNBT & FCB Mobile Banking	Simple - Mobile Banking	Stocktwits	GET Mobile
BRD Bitcoin Wallet & Crypo	U.S. Bank Access® OnlineMobile	BMO Digital Banking	Wells Fargo CEO Mobile
Dave Ramsey Show	Lemonade Insurance	Bank of the West Mobile App	HealthEquity Mobile
PayPal Prepaid	Hiatus: Bill and Money Manager	Turbo: Scores-Income & Credit	Merrill Edge
Navient Loans	SoFi: Mobile Finance & Money	Mr. Cooper	Amazon Store Card

(*continued on next page*)

Table 14 (*continued*).

Venmo Send & Receive Money	PayPal: Mobile Cash	Cash App	Chase Mobile
Progressive Leasing Mobile	Tip Check - Calculator & Guide	BECU	Al Rajhi Bank KSA
RushCard	Edward Jones Mobile	Lexington Law - Credit Repair	Blockfolio - Crypto Tracker
NYC Pay or Dispute	Popmoney	First Horizon Mobile Banking	QuickBooks Payroll
Bloomberg Professional	T. Rowe Price Personal®	Ingo Money – Cash Checks Fast	Sales Tax Calculator FREE Tax Me - Shopping Checkout, Coupon and Discount Helper
Loan Calculator‰	TCF Bank	Webull: Trade Stocks & ETFs	SchoolsFirst FCU Mobile
Stride: Benefits for Less	Self - Build Credit	America First Credit Union	WorldRemit Money Transfer
PayFlex Mobile®	GM Financial	Boss Revolution Money	Wealthfront
Bills Monitor - Bill Reminder	Honeydue: Couples Finance	Suncoast SunMobile	Union Bank - Mobile Banking
Amex Business	Direct Express®	Golden 1 Mobile	Elan Credit Card
AlAhliMobile	MACU Mobile Banking	Mortgage Calculator Plus	Voya Retire
Morgan Stanley Wealth Mgmt	Stockpile - Stock Trading	CoinCap	TIAA
LendingTree	Learn: how to invest in stocks	Branch: Budget & Get Paid Now	PenFed Mobile
Netspend Skylight ONE	Investing.com Stocks & Finance	Empower - Bank with Benefits	FirstBank Mobile Banking App
Morningstar for Investors	Pushpay	RBFCU Mobile	My TRSRetire
CardValet	TipSee Tip Tracker App	SECU	BofA Prepaid Mobile
Allpoint-ATM Locator	First Citizens Mobile Banking	TradingView - Stocks & Forex	Speedy Cash: Instant Loans
rapid!Access	Mortgage Calculator for iPhone	People's United Bank Mobile	TransUnion: Score & Report
Long Game Savings	American Family Insurance App	Empower Retirement	

References

[1] Tensor flow, tensorflow: An end-to-end open source machine learning platform. 2020, [Online]. Available: https://www.tensorflow.org/.

[2] Oh H, Park S, Lee GM, Heo H, Choi JK. Personal data trading scheme for data brokers in IoT data marketplaces. IEEE Access 2019;7:40120–32.

[3] Aktypi A, Nurse JRC, Goldsmith M. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In: International workshop on multimedia privacy and security at ACM conference on computer and communications security. 2017, p. 1–11.

[4] Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. Protection of big data privacy. IEEE Access 2016;4:1821–34.

[5] Belen Saglam R, Nurse JRC. Is your chatbot GDPR compliant? Open issues in agent design. In: International conference on conversational user interfaces. ACM; 2020.

[6] Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecur 2018;4(1).

[7] Nurse JRC, Creese S, De Roure D. Security risk assessment in internet of things systems. IT Prof 2017;19(5):20–6.

[8] Ramachandran GS, Radhakrishnan R, Krishnamachari B. Towards a decentralized data marketplace for smart cities. In: 2018 IEEE international smart cities conference. IEEE; 2018, p. 1–8.

[9] Piek M. Navigating between possibility and reality: an assessment of blockchain's potential for the dutch healthcare sector Master's thesis, Utrecht University; 2018.

[10] Lönnfält I, Sandqvist J. Blockchains, the new fashion in supply chains?-the compatibility of blockchain configurations in supply chain management in the fast fashion industry Master's thesis, Gothenburg University; 2018.

[11] Rumbold JM, Pierscionek BK. What are data? A categorization of the data sensitivity spectrum. Big Data Res 2018;12:49–59.

[12] European parliament, regulation (EU) (2016) 2016/679 of the European parliament and of the council of 27 april on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). Off J Eur Union 2016;59(L 119). [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[13] Cisco annual internet report (2018–2023) white paper. 2020, [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[14] Purtova N. The law of everything. broad concept of personal data and future of EU data protection law, law. Innov Technol 2018;10(1):40–81.

[15] Schwartz PM, Solove DJ. The PII problem: Privacy and a new concept of personally identifiable information. NYUL Rev 2011;86:1814.

[16] Ohm P. Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA L Rev 2009;57:1701.

[17] United states - california legislative information. 1974, [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[18] Estonia - personal data protection act. 2008, [Online]. Available: https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current.

[19] Tene O, Polonetsky J. Big data for all: Privacy and user control in the age of analytics. Nw J Tech Intell Prop 2012;11:xxvii.

[20] Martin-Bariteau F. Blockchain and the european union general data protection regulation: the CNIL's perspective, blckchn. ca, vol. 1. Working Paper Series, 2018.

[21] Hon WK, Millard C, Walden I. Who is responsible for personal data in cloud computing? The cloud of unknowing, part 2. Int Data Privacy Law 2012;2(1):3–18.

[22] Wuyts K, Verhenneman G, Scandariato R, Joosen W, Dumortier J. What electronic health records don't know just yet. a privacy analysis for patient communities and health records interaction. Health Technol 2012;2(3):159–83.

[23] Hodges D, Creese S. Breaking the arc: Risk control for big data. In: 2013 IEEE international conference on big data. IEEE; 2013, p. 613–21.

[24] Elliot M, Mackey E, O'Hara K, Tudor C. The anonymisation decision-making framework. Manchester: UKAN; 2016.

[25] Warken C, van Zwieten L, Svantesson D. Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. Int Rev Law Comput Technol 2020;34(1):44–64.

[26] Levallois-Barth C, Zylberberg H. A purpose-based taxonomy for better governance of personal data in the internet of things era: the example of wellness data, in data protection and privacy:(in) visibilities and infrastructures. Springer; 2017, p. 139–61.

[27] Richthammer C, Netter M, Riesner M, Sänger J, Pernul G. Taxonomy of social network data types. EURASIP J Inf Secur 2014;2014(1):11.

[28] Cradock E, Stalla-Bourdillon S, Millard D. Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform. Comput Law Secur Rev 2017;33(2):142–58.

[29] App download and usage statistics (2019). 2020, [Online]. Available: https://www.businessofapps.com/data/app-statistics/.

[30] Center IA. Data breach report: A study on global data leaks in H1 2018. 2018, [Online]. Available: https://infowatch.com/sites/default/files/report/analytics/Data_Breach_Report_Global_Data_Leaks_H1_2018.pdf.

[31] Elo S, Kyngäs H. The qualitative content analysis process. J Adv Nursing 2008;62(1):107–15.

[32] Lauri S, Kyngas H. Developing nursing theories. Vantaa, Finland: Werner Söderström, Dark Oy; 2005.

[33] Kyngas H, Vanhanen L. Content analysis (finnish). Hoitotiede 1999;11:3–12.

[34] Spain - organic LAW 15/1999 of 13 december on the protection of personal data. 1999, [Online]. Available: https://www.legislationline.org/download/id/1743/file/947c21b7194415dba67549f41b99.pdf.

[35] Google LLC, google fit: Health and activity tracking. 2020, [online]. Available: https://play.google.com/store/apps/details?id=com.google.android.apps.fitness&hl=en_GB.

[36] Lambe P. Organising knowledge: taxonomies, knowledge and organisational effectiveness. Elsevier; 2014.

[37] Nickerson RC, Varshney U, Muntermann J. A method for taxonomy development and its application in information systems. Eur J Inf Syst 2013;22(3):336–59.

[38] Austria - federal act concerning the protection of personal data (DSG). 2020, [Online]. Available: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf.

[39] Belgium - access to information and data protection. 2018, [Online]. Available: http://www.legislationline.org/topics/country/41/topic/3.

[40] Law for protection of personal data. 2019, [Online]. Available: https://www.cpdp.bg/en/index.php?p=element&aid=1194.

[41] Croatia - personal data protection act. 2003, [Online]. Available: https://www.right2info.org/resources/publications/laws-1/croatia-personal-data-protection-act/view.

[42] Cyprus - law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data of 2018 (law 125(i)/2018). 2018, [Online]. Available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3b_en/page3b_en?opendocument.

[43] Czechia - act of 12 2019 on personal data processing. 2019, [Online]. Available: https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837.

[44] Denmark - act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the data protection act). 2018, [Online]. Available: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf.

[45] Finland - personal data act. 1999, [Online]. Available: https://finlex.fi/en/laki/kaannokset/1999/en19990523_20000986.pdf.

[46] France - ACT no. 78-17 OF 6 1978 on information technology, data files AND civil liberties. 2014, [Online]. Available: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

[47] Germany - federal data protection act (BDSG). 2019, [Online]. Available: https://www.gesetze-im-internet.de/englisch_bdsg/index.htm.

[48] Greece - protection of personal data and privacy in the electronic communications sector and amendment of law. 2006, [Online]. Available: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF.

[49] Hungary - act CXII of 2011. 2011, [Online]. Available: https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf.

[50] Ireland - processing of personal data for law enforcement purposes. 1988, [Online]. Available: http://www.irishstatutebook.ie/eli/2018/act/7/section/69/enacted/en/html#part5.

[51] Italy - the Italian data protection authority. 2003, [Online]. Available: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1665291.

[52] Latvia - personal data protection law. 2019, [Online]. Available: http://www.arhivi.lv/index.php?&1170.

[53] Lithuania - Lithuania law on legal protection of personal data of June 11, 1996 no. I-1374 (new version of February 1, 2008, law no. X-1444). 2008, [Online]. Available: https://wipolex.wipo.int/en/text/202094.

[54] Luxembourg - official gazette of the grand duchy of Luxembourg memorial. 2018, [Online]. Available: https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/Act-of-1-August-2018-on-the-organisation-of-the-National-Data-Protection-Commission-and-the-general-data-protection-framework.pdf.

[55] Malta - data protection act. 2001, [Online]. Available: https://idpc.org.mt/en/Legislation/CAP%20586.pdf.

[56] Netherlands - personal data protection act. 2000, [Online]. Available: http://www.legislationline.org/documents/action/popup/id/5342.

[57] Poland - the act of 29 1997 on the protection of personal data (unified text: Journal of laws of 2014, item 1182 with amendments). 1997, [Online]. Available: http://www.giodo.gov.pl/144/id_art/171/j/en/.

[58] Portugal - the CNPD. 1991, [Online]. Available: https://www.cnpd.pt/english/index_en.htm.

[59] Romania - law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, amended and completed. 2001, [Online]. Available: https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj0yoDI5eHQAhXLsxQKHST6CJIQFggoMAA&url=http%3A%2F%2Fwww.dataprotection.ro%2Fservlet%2FViewDocument%3Fid%3D174&usg=AFQjCNEAIqcoMpBH9ukTuQgENSRZZgt95g.

[60] Slovakia - the english version of act 18/2018 on personal data protection and amending and supplementing certain acts. 1992, [Online]. Available: https://dataprotection.gov.sk/uoou/en/content/english-version-act-182018-personal-data-protection-and-amending-and-supplementing-certain.

[61] Slovenia - personal data protection act of the Republic of Slovenia. 1990, [Online]. Available: https://www.ip-rs.si/en/legislation/personal-data-protection-act/.

[62] Sweden - personal data act. 1998, [Online]. Available: https://www.qcert.org/sites/default/files/public/documents/swe-privacy-personal_data_act-eng-1998.pdf.

[63] United kingdom - data protection act 2018. 2018, [Online]. Available: http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

[64] Custers B, Dechesne F, Sears AM, Tani T, van der Hof S. A comparison of data protection legislation and policies across the eu. Comput Law Secur Rev 2018;34(2):234–43.

[65] Degeling M, Utz C, Lentzsch C, Hosseini H, Schaub F, Holz T. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. 2018, arXiv preprint arXiv:1808.05096.

[66] 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;6:9390–403.

[67] Apple app store. 2020, [Online]. Available: https://www.apple.com/uk/ios/app-store/.

[68] Google play. 2020, [Online]. Available: https://play.google.com/store.

[69] Moher D, Liberati A, Tetzlaff J, Altman DG, Group others P. Preferred reporting items for systematic reviews and meta-analyses: the prisma statement. PLoS Med 2009;6(7):e1000097.

[70] Sweeney L. Simple demographics often identify people uniquely. Health (San Francisco) 2000;671:1–34.

[71] Creation CA. Health tracker. 2020, [Online]. Available: https://play.google.com/store/apps/details?id=com.jvsmobileappssolution.healthtracker&hl=en_GB.

[72] Anhui huami information technology, mi fit. 2020, [Online]. Available: https://play.google.com/store/apps/details?id=com.xiaomi.hm.health&hl=en_GB.

[73] Ribaric S, Ariyaeeinia A, Pavesic N. De-identification for privacy protection in multimedia content: A survey. Signal Process, Image Commun 2016;47:131–51.

[74] Kwon YC, Lee SW, Moon S. Personal computer privacy: Analysis for korean pc users. In: International workshop on security. Springer; 2006, p. 76–87.

[75] Jones W. The future of personal information management, part i: our information, always and forever, synthesis lectures on information concepts, retrieval, and services. 4, (1):2012, p. 1–125.

[76] Presser L, Hruskova M, Rowbottom H, Kancir J. Care.data and access to uk health records: patient privacy and public trust. Technol Sci 2015;2015081103:1–35.

[77] Kim W, Jeong O-R, Kim C, So J. The dark side of the internet: Attacks, costs and responses. Inf Syst 2011;36(3):675–705, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306437910001328.

[78] Global banking and finance. 2020, [Online]. Available: https://www.globalbankingandfinance.com/the-world-is-shifting-to-virtual-wallets-heres-a-take-on-how-it-works-benefits/.