UiO : Faculty of Law
University of Oslo

Privacy risk assessment in relation to health and wellbeing apps:

Towards harmonizing the European laws, industry interests and the privacy expectations of the users

Candidate number: 8005

Submission deadline: 01/12/2015

Number of words: 17987

Privacy risk assessment in relation to health and wellbeing apps:

Towards harmonizing the European Laws, industry interests and the privacy expectations of the users

Table of Contents

Abstract

Health and wellbeing apps are proliferating at an exponential rate. It has created a billion dollar market that would make the industry seek every opportunity to take a competitive advantage. At times, this may be at the expense of the privacy of the app users. While most such apps do not collect sensitive medical data, some may collect or generate sensitive data during processing thus creating a high degree of risk towards users privacy. However, the current EU laws seem to be inadequate in protecting the privacy expectations of the users of such apps especially in the light of technologies such as cloud computing, big data and profiling. Meanwhile the EU and the National regulators seem to be facing a dilemma of harmonizing economic and wider societal benefits of personal and sensitive data processing and the data subject's right to privacy. This thesis postulates that privacy risk assessment is one strategy to harmonize these interests and ensure privacy of the health and wellbeing app users. Thus, it embarked first on enumerating the contribution to privacy risks by the health and wellbeing apps before recognizing the current state of privacy risk assessments within the EU context. It then recognized means of harmonizing the EU laws, industry interests and the privacy expectation of the app users. Through its analysis, the thesis proposes a scalable and a transparent privacy risk assessment obligation on the app developers and data controllers as a solution. However, in order to implement such an obligation, the EU laws ought to provide appropriate methodologies to ease the legal uncertainties as recommended through this thesis. At the same time, the National laws ought to provide standards for privacy risk assessments based on reasonable expectations of the app users, principles of proportionality, reasonable terms and qualitative parameters of privacy rights, supplementing the EU laws.

1. Introduction

1.1. Background and justification

Mobile health or m-Health apps is the generic term used to identify apps dealing with health data[1]. Among m-Health apps, some deal with prevention, diagnosis and treatment of diseases and communicate with the health care professionals. Other m-Health apps collect and process data related to lifestyle, fitness and wellbeing of a person mainly for the persons own use[2]. While the distinction may not be clear cut at all times, apps contributing to the care pathways[3] are regulated to a certain extent through national and international laws (e.g. Council Directive 93/42/EEC on Medical Devices) and m-Health specific accreditation mechanisms (e.g. Accreditation programs for m-Health apps by National Health Services, United Kingdom and Federal Drug Authority, USA). The second group of apps, referred hereafter as 'health and wellbeing apps', are not so regulated given its seemingly non-impacting nature on care pathways. However, such apps are capable of collecting numerous health related and non-health related personal data from users as with any other mobile app.

At present, there are more than 100,000 such apps available in the market and this number is expected to multiple many folds[4]. Health and wellbeing apps market in Europe will reach 5.4 billion Euros by 2017, exceeding that of North America[5]. Given the ability of health and wellbeing apps to empower citizens, cut costs for healthcare systems, function as an effective channel of communicating health messages to a large section of the population, and contribute to improved health outcomes among the population[6], it is likely that such apps would dominate the

[1] Kay, Misha, Jonathan, Santos and Marina, Takane. *mHealth – New horizons for health through mobile technologies*. Geneva, World Health Organisation, 2011. (Global-Observatory for eHealth series–3/2011).
[2] Ibid.
[3] Vanhaecht K, De Witte K, Sermeus W. *The impact of clinical pathways on the organisation of care processes*. Belgium,(KU Leuven) 2007.
[4] European Commission. *Green paper on mobile health ("mHealth")*.Brussels, (European Commission) 2014.
[5] Ibid.
[6] *Supra*, note 2

market in the coming years. At the same time, given the freedom enjoyed by health and wellbeing apps from the regulators, businesses and individuals can come up with innovations that propagate the industry further. While the wealth of data collected through these apps provides researchers, governments, industry as well as the users many benefits, there may be instances where such benefits are gained at the expense of users' privacy[7].

From a practical point of view, the different types of data collected through health and wellbeing apps may include vital signs such as heart rate, blood pressure, body temperature, blood glucose levels and other lifestyle data such as food consumption and number of steps taken during the day. According to Article 7 of the European Union (EU) data protection directive[8], these data are to be considered personal data if the same relates to an identified or identifiable natural person. In some instances, as in the case of medical data, EU directives consider the same as sensitive data necessitating special provisions for its processing[9]. However, there are issues pertaining to health and wellbeing apps, in terms of determining whether such apps are dealing with sensitive data or not. For instance, some data may not be considered as 'sensitive data' when registered once or used as it is. However, when combined with other data sets and information, it may give rise to sensitive information regarding the health and lifestyle of a particular person[10]. The sensitive data thus created may be used by a third party for targeted actions.

At present, it is perceived that m-Health apps can be made to comply with the EU directives simply by obtaining the consent of the user or the data subject[11]. However, this would require data subjects being able to review the privacy policy and be informed about what data collected and for what purpose. Nevertheless, such privacy policies are not mandatory for health and well-

[7] Lupton, Deborah. *M-health and health promotion: The digital cyborg and surveillance society*. In:Social Theory & Health.Vol.10 (2012), pp. 229-244.
[8] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter 'DPD'), 24 October 1995, Article 7.
[9] DPD, Article 8.
[10] *Supra*, note 4.
[11] Mylonas, Alexios, Marianthi Theoharidou, and Dimitris Gritzalis. *Assessing privacy risks in Android: A user-centric approach*.Geneva, Springer International Publishing, 2014. (Lecture notes in Computer Science Series; 8418/2014)

being apps currently available in the market, at least from the point of view of sellers or distributors of these apps[12]. At the same time, even if such policies are made available, it is recognized that app users are generally oblivion to privacy policies and therefore may ignore the privacy statements or may not understand them at all[13]. Thus, there is a need for a responsible party to minimize the privacy risks enforced upon the users[14].

Recognizing this need, particularly in relation to health and wellbeing apps, the Article 29 Working Party accepted risk-based approach to privacy as a balanced means of recognizing the potential privacy risks[15]. It also recommended to develop guidelines for privacy impact assessment and other accountability tools in line with privacy risk management methodologies adopted by CNIL (Commission nationale de l'informatique et des libertés – French Data Protection Authority) and ICO (Information Commissioner's Office, UK)[16]. The Article 29 Working Party opinion complements Article 33 of the proposed Data Protection Regulations (GDPR)[17], which describes the contents of a data protection impact assessment to be carried out in relation to data processing operations that pose a specific risk. In that, one area is to perform a risk assessment in-line with the rights and freedoms of the data subjects, including privacy rights[18]. At the same time, the GDPR also states that commission may specify standards and procedures for carrying out, verifying and auditing such assessments[19]. In other words, those who are developing health and wellbeing apps or those who are controlling or processing personal data would be liable for not adhering to acceptable data protection impact assessments, of which privacy risk assessment plays a central role. This also means that at least in the EU context, privacy risk assessment re-

[12] *Supra*, note 11.
[13] Felt, A, Ha, E, Egelman, S, Haney, A, Chin, E and Wagner, D. *Android permissions: user attention, comprehension, and behavior*. In: Proceedings of the 8th Symposium on Usable Privacy and Security.ACM (2012).
[14]Article 29 Working Party. *Opinion 02/2013 on apps on smart devices – WP202*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [visited 2nd October 2015].
[15]Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks - 14/EN WP 218*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf [visited 28th September 2015]
[16]*Supra*, note 15
[17] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter 'GDPR'), 25 Jan. 2012, COM(2012) 11 final—2012/0011(COD)
[18]GDPR, Section 3, Article 33 (3)
[19]GDPR, Section 3, Article 33 (7)

garding health and wellbeing apps has not yet been guided in accordance with the actual privacy expectations of its users. In the absence of a holistic guidance, uncertainty manifests in the minds of those who develop such apps, those who determine and control data processing operations and among the users. In such a situation, exploitation of data might take place and the industry will undertake innovations overenthusiastically. Furthermore, undue fears about privacy breaches among the users may prevent them from using such apps and thereby loosing the individual and societal benefits afforded to them by such apps.

Thus, this thesis expects to fill this vacuum by discussing some of the key elements of a privacy risk assessment for health and wellbeing apps in view of harmonizing the EU laws, industry interests and actual privacy expectations of the app users.

1.2. Research questions

Thus, this thesis undertakes answering several research questions. These include;

1. How mobile health and wellbeing apps contribute to privacy risks?
2. What is the state of privacy risk assessment approaches relevant to mobile apps processing personal data?
3. What are the important considerations in relation to privacy risks assessment approaches that would facilitate harmonisation the EU laws, industry interests and actual privacy expectations of the users of health and wellbeing apps

1.3. Scope and limitation of the thesis

Given the nature of privacy risk assessments and related processes such as privacy impact assessment (PIA) and data protection impact assessment (DPIA), this research needs to be specific in areas that it shall focus and areas that it shall exclude.

As a start, the thesis limits itself to privacy risks related to health and wellbeing apps.

At the same time, as indicated in the background and justification, this thesis also limits its scope to the privacy risk assessment, which is usually embedded within much wider privacy impact assessment (PIA) methodologies. There are several reasons for the thesis to limit its focus to privacy risk assessment. Firstly, a fully-fledged PIA for health and wellbeing apps is beyond its time and resource availability. Secondly, gaining the support of the industry for a privacy risk assessment process has been recognized as one of the biggest challenges within the PIA as industries are less motivated in undertaking a time consuming and costly privacy risk assessment than adhering to a less stringent requirements set out by the law[20]. Thus, most PIAs conducted by the industry are mere legitimizations than true risk assessments. Therefore, by focusing on the privacy risk assessment of the PIA, the thesis should be able to enumerate ways and means of mitigating this challenge. Thirdly, given the specialized nature of health and wellbeing apps, any recommendation related to privacy risk assessment should be concrete enough to uncover all potential risks and be generic enough to be applicable to all potential applications of such technologies[21]. This emphasizes that even the privacy risk assessment component within the PIA is substantial enough to warrant an in-depth analysis.

From a different point of view, the thesis distances itself from the traditional information technology (IT) risk assessment methods (or IT security risk assessment), which are more focused on tangible assets and system security[22]. While acknowledging that privacy and security risks are interconnected, a security focused risk assessment is known to cause ineffective communication strategies, high level of uncertainty in risk estimation and incomprehensible risk estimation measures[23]. Furthermore, one of the main objectives of this thesis is to discuss important legal norms in privacy risk assessment thus leading to a comprehensive understanding of legal privacy

[20] *Privacy impact assessment*. Edited by Wright, David and Paul De, Hert. Houten,(Springer Science & Business Media) 2011.
[21] *Supra*, note 20.
[22] Terje, Aven. *A semi-quantitative approach to risk analysis, as an alternative to QRAs*. In:Reliability Engineering & System Safety. Vol.93(2008), pp.790 – 797.
[23] Paintsil, Ebenezer and Lothar, Fritsch. *Towards Legal Privacy Risk Assessment Automation in Social Media*. erschienen im Tagungsband der INFORMATIK 2011. http://www.user.tu-berlin.de/komm/CD/paper/090221.pdf [Visited 17th November 2015].

risk assessment pertaining to health and wellbeing apps. This is another reason for the thesis to distance itself from the traditional IT risk assessment methods.

Lastly, given the variation in technology, application and the context pertaining to health and wellbeing apps, it is beyond the scope of this thesis to enumerate a comprehensive list of privacy risks emanating from such apps or to define best practices for the industry in undertaking a privacy risk assessment. Instead, as indicated through the research questions, the thesis will focus on important considerations in relation to privacy risk assessment approaches that would allow harmonising the EU laws, industry interests and actual privacy expectations of the users.

1.4. Legal method

When considering the focus of this thesis, which is to harmonize the EU laws, industry interests and actual privacy expectations of the users of health and wellbeing apps, it is clear that the thesis needs to adhere with a non-doctrinal legal research methodology[24].

Thus, at the heart of this thesis will be the European Data Protection Directive[25] (referred hereafter as the DPD) and the Directive on privacy and electronic communications[26] (referred hereafter as the e-Privacy directive). However, given the state of flux existing within the EU context regarding data protection laws, the proposed EU General Data Protection Regulation (referred hereafter as GDPR) will also act as a primary source of data. In addition, court decisions (European Court of Justice, European Court of Human Rights and other court decisions pertaining to the European context), Article 29 Working party opinions and national legislation in European contexts shall also be utilized as sources of data.

---

[24] *The Oxford handbook of empirical legal research.* Edited by Cane, Peter and Herbert, Kritzer.Oxford, (University Press) 2010.
[25] Directive 95/46/EC (DPD)
[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)(e-Privacy Directive)

From the point of view of privacy risk assessment, the thesis will make use of privacy risk management methodologies adopted by CNIL (Commission nationale de l'informatique et des libertés – French Data Protection Authority), ICO (Information Commissioner's Office, UK) and the Privacy and Data Protection Impact Assessment Framework for RFID Applications. These will be referred hereafter as CNIL PIA, ICO PIA and RFID PIA respectively. At the same time, the thesis will also make use of other relevant privacy risk assessment literature that would provide an understanding of the current state of affairs in relation to risk-based approach to privacy in the EU context. The RFID PIA was chosen for this analysis on the basis that it was recognized as generic enough to be utilized as a blue print for privacy impact assessment in relation to the internet of things[27]. The ICO PIA and the CNIL PIA were selected on the basis that these were recognized by the Article 29 working party as suitable references for developing guidelines on impact assessment[28].

However, for the purpose of this thesis, which is limited by time and resources, the empirical data utilized in traditional non-doctrinal research would be gathered through secondary sources. This would mean that when it comes to enumerating the actual privacy expectations of health and wellbeing app users, this thesis will depend on secondary data sources such as journal articles and texts books, which discuss privacy expectations from a user-based perspective. Similarly, in order to understand the implications of the health and wellbeing app technology on privacy and to deduce the innovative potential of the app industry, the thesis will depend on secondary sources.

During the legal analysis, the thesis will discuss both the applicability of the current laws, regulations, guidelines and judicial decisions (de lege lata) and how it ought to be in the future (de lege ferenda) practice of privacy risk assessment pertaining to health and wellbeing apps.

---

[27] *Privacy Impact Assessment*, *Supra*, note 20.
[28] *Supra*, note 15.

1.5. Organization of the thesis

The thesis is organized into seven chapters including the introduction chapter. The second chapter will present the core concepts related to this thesis and will provide the thesis with a firm grounding. The third chapter will present an overview of health and well being apps and various aspects related to the privacy discourse around the same.

The fourth chapter will discuss the current legal discourse around risk-based approach to privacy and would link the same with privacy risk assessment in health and wellbeing apps.

The fifth chapter will compare between three different privacy impact assessment approaches namely the RFID PIA, ICO PIA and the CNIL PIA. The aim of this chapter will be to enumerate the current state of privacy risk assessments in the EU.

The sixth chapter will discuss the issue of harmonizing the different interests within privacy risk assessments.

The seventh chapter will present the conclusions and will make recommendations related to harmonizing the EU laws, industry interests, and the privacy expectations of the health and well-being app users.

2. Core concepts

The purpose of this chapter is to introduce some of the core concepts used within this thesis, which provide this thesis with the necessary grounding and a point of departure. Thus, it will bring to the forefront the concepts of personal data and its processing, sensitive data, data controller and data processor and the different terms used in the privacy discourse.

2.1. Personal data and processing

According to the DPD[29] Article 2(a), personal data refers to "any information relating to an identified or identifiable natural person." It further explains that within the ambits of personal data, its potential to identify a person may be either direct or indirect and may refer to an identification number or to one or more factors specific to his or her "physical, physiological, mental, economic, cultural or social identity." This means that even if it is not apparent at the time of collection, if a particular data, on its own or in combination with other data, refers to an identifiable person, such data can be considered as personal data.

Within the DPD, processing personal data is elaborated in detail and this covers "any operation or set of operations performed upon personal data", either manually or through automated means[30]. Thus, it is interesting to note that the collection of personal data itself is also part of data processing. From a DPD perspective, this would mean that collection of personal data of any nature requires obtaining the data subjects unambiguous consent or fulfilling other criteria such as the need to fulfill contractual obligations by the data controller, protecting the vital interests of the data subject, abide by legal obligations...etc.

2.2. Sensitive data

The necessity to consider certain types of personal data as 'sensitive data' emerged as a result of such data being able to impart severe consequences on the individual's right to privacy and the

[29]DPD
[30]*See* DPD, Article 2 (b).

right for non-discrimination[31]. Within the EU, it is recognized that data types such as health data and sexual orientation related data may have irreversible and long-term consequences when misused than when other types of personal data are misused[32]. Thus, special provisions for processing such data are provided through the Article 8 of the DPD under 'special categories of sensitive data'. In general, Article 8(1) imparts a general prohibition on the processing of personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." Thus, when it comes to sensitive data, the DPD not only considers data which by its very nature contains sensitive information, but it also considers data through which sensitive information can be concluded through processing or otherwise. Nevertheless, Article 8(2) describes exceptions to section 1, out of which the most important would be instances where the data subject's explicit consent has given to the processing of such data.

2.3. Data subject, data controller and data processor

While the DPD is not explicit about the definition of the data subject, it is understood that the data subject means an individual who is the subject of the personal data being discussed within the said directive.

On the other hand, the DPD is much clearer about the data controller and the data processor, the two entities responsible for adhering with the DPD. Article 2 of the DPD describes that a data controller is a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;…". Data processor on the other hand is defined as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[33]

[31]European Union Agency for Fundamental Rights. *Handbook on European data protection law*. Belgium. 2014. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [Visited 14th October 2015].
[32] *Supra*, note 31.
[33] DPD, Article 2 (e).

Most data controllers within the ambit of the DPD are organizations although individuals may also be considered as data controllers. However, data processors may not directly be subjected to the current Directive.

In addition to these two concepts, the GDPR introduces a new legal entity known as the 'producer'. Producer refers to an entity creating automated data processing and filing systems for processing personal data by the data controllers and data processors[34]. From the point of view of the GDPR, producers and data processors together are responsible for technical and organizational measures that would allow data controllers by-default to adhere with its regulations[35].

2.4. Privacy and privacy risk

Privacy is a term defined in Oxford dictionary as the "state in which one is not observed or disturbed by other people."[36] When it comes to the legal domain, privacy has been described as an amorphous concept that is difficult to define[37]. With respect to this thesis, privacy would refer to informational privacy as the key focus here is personal and sensitive data.

The European perception on privacy is largely grounded on the statements set forth within the Charter of Fundamental Rights of the European Union. In that, Article 7 states, "Everyone has the right to respect for his or her private and family life, home, and communications." Article 8 on the other hand lays down the basic rights for personal data protection. However, it is under the Treaty on the Functioning of the European Union (Lisbon Treaty) [38] that protection of personal data became a fundamental right from the perspective of the EU. As a result, within the EU context, upholding the core elements in the exercise of data protection and privacy became foundation to most, if not all, legal and policy measures.

---

[34] *See* GDPR
[35] *See* GDPR, Article 23
[36] Available at http://www.oxforddictionaries.com/definition/english/privacy
[37] Bernstein ao v Bester NO AO 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC)
[38] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007

Within the EU, the Data Protection Directive (DPD)[39] and the E-Privacy Directive[40] provide the necessary legal provisions to uphold the values set forth by the above treaties in ensuring privacy and data protection. These legal provisions are formulated around the data protection principles set out by the Article 5 of the Convention 108, and it is these principles that drive the privacy discussion even at present.

However, in accordance with the principle of lawful processing, privacy as set forth within the directives and within the Charter of the Fundamental Rights of the EU, is not an absolute right[41]. The point here is that privacy should be considered in relation to its function in the society[42] and this would mean that the EU understanding of privacy protection is necessarily a balance against the fundamental freedoms of free movement of persons, goods, services and capital.

Privacy risk on the other hand is a state in which an individual's privacy is threatened as a result of his or her personal data being mishandled[43]. For the purpose of this thesis, it can also be viewed as the "potential loss of control over personal information" even when a person has given his or her consent to the processing of such data[44].

2.5. Risk analysis and risk assessment

In simple terms, risk analysis is the method used in estimating risks. Risk assessment on the other hand, is the method in which risks can be qualitatively and quantitatively estimated[45].

---

[39] *See* DPD
[40] E-Privacy Directive
[41] See, CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 48.
[42] *Supra*.
[43] Martin, Hansen...(et al.). *Shaping the Future of Electronic Identity Privacy Requirements*. http://futureid.eu/data/deliverables/year1/Public/FutureID_D22.03_WP22_v1.0_PrivacyRequirements.pdf [Visited 20th October 2015].
[44] Greenaway, Kathleen, Susan Zabolotniuk, and Avner Levin. *Privacy as a Risk Management Challenge for Corporate Practice*. 2012. Ted Rogers School of Management. http://ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf [Visited 11th November 2015].
[45] *Privacy impact assessment*, Supra, note 43

While most risk analysis methods depend on historical incidents, their known damages and the frequency of occurrence under different circumstances, such methods are bound to become ineffective when it comes to complex systems and when analyzing privacy risks[46]. The reason being that in privacy risk analysis, a particular event that may seem innocent in terms of its handling of data at present, may in fact cause personal distress to a person at a later stage. At that point, the previous handling of data may be interpreted as a mishandling. Such events are likely to manifest particularly when it comes to sensitive data such as health data. Thus, these situations demand for a risk assessment that would be sensitive to a wide range of factors that contribute to the manifestation of a privacy risk.

2.6. Data Protection Impact Assessment

DPIA can be described as a method of checking whether the legal requirements spelt out by various directives and regulations within the EU are met when undertaking a data processing task[47]. In general, DPIAs require following a checklist that would detail the various actions and measures to be taken in terms of different data protection principles as provided through different directives and regulations. At present, there isn't an obligation towards carrying out a DPIA within the EU other than the general obligation to comply with the data protection laws[48]. Thus, one may argue that DPIA is a compliance exercise than an attempt at assessing the true privacy risks to the data subjects.

2.7. Privacy impact assessment

Privacy Impact Assessment (PIA) on the other hand is a concept that extends beyond being a compliance check as described in terms of a DPIA[49]. According to the European Commission, Privacy Impact Assessment (PIA) is "a process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal

[46] *Supra*, note 43
[47] *Privacy Impact Assessment, Supra*, note 20.
[48] *Supra*, note 20
[49] *Supra*, note 20

data."[50] Thus, PIA entails identifying privacy risks, foreseeing problems and determining solutions that would be able to mitigate such problems. PIA can also be defined as a "methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts."[51] In most instances, the final aim of a PIA is to minimize the risks. However, similar to the DPIA, PIA is still not a mandatory legal requirement.

[50] *A Privacy Impact Assessment Framework for data protection and privacy rights*. Edited by David Wright, Kush Wadhwa, Paul De Hert and Dariusz Kloza. Seventh Framework Program.
http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf [Visited 28th September 2015]
[51] *Supra*, note 20

3. Health and wellbeing apps and privacy

The aim of this chapter is to understand how health and wellbeing apps create risks to the privacy of its users. In doing so, the chapter will position the core concepts discussed in the previous chapter within the privacy discourse around health and wellbeing apps. Thereafter it will enumerate the industry interests, privacy expectations of the users, and the impact of cloud computing, big data and profiling technologies on app users' privacy.

3.1. Overview

Mobile apps are software programs designed to run in mobile devices such as smart phones and tablet computers. Such software are usually distributed through application distribution platforms owned by the owners of operating systems (OS) installed in various mobile devices as in the case of Apple App Store, Google Play for Android apps and Windows Phone Store. Although the distribution channels for mobile apps are largely limited, there are other application distribution channels owned by third parties as well. The apps made available in any distribution platform may be developed either by individuals or by organizations and may be available for a fee or for free.

Health and wellbeing apps are also made available through application distribution platforms and it belongs to the broad category of mobile apps known as 'mHealth' apps[52]. These apps may utilize a range of technologies such as short message service (SMS), 3G systems, global positioning systems (GPS), Bluetooth technologies and even external sensors in providing its services[53]. In most instances, these apps would directly or indirectly help or will claim to be helpful to its users

[52] *Supra*, note 1.
[53] West, DM. *Improving health care through mobile medical devices and sensors*. *Brookings Institution Policy Report*. 2013. http://www.brookings.edu/~/media/research/files/papers/2013/10/22-mobile-medical-devices-west/west_mobile-medical-devices_v06.pdf [Visited 23rd October 2015].

in maintaining or improving their healthy behaviour, quality of life and wellbeing in various ways[54].

3.2. Types of data collected

While many other mobile apps would not evoke privacy and data protection concerns when used by the consumers, health and wellbeing apps attract attention from the regulators. The reason being that such apps collect personal data that may or may not be classified as health data as described earlier. If such data is used for the persons own benefit and is not processed further, it is unlikely that it would evoke a threat to privacy. However, if the personal data collected through these apps are processed further, it may evoke the regulations set forth in the DPD and other laws.

While most health and wellbeing apps may be recognizable as collecting personal data, it isn't easy to determine whether such apps are dealing with sensitive data or not. However, if a health and wellbeing app processes health data, it evokes Article 8 of the DPD that governs the processing of special categories of data as discussed earlier.

However, although the DPD offers protection to health data, the problem there in is the difficulty in determining whether a particular type of data can be classified as health data or not. For instance, non-medical data such as a person's weight, the number of steps taken, his or her blood pressure...etc may not be classified as health data. The reason being that these data on its own would not refer to a person's health status. However, it is not only the intrinsic nature of the data that makes them health data[55]. In other words, if personal data is processed in a medical context,

---

[54] Milošević, Mladen, Michael T. Shrove, and Emil Jovanov. *Applications of smartphones for ubiquitous health monitoring and wellbeing management*. In: *JITA-Journal of Information Technology and Applications (Banja Luka)-APEIRON* 1.1 (2011).

[55] European Data Protection Supervisor. *Opinion 1/2015 on Mobile Health - Reconciling technological innovation with data protection.* Brussels. 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf [Visited 12th September 2015].

is monitored over a period of time and is capable of inferring reasonably to a person's health, such data may be considered health data within the ambits of the DPD[56].

This means that when health and wellbeing apps collect and store data related to one's eating habits, movements, weight, drinking or smoking habits, blood pressure, heart rate, daily exercises...etc over a period of time, such data would become health data as these can be used to infer to a person's health status (e.g. disease risk and nutritional state)[57]. However, it is not possible to provide a blanket cover by saying all data collected by health and wellbeing apps are health data, as it would depend on the nature of the data collected, circumstances of its collection and the nature of its processing.

3.3. App developer, data controller and data processor

When it comes to health and wellbeing apps, there are different entities that can play the roles of data controller and data processor. For instance, in terms of data processing related to smart devices and apps, app developers, manufacturers of operating systems and devices, app stores and other parties involved in processing personal data[58] could all be playing the above two roles.

Out of these entities, the app developer refers to an entity, which creates or deploys an app to be used by the consumers[59]. These developers can decide the purpose and the process in which consumer's data would be processed, either within the device itself or through external processors. Therefore, the app developer may evoke the Article 2 (b) of the DPD in terms of being a 'data controller' and thereby should align themselves with the directives requirements. At the same time, a developer may also evoke Article 5(3) of the ePrivacy directive if it accesses information that is stored within the consumer's device.

---

[56] Article 29 Working Party. Clarification of the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps -Annex - health data in apps and devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [Visited 12th September 2015].
[57] *Supra*, note 56.
[58] Opinion 02/2013, *Supra*, note 14
[59] *Supra*, note 14

From the point of view of health and wellbeing apps however, other parties as mentioned earlier may not play an important role as a data controller when compared with the app developers. For instance, certain apps may utilize the GPS of the device to track the movements of a person and determine the geo-location of the person. In some instances, it may be possible that the OS and device manufacturers decide to use the personal data thus collected to improve its own location services. In such instances, the manufacturer would also become a data controller[60]. However, in terms of health and wellbeing apps, it is unlikely that OS and device manufacturers would handle health data, as was the case with the app developers.

Similarly, app stores may also be playing the role of a data controller when it collects and process personal data of the clients who are downloading apps from its stores. While it may be true that personal data of consumers who download health and wellbeing apps may also be handled in a similar manner by app stores, it is unlikely that these personal data be considered health data.

Third parties on the other hand may act as both data controllers or as data processors. For instance, if a data controller of a health and wellbeing app recruits a third party to process data or to provide analytics within its app, the third party is undertaking the role of a data processor. However, when a third party service utilizes the information gathered from a health and wellbeing app for its own use (e.g. for targeted marketing), they would become data controllers[61] as well. Nevertheless, this thesis sees the potential of app developers to track the path taken by a particular set of data in its processing cycle and therefore their ability to foresee the potential privacy risks towards the data subjects.

[60] *Supra*, note 14
[61] *Supra*, note 14

3.4. EU economic policies and industry interests

Within the European context, mHealth has been recognized as a key area of innovation and research[62]. The importance placed by EU policymakers on mHealth developments can be understood when considering that funding for mHealth projects began through Fifth Framework Program in 1998 and have continued under the Horizon 2020 program[63]. One of the key objectives in promoting mHealth by the European community is its potential to make citizens co-managers of their own health and wellbeing.

From an economic point of view, this would translate into cost savings for public health services and benefit the European economy as a whole. At the same time, a competitive mHealth market also means that Europe could attract investors, entrepreneurs, scientists and other professionals making EU a forerunner in mHealth developments and research[64]. Such leadership in the mHealth market has been seen as a wealth generator for any economy in the coming years[65]. Therefore, the EU has made it a priority to support web entrepreneurs through its eHealth Action Plan 2012-2020. In that, the goals are to network European high-technology accelerators to provide legal, financial and technical advice and training for eHealth start-ups[66]. The ultimate aim is therefore to create favourable market conditions for the entrepreneurs to develop innovative products and services including health and wellbeing apps.

However, the EU policymakers have also recognized the usefulness of data gathered through mobile apps beyond its intended purpose for the benefit of the wider society. In fact, Article 29 Working Party recognizes that such data are genuinely useful in other purposes and therefore the EU should facilitate some degree of additional use of such data with carefully balanced limits[67]. Specifically, the EU policymakers consider the vast amount of data gathered through mHealth

---

[62] Walshe Kieran...[et al.]. *Health systems and policy research in Europe:Horizon 2020.* In: The Lancet .Vol. 382(2013).pp.668-669.
[63] *Green paper on mobile health*, Supra, note 4
[64] *Supra*, note 63
[65] European Data Protection Supervisor. Supra, note 55
[66] European Commission. *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century*. Brussels, 2012. http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf [Visited 14th October 2015].
[67] *Opinion 1/2015 on Mobile health*, Supra, note 55

apps or 'big data' as valuable to the EU and its population in many different ways[68]. Interestingly enough, the app industry also has the same understanding.

From a practical point of view, mHealth industry also sees potential barriers in the form of lack of interoperability and open platforms[69]. While these issues are mostly recognized in relation to medical apps, this also indicates that the industry expects mHealth apps such as health and well-being apps to communicate with one another and also with other services. In relation to open platforms, the industry sees the same as facilitating the innovative potential[70] although the same would be much difficult to regulate and would be 'unsafe' than closed proprietary platforms[71]. In other words, this thesis recognizes that an open approach to innovation without regulation may not promote consumers to take up health and wellbeing apps as they would with any other type of app.

3.5. Actual user expectation

From users point of view, they consider apps that support monitoring, tracking and reviewing behaviour, as in the case of certain health and wellbeing apps, useful and interesting[72]. At the same time, consumers are generally averse to sharing information related to health behaviour via social networks and react negatively towards constant intrusions by such apps through prompting and reminding[73]. In addition, the use and the perception regarding apps have also been recognized as changing with the mood and the motivation of the user[74].

---

[68] *Supra*, note 55.
[69] European Commission. *Digital Agenda for Europe*. 2015. http://ec.europa.eu/digital-agenda/en/news/mhealth-green-paper-next-steps [Visited 11th October 2015].
[70] PA Consulting, *Policy and regulation for innovation in mobile health*. London. 2012. http://www.gsma.com/connectedwomen/wp-content/uploads/2012/04/policyandregulationforinnovationinmobilehealth.pdf [Visited 14th October 2015].
[71] *Supra*, note 70
[72] PWC. *Emerging mHealth: Paths for growth*. 2014. https://www.pwc.com/gx/en/healthcare/mhealth/assets/pwc-emerging-mhealth-full.pdf [Visited 12th October 2015]
[73] Deloitte center for health solutions. *Connected Health: How digital technology is transforming health and social care*. 2015. http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf [Visited 20th October 2015].
[74] Dennison, Laura...[et al.]. *Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study*. In:Journal of medical Internet research. Vol.15(2013).

In terms of perceived risks, users have conveyed their unease with regard to privacy of the data collected through health and wellbeing apps particularly when such apps use features of context sensing[75]. Adding to these concerns is users suspicion of these apps processing their data without their awareness or authorization[76]. However, it is unclear whether these fears have risen as a result of the users awareness regarding lack of laws and regulation on health and wellbeing apps or is it because of their inherent fears regarding data being kept on electronic devices or online.

3.6. Technologies related to health and wellbeing apps

Big data

The concept big data refers to the "capacity to analyze a variety of (unstructured) data sets from a wide range of sources"[77]. Through such analysis, which are usually done through cost effective automated means, potentially valuable data can be extracted from unstructured raw data. The key to such extractions is the process of link building between different data sets and this would mean that in big data, relationships between data can be made apparent[78].

When considering health and wellbeing apps, the data collected may become part of the data sets linked and analyzed in big data processes. This could happen when these apps share data with a third party or else when the controllers of the collected data decide to do the processing by themselves. Through big data processes, it may be possible to harness valuable insights into health and wellbeing of a larger population, and also to make inferences regarding data subjects[79].

[75] *Supra*, note 74
[76] *Supra*, note 74
[77] *Green paper on mobile health*, *Supra*, note 4
[78] Hasan, Osman...[et al.]. *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case*. In: 2013 IEEE International Congress on Big data. IEEE (2013)
[79] *Supra*, note 55

While there are many potential benefits of big data processes, it may also lead to privacy invasions as in the case of commercial exploitations[80]. Given that having more knowledge about the consumers would give commercial establishments an advantage in a competitive market such as in the EU, the tendency towards exploiting big data techniques around health and wellbeing apps would continue to pose a threat to privacy.

Nevertheless, the DPD even in its present state provides some degree of safeguards for privacy concerns in an event such as big data. For instance, as per Article 6 of the DPD, data controllers are bound by the principles of legitimacy, data minimization, purpose limitation, transparency, data integrity and data accuracy. When applied to big data, any data controller would be bound to maintain data quality resulting from such processes. Further, the transparency principle is inseparably connected within the legal grounds of consent, thereby requiring big data controllers to adhere with the same[81].

However, the market dynamics are such that data controllers, also being innovators, will constantly recognize new opportunities and purposes that were not recognized earlier. To stay ahead of the market, they must grab opportunities presented to them and therefore may resist tracking or limiting such purposes[82]. Furthermore, re-informing the data subjects of the new purposes emerged as a result of big data may also not be feasible at all times given the automated nature of most such processes. It may be such factors that lead Article 29 Working Party to recognize the usefulness of allowing some degree of flexibility in additional use within carefully balanced limits[83].

---

[80] Crawford Kate and Jason Schultz. Big data and due process: Toward a framework to redress predictive privacy harms. In:*BCL Rev.* 55 (2014). p.93.
[81] Opinion 02/2013, Supra, note 14
[82] *Supra*, note 55
[83] Article 29 Working Party. *Opinion 03/2013 on purpose limitation*. http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf [Visited 12th October 2015].

Profiling

User profiling refers to a process in which information about a user is collected to construct a particular profile[84]. Such profiles will consist of various attributes including geographical location, academic and professionals' credentials, interests, memberships in professional groups, opinions and other attributes, which will aid in describing a person. The attributes recognized through profiling may be used for various purposes and among them, one of the primary uses is to recommend material and non-material things to a user that might have not yet thought about and may find it useful nevertheless[85].

In terms of health of a person, such profiling may aid predicting health risks based on the present lifestyle and other information extracted from the said person[86]. While profiling would inevitably be beneficial in terms of preventing harmful health outcomes and improving the quality of life of a person, the market driven economy might overtake the benefits of profiling through its exploitations. For instance, an insurance company might refuse to insure a person on the basis that the person in question is linked with another person who is having a particular disease condition. Thus, profiling can impact on the privacy of the data subjects in an unprecedented level.

In line with these views, the EU has recognized several areas of privacy concerns in relation to profiling that warrants its legislation to be amended accordingly[87]. For instance, it recognizes that by linking large number of individuals through profiling techniques, it would be possible to place individuals in a pre-determined category without their knowledge and therefore subjected to discrimination[88]. At the same time, such techniques make it possible to create new personal data other than the data communicated to the data controllers by the data subjects. While the EU

---

[84] Committee of Ministers. *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*. https://wcd.coe.int/ViewDoc.jsp?id=1710949 [Visited 11th October 2015].
[85] Article 29 Working Party. *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation.* Brussels. 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf [Visited 16th October 2015].
[86] Ibid.
[87] Ibid.
[88] *Supra*, note 85.

also sees the necessity to implement appropriate safeguards, it is of the view that such safeguards need to be balanced between privacy risks and benefits of profiling[89].

Although the DPD does not explicitly cover instances of profiling, Article 15 for instance recognizes that individuals have a general right to object automated decision making. However, the DPD also justifies such automated processes in different circumstances as long as the individuals legitimate interests are recognized[90].

Article 29 working party however, after assessing the benefits and the negative consequences of profiling, determined that data controllers need to be clear with their data subjects regarding the "purposes for which the profiling is carried out and the logic involved in the automatic processing"[91]. The working party also determined that when profiling does not significantly affect the individuals rights, such profiling should not be subjected to specific rules and regulations except for the general data protection rules. However, it is unclear as to how to assess a 'significant affect' as indicated by the Working Party.

Given the importance of profiling as a potential threat to data protection and privacy, the proposed GDPR reserves its Article 20 for 'measures based on profiling'[92]. In fact, it is an extension of the Article 15 of the DPD and focuses on the data subjects legitimate interests, suitable safeguards and consent. At the same time, it focuses on having a balance between benefits of profiling and privacy risks by emphasizing on the need to disclose the existence of an automated data processing method and the envisaged effects of such a process before the commission. However, Article 29 working party considers Article 20 of the GDPD as focusing merely on the outcomes of profiling than its process[93]. Thus, it proposes to broaden the scope of Article 20 in line with

[89] *Supra*, note 85.
[90] DPD, Art 15, a and b.
[91] *Supra*, note 85
[92] GDPR
[93] *Supra*, note 85

providing greater transparency and control for the data subjects and more responsibility and accountability of data controllers while maintaining a balanced approach to profiling[94].

Cloud computing

By definition, cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction"[95]. Thus, in cloud computing, the data might be subjected to a chain process involving multiple processors and sub-contractors. The processing in cloud computing may also take place in different geographical locations even within the European Economic Area (EEA), thus leading to a confusion regarding applicable data protection laws when disputes arise. More concerning is the transfer of personal and sensitive data outside the borders of the EEA to third countries where there isn't adequate data protection or safeguards for personal data. All these factors culminate in pointing out that cloud computing is an important consideration in any regime that expects to handle data protection and privacy concerns of the data subjects.

From a legal point of view, the generalizability of the DPD provides for determining the responsibility of different players including the data controllers and data processors in a cloud environment. However, as described earlier, when the data controller and the processor is not apparent, there can be issues in terms of accountability for data processing actions.

As opined by the Article 29 Working party, a cloud client wishing to use cloud providers as a first step needs to undertake a thorough risk analysis[96]. For such analysis, the cloud providers are expected to provide all the information necessary to assess the pros and cons of adopting such a service. In relation to health and wellbeing apps, the cloud clients may often be the developers of

---

[94] *Supra*, note 85

[95] Peter Mell and Timothy Grance. *The NIST Definition of Cloud Computing*. 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Visited 12th October 2015]

[96] Article 29 Working Party. *Opinion 05/2012 on Cloud Computing*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Visited 13th October 2015].

such apps as they may decide on adopting cloud services on behalf of the consumers. In other words, the responsibility emanating through the use of cloud services for health and wellbeing apps and its data may also be assigned to the apps developers. Furthermore, the cloud clients have been recognized as responsible for guaranteeing the lawfulness of any cross-border data transfers particularly in relation to cloud computing. In terms of app developers, this would mean that they may have to undertake multiple legal responsibilities when such technologies are used for processing data.

3.7. Contribution to privacy risk by health and wellbeing apps

Through these discussions, it became clear that health and wellbeing apps may collect personal data. In most instances, such data may not give rise to a significant privacy threat on its own. However, as a result of big data techniques and automated processing, even the un-related, un-structured, and raw data collected by health and wellbeing apps may generate new personal and sometimes sensitive data that may infer to a person's health status or lead to profiling of a person. Given that the data subjects might have not consented to processing of new data emerging through big data and profiling, such actions may breach the privacy of the data subjects and may also be considered unlawful.

While it is clear that health and wellbeing apps can lead to privacy issues, the laws that are in place to tackle such issues have become vulnerable. Understandably, it is the fast paced evolution of the technology that has made the laws weak. However, the struggle to balance between market requirements and rights of the data subjects seem to have caused delays in laws catching up with the technology as well.

At present, the DPD provides a generalized approach to tackling the emerging privacy issues in instances such as health and wellbeing apps. These laws however are more or less dependent on identifying the data controllers and the data processors at a particular instance. In an era of cloud computing, the roles of data controller and the data processor may become unclear. Therefore, as far as the current DPD is concerned, accountability and responsibility for privacy and data protection may become difficult to achieve.

In relation to identifying who's responsible for processing data, it may be possible to argue that app developers most often than not may become the data controller. However, the OS, app stores and even the third parties could also act as data controllers in different instances. Nevertheless, the app developers are placed in such a way that they would have the capacity to determine the means of processing even when the data gathered through such apps are made available to third party data processors. Further, when it comes to cloud computing, the app developers would often act as the cloud client and thereby may also become the data controller on behalf of the data subjects. Therefore, these discussions indicate the important role played by app developers as data controllers, especially in the case of health and wellbeing apps.

In terms of privacy risk assessment, this chapter highlights several important themes that need to be focused. One such theme is the appropriate linking between data protection principles and the privacy risk assessment. Second, is the role of consent in terms of privacy risks and third is the question of accountability. At the same time, it is interesting to assess the path taken by the EU in implementing privacy risk assessment given their dilemma to balance between different interests. These themes will form part of the discussion in chapter five.

4. Risk based approach to privacy

This chapter will look into the legal discourse around risk-based approach to privacy. Thus, the chapter will start by presenting an overview of the risk-based approach followed by a discussion on the current and proposed EU laws supporting such an approach. Based on the discussions, this chapter will synthesize the implications of a risk-based approach on privacy risk assessments around health and wellbeing apps.

4.1. Overview of risk-based approach to privacy

From a data protection and privacy perspective, risk-based approach entails assessing the risks pertaining to data processing operations, which would determine the obligations of the data controllers and the processors[97]. This means that in terms of data privacy, as discussed in chapter 2, a risk-based approach should focus on the threat towards privacy and the harm that may be caused as a result. However, the goal of a risk-based approach is to control relevant risks[98] and therefore such approaches should weigh-in the benefits of managing privacy risks before implementing controls to minimize such risks.

Threats to privacy

When it comes to personal data, threats to privacy can manifest at any stage of the information cycle including at the time of collection and disclosure. However, it is a variable entity as the characteristics of the data and the way in which the data is being handled (e.g. degree of anonymisation) would vary from one instance to another. As a result, threats need to be assessed in a contextual manner taking into account the likelihood of the threat and the severity of its harm[99].

---

[97] Centre for Information Policy Leadership. *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*. 2014. https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/A_Risk-based_Approach_to_Privacy_Improving_Effectiveness_in_Practice.pdf [Visited 17th October 2015].
[98] Organisation for Economic Co-operation and Development. *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data*. 2013. http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [Visited 13th November 2015].
[99] GDPR

Within the information lifecycle, there can be different categories of threats. These include unjustifiable or excessive collection of data, use or storage of inaccurate or outdated data, inappropriate use of data, lost or stolen data and unjustifiable or unauthorised access, transfer, sharing or publishing of data[100]. When looking at these threats, it can be deduced that these have been recognized in line with the data protection principles such as legitimate purpose, purpose specification and limitation, data relevancy, data accuracy and limited retention of data, fair processing and accountability. In other words, this alignment complies with the view that risk-based approach should supplement the existing data protection principles and laws.

Harm

Recognizing harm is a complex process. Not only it can be classified as direct and indirect harms, harm could also manifest in variety of ways including monetary, social, mental and physical harm[101]. Some describe harm in terms of tangible and intangible damage[102]. Tangible damage could be physical or economic while intangible damage may include distress caused, reputational harm, apprehension or anxiety, intrusions into private life, discrimination and stigmatisation. While tangible damage may be assessed objectively, intangible damage such as that caused through privacy breaches in health and wellbeing apps may be difficult to assess objectively.

On the other hand, harm may be classified differently as in the case of information based harm such as information inequality, information injustice and restriction of moral autonomy[103]. At times though, harm may not only be confined to an individual as certain types of harm such as loss of confidence and trust on data processing could have societal implications[104].

---

[100] Supra, note 97
[101] Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri. *Review of the European Data Protection Directive*. 2009. https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf [Visited 14th November 2015].
[102] Supra, note 97
[103] Information Technology and Moral Philosophy. Edited by Weckert, J and Hoven, Jvd.London,(Cambridge University Press) 2008, p. 311.
[104] Ibid.

Factoring in the benefits

As described in earlier chapters, privacy is not an absolute right but a right that should be weighed in comparison to other fundamental rights. This means that a risk-based approach should focus on balancing between the benefits and the harms rather than trying to determine only the threats and the harms[105].

However, it is also understood that risks may not be remedied completely. In other words, if benefits sufficiently outweigh the risks, the said actions may be justified. The issue here is to determine and quantify the benefits as it was the case with assessing the harm emanating from various threats.

From an individual perspective, benefits afforded through personal data processing may make a person relinquish personal information with the understanding that the said information would be used within a particular context[106]. The government on the other hand may decide on relinquishing certain privacy rights of individuals, as in the case of law enforcement, on the basis that such information may be usable to the greater good of the society.

These examples highlight the fact that assessment of benefits is also extremely contextual and that individual perceptions regarding their perceived benefits and harms may also play a key role in balancing between the two. Moreover, in a risk assessment process, the need to minimize the subjectivity is also highlighted, both in relation to assessing harm and the benefits afforded through data processing.

4.2. Current and proposed EU laws supporting a risk-based approach to privacy

Within the DPD, the risk-based approach has been endorsed to a certain extent. For instance, under Article 17, implementation of appropriate technical and organizational measures to safe-

[105] *Statement on the role of a risk-based approach in data protection legal frameworks*, *Supra*, note 15
[106] *Supra*, note 103

guard personal data has been made proportionate to the risks represented by the nature of the data to be protected. Similarly, under Article 20, the DPD emphasizes on the need to assess the risks to the rights and freedoms of data subjects before data processing operations. Furthermore, the Article 29 working party views Article 8 of the DPD as a means of endorsing a risk-based approach as it considers special categories of data separately based on the increased risk imparted by such data to the data subjects privacy. While these measures may not explicitly state or support an implementations of a risk-based approach to privacy, to an extent, the value of such an approach was seen by the EU.

Nevertheless, the importance of a risk-based approach was emphasized through the proposed GDPR through specific provisions. For instance, Article 22 of the GDPR adopts a risk-based approach to ensure accountability of the data controllers and Article 30 does the same for ensuring security of processing. In the latter case, the GDPR illustrates its willingness to balance between risks, ensuring security, degree of harm, state of the art and the cost of implementation. In other words, this may also be considered as an instance where the GDPR was trying to use risk-based approach to balance between individual rights (security in this instance), harm, best practices (state of art) and industry interests (the cost).

However, the most notable of the provisions within the GDPR in terms of risk-based approach is arguably the Article 33, which prescribes the use of an impact assessment. Article 33 lays down several instances of data processing operations with specific risks, which will necessitate undertaking of an impact assessment. One component of the impact assessment according to Article 33.3 is an undertaking of a risk assessment as envisaged through this thesis.

Furthermore, the proposal to enforce protection by design as stated in Article 23 of the GDPR could also be viewed as a means of enabling a risk-based approach, which also leads way towards implementing privacy-by-design.

4.3. Implications of a risk-based approach

When looking at the evolution of the GDPR from its introduction in 2011, it is clear that the members of the EU and other stakeholders including the industry were critical of the burdening of data controllers and the producers. However, this was not because the industry was against a risk-based approach but because the GDPR may warrant the application of a disproportionate risk-based approach including an impact assessment across all instances of data processing as against a scalable approach[107].

However, Article 29 working party is of the view that data subjects should be afforded the same degree of protection in accordance with the data protections principles and regulations no matter the degree of risk, nature of the data and the scope of processing[108]. Nevertheless, this does not mean the risk-based approach should make data controllers undertake full-scale risk assessment or impact assessments. In the opinion of the working party, the obligation of the data controllers may vary according to the degree of risk, harm, nature of processing, type of data processed and other considerations[109]. It is in this sense that a risk-based approach would be useful as it will allow clarity in terms of the obligations of the data controller and a more objective assessment of the risks, harms and benefits associated with data processing.

Through this discussion, this thesis also enumerates several themes that need to be considered when it comes to a privacy risk assessment. One such theme is the 'determination of likelihood, threat and level of privacy risks' by factoring in the benefits of any kind of data processing operation. Secondly, the 'scalability' of a privacy risk assessment. Thirdly, the concepts of 'privacy-by-design and privacy-by-default'. These themes will be part of the discussion in the next chapter.

---

[107] *Supra*, note 15
[108] *Supra*, note 15
[109] *Supra*, note 15

5. State of privacy risk assessment approaches

As justified in the legal method, this thesis focused its attention on three PIA approaches, namely; RFID PIA, ICO PIA and the CNIL PIA[110] in order to assess the current state of privacy risk assessments within the EU. While a detailed elaboration of each privacy risk assessment component is beyond the scope of this thesis, several important themes that were enumerated in chapter 3 and 4 of this thesis were used in structuring the rest of the discussion herein.

5.1. Important themes related to current privacy risk assessment approaches

5.1.1. Link between data protection principles and privacy risk assessment

The three PIAs considered for this research have selected either the DPD (e.g. RFID PIA) or the national data protection legislation (e.g. ICO PIA and CNIL PIA) as the starting point for its privacy risk assessment. Furthermore, in the case of RFID PIA, regulators to an extent have distanced themselves from differentiating between data protection and privacy principles[111], leaning more towards the industry requirements than privacy concerns of the data subjects. However, in terms of health and wellbeing apps, such partiality may set a dangerous precedence given the potential of these apps to generate new personal and sometimes sensitive data through big data and profiling techniques.

At the same time, the privacy risks emanating through processing personal data may not only be limited to information privacy but may also extend into various other privacy types. For instance, if the app intends to make use of biometric features in the mobile device, it may be invading into the privacy of the person as described by the ICO[112]. Similarly, an app that makes use of location tracking services of the mobile phone may be considered as invading the persons private space

---

[110] CNIL. Privacy Impact Assessment (PIA) Methodology (How to carry out a PIA). http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf [Visited 15th October 2015].
[111] Sarah Spiekermann. *The RFID PIA – Developed by Industry, Endorsed by Regulators*. In: Privacy impact assessment.Houten,(Springer Science & Business Media) 2011. pp. 323-346.
[112] Information Commissioner's Office. *Privacy Impact Assessment Handbook Version 2.0.* 2009. Cheshire. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Visited 12th October 2015]

through constant monitoring and could well be considered as invading the privacy of personal behaviour[113]. Thus, the scope of the concept privacy around personal and sensitive data seems to be expanding with the introduction of new technologies. Therefore, limiting the basis of privacy risk assessments to the fundamental principles of data protection, or even to information privacy per se, may not prove sufficient.

Thus, as also suggested through literature[114], focusing only on the data protection principles in the form of privacy targets (e.g. RFID PIA), privacy principles (e.g. ICO PIA) or legal controls (e.g. CNIL PIA) during privacy risk assessments may not capture the real privacy risks faced by the users of health and wellbeing apps. From the point of view of the data controllers and the regulators however, concentrating solely on the data protection principles in assessing privacy risks may not only be feasible but may also be cost saving. This would also mean that there is a certain imbalance in catering to the interests of the data subjects and the interests of the industry by the regulators. However, as opined by CJEU[115], the balance between different interests influenced by the DPD should take place at National level pertaining to individual cases. This emphasize on the obligation from the part of the national regulators to implement desirable privacy risk assessments that could balance between different interests.

5.1.2. Consent and privacy risks

Within the three PIAs assessed, consent seems to be a key focus. For instance, in the RFID PIA, consent features in the privacy target "legitimacy of processing personal data". Consent also features in relation to privacy risks such as "invalidation of explicit consent" and "illegitimate data processing" as described in the RFID PIA. Within the ICO PIA, consent features in relation to linking PIA with the data protection principles. It does so by prescribing to ask questions such as "If you are relying on consent to process personal data, how will this be collected and what will

[113] Supra, note 112.
[114] Bennett, Colin. *The accountability approach to privacy and data protection: Assumptions and caveats*. In:Managing privacy through accountability.London,(Palgrave Macmillan) 2012. pp.33-48.
[115] Bodil Lindqvist v. Division of the office of public prosecutor in Jönköping (Case C-101/01), Court of Justice of the European Union, Luxembourg, 6 November 2003.

you do if it is withheld or withdrawn?" The CNIL PIA on the other hand has introduced consent as one of the legal controls. Thus, as expected, it is clear that absence of the data subjects consent has been seen as a threat in almost all privacy risk assessments.

However, the DPD in its present form, does not always bind the data controllers to obtain consent from the data subjects. The reason for this is that consent is only one of several pre-requisites for processing personal data as stated in the Article 7 of the DPD. Given that the other pre-requisites are broadly defined, in practice, data controllers could afford themselves to process personal data without having to obtain consent from the data subjects[116]. Even when the data controller obtains consent once, it does not mean the privacy risks to the data subject would be mitigated as a result. This may be particularly true when it comes to health and wellbeing apps where personal and sensitive data may be processed and sometimes created during the processing.

At the same time, the ICO brings to the forefront an important aspect associated with consent, which is the risks pertaining to vulnerable individuals. In fact, the GDPR highlights the need to consider children as a special category of the population when obtaining consent for data processing[117].

In terms of health and wellbeing apps, another area of concern is its potential use of various device dependent features such as biometrics, geo-location data and various other sensors[118]. Thus, in order to comply with the DPD, the data controllers need to obtain consent from a user each time the app accesses these device features for a different purpose other than for the purpose to which the consent was given[119]. For instance, a health and wellbeing app may use geo-location services to provide the user with information regarding lifestyle activities around his or her loca-

[116] Lee Bygrave. *Data privacy Law: an international perspective*. Oxford (Oxford University Press) 2014.
[117] GDPR, Article 45 on 'Duties'
[118] Van Der Sype, Yung Shin, and Wiem Maalej. *On lawful disclosure of personal user data: What should app developers do?.* In:Requirements Engineering and Law (RELAW), 2014 IEEE 7th International Workshop on. (2014)
[119] Ibid.

tion. This would be a form of behaviour advertising and data controllers would have to obtain consent each time it accesses the geo-location service. In this instance, the DPD may not be evoked as the collected data may not be personal in nature. However, as the app may be providing access to a third party at different locations, it has to comply with the Article 5(3) of the e-Privacy Directive as mentioned earlier in the thesis.

Thus, privacy risk assessment pertaining to health and wellbeing apps have to align itself with both the DPD and the e-Privacy Directive when determining the instances where data controllers need to obtain consent. At the same time, privacy risk assessments cannot consider its user base as homogeneous and assess risks pertaining only to one user group. This means that the users right to consent or not should be respected at a much granular level at least when processing personal and sensitive data within the privacy risk assessments[120]. From the point of view of the data controllers, the thesis recognizes such granularity as a chance to minimize instances requiring consent of the users and therefore to avoid cumbersome obligations for notification as in the case of ICO. From the point of view of the users, such granularity would afford them more control over their personal data although with the downside of being flooded with notifications and requests for consent. For the regulators however, consent may be one legal obligation that could be better utilized in ensuring the privacy rights of the users.

5.1.3. Accountability for the privacy risk assessment

As discussed in chapter 3, accountability in terms of personal data processing is a concern for the data subjects and the regulators alike. In light of this unclearness, there is also an unclearness regarding who should take the responsibility and be accountable towards a privacy risk assessment. As per the definition of a data controller[121], the RFID PIA designates the responsibility of performing the RFID PIA on the RFID application operator who is described as a natural or a legal person who develops, implements, uses or maintains a RFID application[122]. Within the ICO

[120] Opinion 2/2013, *Supra*, note 14
[121] DPD
[122] International Association for Public Transport. *Position on European Commission consultation on "Draft Recommendation on the implementation of privacy, data protection and information security principles in applications*

PIA, carrying out the privacy risk assessment is the responsibility of the organization which plays the role of the data controller. While data controller is also one of the recognized entities responsible for carrying out the privacy risk assessment within the CNIL PIA, it also elaborate on another entity known as the 'product producer', whom would also be responsible for carrying out the assessment in some instances.

In terms of health and wellbeing apps, one could argue that the privacy risk assessment should be carried out by the data controller as per the opinion of the Article 29 working party[123]. However, as described in chapter 3, recognizing the data controller pertaining health and wellbeing apps may not be an easy task especially in the event of mobile apps utilizing cloud computing and big data technologies. Further, the proposed GDPR introduces the term 'producer' to whom the GDPR assigns partly the task of implementing measures that would allow data controllers to meet regulatory requirements[124]. This would mean that according to the GDPR, the producer is not accountable for personal data processing.

However, this thesis is of the view that the 'producer' as introduced by the GDPR, performs the same role as the app developer as discussed earlier. Given the superior contextual and architectural understanding of the app developers regarding the information processes, this thesis believes app developers or producers to be in the best position to undertake a privacy risk assessment. However, as often the case may be, app developers or producers would work to the blue print determined by an organization that desires obtaining information from the data subjects. Thus, the data controller within the ambits of the DPD in this case may not be the app developer.

Given this uncertainty, the thesis perceives the need to implement a methodology towards recognizing not only the data controller and the data processors, but also the entity responsible for performing the privacy risk assessment. From the point of view of the regulators, having such a

---

supported by Radio Frequency Identification (RFID). 2008. http://www.uitp.org/sites/default/files/Position_Papers/ [Visited 2nd November 2015].

[123] *Supra*, note 56

[124] GDPR, Article 23

methodology would ease its regulatory activities. From the point of view of the data controllers, app developers and data processors, recognizing their roles would ease their legal uncertainty and will be better motivated in undertaking a privacy risk assessment.

5.1.4. Scalability

In chapter 4, it was enumerated that a risk-based approach to privacy should ideally be scalable in terms of the size of the organization, amount of data processed and other determinants. However, it was also enumerated that despite the scalability of a risk-based approach, the legal obligations arising from processing personal data as per the data protection principles should remain the same for all.

The RFID PIA in its initial analysis phase provides the privacy risk assessor with the option of determining an applicable PIA, based on processing of personal data. It also considers that not all RFID operators would have to be accountable for all the privacy targets defined. This means that the privacy risk assessment process in RFID PIA, could afford to adjust itself based on the privacy targets it perceives as needing to achieve. However, although the accountability in terms of privacy obligations may be scalable, RFID PIA emphasizes that accountability in terms of data protection obligations should be the same for any organization despite the nature of the data they process[125]. Nevertheless, critiques argue that RFID PIA is not necessarily scalable but instead it is only offering two options of PIAs, which may not necessarily reflect the true nature or the complexity of a given project and its impact on privacy[126].

ICO and the CNIL on the other hand provide more scalability through different mechanisms. For instance, the ICO PIA offers the flexibility of determining the nature of the PIA adopted based on the project size, project goals, vision, actual privacy risks and based on the available re-

[125] European Commission. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. 2011. http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf [Visited 14th October 2015].
[126] Slaughter and May. *ICO publishes new privacy impact assessments code of practice – Briefing*. 2014. https://www.slaughterandmay.com/media/2090383/ico-publishes-new-privacy-impact-assessments-code-of-practice.pdf [Visited 3rd November 2015].

sources. The CNIL on the other hand affords the businesses the option to scale its PIA based on multiple factors including legal and risk-treatment controls. However, the data protection obligations, which CNIL defines as 'primary assets', are non-negotiable and must be complied. Within the GDRP however, there are suggestions to apply less strict data protection regime if apps undertake pseudoanonymisation of personal data[127]. This thesis perceives this as an attempt at scaling the legal obligations of the data controllers.

From the data controllers' point of view, scalability of privacy risk assessments and their obligation to data protection and privacy principles would be highly desirable due to cost and liability reduction. Regulators may also be keen on scaling privacy risk assessments and the relevant legal obligations on the basis that it will promote industry innovation and make markets more attractive for businesses. From the point of view of the users however, scaling of the data controllers obligations towards data protection and privacy principles may be detrimental. Thus, this thesis perceives that if scalability of privacy risk assessments are guided inappropriately by the EU regulations, this research sees the potential of such assessments not living up to its expectations.

5.1.5. Determining likelihood, threat and level of privacy risks

In relation to the RFID PIA, some degree of guidance has been provided with regard to recognizing the privacy risks that may threaten the achievement of privacy targets as defined. In the assessment however, although the RFID PIA states that likelihood of occurrence should be stated in accordance with the 'principle of proportionality' and in 'reasonable terms', it does not elaborate on achieving proportionality or what it intends by 'in reasonable terms'. CNIL also asserts that PIA is a way of prioritizing the risks and treat them in a proportionate manner. The ICO on other hand refers to proportionality at different points. For instance, with regard to PIA, ICO

[127] Article 29 Working Party. *Opinion 05/2014 on Anonymisation Techniques, and annex mobile devices.* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Visited 1st November 2015].

states that such assessments need not be complex or time consuming but should be performed with adequate level of rigor proportionate to the privacy risks arising.
In terms of implementing the core PIA principles, the ICO views that it should be proportionate to the nature of the organization processing the data. This means that ICO has given organizations conducting PIAs the necessary flexibility in using their own expertise, methodologies and industry best practices in assessing risks, its likelihood, threats and degree of harm. In line with this view, this thesis also sees proportionality as an integral part of privacy risk assessments.

When considering the meaning of 'in reasonable terms' as stated within the RFID PIA, it may refer to the nature of the personal data being processed, the purpose of its processing, the industry standards and the professional practices relevant to a privacy-by-design approach[128]. For example, if a data controller for a health and wellbeing app decides to adopt an RFID PIA such as the one developed by Bundesamt für Sicherheit in der Informationstechnik[129], the decision should partly fulfil the requirement for 'in reasonable terms'. In this regard, it is also interesting to note the ECtHR ruling on MS vs Sweden[130], where the Court asserted that even when sensitive data related to a person is transferred without consent to a third party for processing (another public institution in this case), it does not violate the person's right to private life. The justification for this ruling was that the said action was not disproportionate to the legitimate aim pursued and was undertaken with adequate safeguards.

Thus, it is the view of this thesis that the principle of proportionality justified by means of reasonable terms could help data controllers determine the level of risks, its likelihood, threats and harms in an objective manner.

---

[128] *Principles of European contract law and Italian law (Vol. 2).* Edited by Veneziano, A (Kluwer Law International) 2005.
[129] Marie Oetzel, Sarah Spiekermann, Ingrid Grüning, Harald Kelter, Sabine Mull. *Privacy Impact Assessment Guideline for RFID Applications*. Bonn (Bundesamt für Sicherheit in der Informationstechnik) 2011.
[130] MS v Sweden, ECtHR,Strasbourg, 27 August 1997.

5.1.6. Implementation of privacy risk assessments

In relation to implementing privacy risk assessments as a legal obligation, there seems to be little backing until GDPR proposed its implementation. Among the three PIAs analyzed, both ICO and CNIL PIAs are used as legal instruments in assessing the privacy compliance of data controllers. However, none of the PIAs make it mandatory for submitting PIA reports to the regulators although recording of the privacy risk assessment, the decisions taken and various outputs of different risk assessment stages have been recognized as essential when data controllers have to demonstrate their compliance to Courts or to national regulators. At the same time, while almost all PIAs encourage the publication of PIA reports, none has made it mandatory given the sensitive nature of certain aspects of a PIA and the potential burden on the industry.

However, when it comes to health and wellbeing apps, which sometimes process sensitive health data, there may be an argument to publish the PIA reports including the privacy risk assessment process or submit these documents to a regulatory authority.

So far, the arguments against an obligation to publish the PIA report or privacy risk assessment emanated from the fact that industry sees such a mandatory provision as burdensome, costly, introduce bureaucratic processes, and time consuming[131]. Further, others may argue that mandatory reporting would become a mere compliance process than a true effort towards mitigating the privacy risks[132]. Nevertheless, it is argued that a PIA, which elaborates the privacy risk assessment, may provide greater transparency towards handling of personal and sensitive data. This may improve trust and avoid fears of privacy breaches among the general public.

Thus, the thesis perceives the need to impose some degree of legal obligation on the data controllers of health and wellbeing apps in performing and reporting the PIA including privacy risk assessment, at least when such projects handle sensitive personal data. Given the overall under-

[131] David Wright. *Should privacy impact assessments be mandatory?* In: Communications of the ACM. Vol. 54 (2011).
[132] Ibid

standing that privacy risk assessments should be scalable to fit different projects and potential privacy breaches, the thesis also perceives the possibility of scaling reporting requirement as well.

5.1.7. Concept of privacy-by-design and privacy-by-default

Privacy-by-design and privacy-by-default are two concepts that have come into the limelight particularly after its inclusion in the proposed GDPR. According to the RFID PIA, PIA is useful in evaluating the success of privacy-by-design efforts at an early stage of development and product specification. The ICO views PIAs as an integral part of a privacy-by-design approache while the CNIL views PIAs as a way of enabling data controllers to demonstrate that their product do not breach privacy.

In implementing privacy-by-design and privacy-by-default, there are several principles that need to be adhered to[133]. These principles focus on proactively recognizing threats to privacy and remedying the same not only at the time of collection but also throughout the data life cycle in all aspects of a project. Thus, in order to realize privacy-by-design and privacy-by-default, it is vital that a privacy risk assessment is carried out at the very beginning of the project.

When it comes to processing personal data, privacy-by-design concept also shows potential in easing the reporting burden for the industry and information intensiveness for the users[134]. With regard to health and wellbeing apps for instance, the data controller may have to face a reporting burden when working with personal data as they have to obtain informed consent from the users at regular intervals. Such information flooding would also be unattractive from a marketing point of view and may add a considerable transaction costs to the users. However, by adopting privacy-by-design and privacy-by-default, organizations can minimize the amount of personal data that it has to deal with and therefore minimize the reporting burden and information flooding[135].

---

[133] Cavoukian, Ann. *Creation of a Global Privacy Standard*. Ontario. 2006. www.ipc.on.ca/images/Resources/gps.pdf [Visited 3rd November 2015].
[134] Supra, note 129
[135] Supra, note 129

Therefore, this thesis perceives privacy-by-design and privacy-by-default as a means of enhancing business processes along with user experiences while dealing with the privacy risks.

5.2. Synthesis of the current state of privacy risk assessment approaches pertaining to mobile apps

Through this discussion, it was made apparent that current privacy risk assessment approaches are largely compliance driven and are based on the data protection principles laid down within the DPD. These assessments consider consent to be a central component in the privacy risk assessment process although the granularity in its application and sensitivity towards special groups of people remain lacking. Further, lack of accountability is seen as a key factor that can jeopardize the undertaking of privacy risk assessment responsibilities.

It was also clear that current privacy risk assessments incorporate principles of scalability to different degrees. However, the attempt at scaling the data protection and privacy obligations of the data controllers is seen by this thesis as a concern from the part of the data subjects. At the same time, the privacy risk assessment approaches seem to distance itself from the proportionality principle and legitimate expectations of the users in assessing privacy risks.

In terms of carrying out privacy risk assessments, the thesis recognizes a need to motivate the data controllers by implementing legal obligations on reporting such findings. Last but not least, current privacy risk assessment approaches were recognized to be supportive of privacy-by-design and privacy-by-default concepts. However, this thesis understands that the EU legislation still lacks means of motivating data controllers to implement such processes, which would also require clear guidance from the part of the regulators.

Out of the themes discussed in this chapter, it is noticeable that in certain instances data subjects' privacy interests were not upheld sufficiently. Confining privacy risk assessments to mere adherence of data protection principles and the coarse nature of assessing consent requirement are two of these instances. In some instances, as in the case of imparting non-scalable and non-proportionate privacy risk assessments on the data controllers, there is a possibility that it may dampen the market and innovation related interests of the industry. Furthermore, lack of responsibility and accountability from the part of the data controllers towards privacy risk assessment

may also be an instance where the interests of the regulators put to test. These three aspects would be the subject of discussion in the next chapter.

6. Harmonizing interests around health and wellbeing apps

In the previous chapter, several areas were enumerated in which interests of the data subjects were disproportionately treated against the interests of the data controllers and the regulators. It is the view of this thesis that unless these interests can be balanced or harmonized, the harm related to privacy may outweigh the benefits of health and wellbeing apps. Therefore, this chapter will discuss each of these recognized areas in view of harmonizing the different interests under the themes, privacy beyond compliance, proportionality instead of stringency and accountability without borders.

6.1. Privacy beyond compliance

This thesis already recognized that privacy risk assessment ought to be more than a mere compliance check. In terms of PIAs, it was enumerated that the concept of privacy expands with new technologies such as profiling and therefore limiting the concept to the fundamental principles of data protection and information privacy may not uphold the true privacy rights of the users of health and wellbeing apps.

In order to see beyond a compliance check, it is argued that privacy risk assessments need to consider more qualitative requirements such as legality, legitimacy, participation and proportionality[136]. While these requirements are addressed within the DPD to a certain extent, such attempts are recognized as inadequate in the context of the European Convention on Human Rights (ECHR) and the relevant case laws of the European Court of Human Rights (ECtHR)[137].

When it comes to privacy, Article 8 of the ECHR states that "everyone has the right to respect for his private and family life..." and that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society". The value placed on these statements can be illustrated in the case of Z. v.

[136] Privacy impact assessment, *Supra*, note 20
[137] *Supra*, note 20

Finland, where the ECHR opined that the ruling of the National Court and the Court of Appeal to release Z's medical records containing Z's HIV status even after 10 years violates Article 8 of the ECtHR[138]. The basis of this judgement was that such an interference was not warranted in a democratic society and that protection of medical data is fundamental to the person's right to respect for private and family life. However, one may argue that as only States can be sued in ECtHR, it may not be useful to consider its case laws in determining privacy risk assessments to which contributory parties would most likely be private entities. Although this may be partly true, cases such as Oluic v. Croatia[139] illustrate that even when private parties are involved, the State can be held liable, as it is the State, which should implement adequate privacy protection measures on behalf of its citizens in the context of ECHR.

When focusing on the qualitative requirement of 'legality', the ECtHR stated that monitoring by public authorities must be both in accordance with the law and necessary in a democratic society[140]. Thus, in the context of ECHR, the laws under which the monitoring is carried out should be explicitly stated within the law and be sufficiently clear to the individual concerned. From the point of view of health and wellbeing apps, this would mean that various data processing technologies such as profiling, cloud computing, data mining...etc, which may at present do not have sufficient legal basis within the EU, would risk violating the ECHR. This view was upheld in the case Liberty v. United Kingdom[141].

In relation to the qualitative requirement for 'legitimacy', ECtHR in Heinz Huber v. Germany stated that even when the purpose of processing data is legitimate, if the processing is beyond its original purpose, this needs to be consented by the data subject or made legal through other means[142]. While the DPD provides for legitimacy by prescribing to obtain consent[143], it may not motivate privacy risk assessments to see consent as necessary in subsequent processing of the

[138] Z v. Finland (9/1996/627/811), ECtHR,Strasbourg, 25 February 1997
[139] Oluic v. Croatia, ECtHR, Strasbourg, 5 May 2009
[140] COPLAND v. The United Kingdom, ECtHR,Strasbourg, 3 July 2007
[141] Liberty and Others v. United Kingdom, ECtHR,Strasbourg, 1 July 2008.
[142] Heinz Huber v. Germany, CJEU (C524-06),Luxembourg, 16 December 2008
[143] *Supra*, note 125

same data for a different purpose perceived 'legitimate' by the data controller. The opinion of the Courts in Heinz Huber v. Germany also aligns with the call made by this thesis in the previous chapter for a more granular assessment of the instances requiring consent of the data subjects.

When it comes to 'necessity' requirement, ECtHR has observed that it extends beyond the rights of an individual into number of societal aspects such as pluralism, tolerance, broadmindedness, liberty, equality,…etc[144]. However, in the absence of a proper definition for 'necessity' requirement by the ECtHR, the Courts have often adopted a proportionality test in determining the necessity of a given action. For instance, in Luordo v. Italy[145], the ECtHR asserted that although the government interference was legal, the said interference was unnecessary given its disproportionate nature.

Another important aspect of these qualitative parameters is that the priority for the Court is the legality of the said action[146]. If an action is deemed illegal, the Court would not proceed to determine whether the said action adheres with the legitimacy, necessity or proportionality requirements. Thus, in terms of privacy risks assessments pertaining to health and wellbeing apps, it is imperative that data controllers avoid processing of personal data as much as possible, which hasn't been afforded clear legal provisions through National, or EU laws.

In terms of harmonizing different interests, this thesis therefore argues that a privacy risk assessment that is sensitive to the provisions of the ECHR in terms of the said qualitative parameters in addition to the requirements of the DPD would better serve as a tool to capture the privacy risks faced by the data subjects.

6.2. Scalability and proportionality instead of stringency

In chapter 5, scalability was enumerated as one important characteristic in privacy risk assessments. Its importance was largely associated with its potential to ease the burden and the cost of

[144] Refah Partisi (the Welfare Party) v. Turkey, ECtHR, Strasbourg, 13 February 2003.
[145] Luordo v. Italy, ECtHR,Strasbourg, 17 October 2003
[146] P.G. and J.H. v. The United Kingdom, ECtHR,Strasbourg, 25 December 2001.

conducting a one-size-fits-all type of a PIA by a data controller. This would mean that even a small organization would be able to undertake a privacy risk assessment depending on the size of the project and the volume and sensitivity of the data being handled.

Proportionality on the other hand was seen by this thesis as beneficial in relation to assessing the likelihood of a privacy risk, associated threats and the degree of harm. Being a general principle of the EU law[147], proportionality principle is inherent in a series of infinite applications of the law. At the same time, as it is present in most other national laws, it transcends barriers erected between them[148]. These characteristics therefore made this thesis to consider proportionality as a useful approach in harmonizing the different interests and create a generalizable understanding of privacy risk assessment pertaining to health and wellbeing apps.

In this regard, it may be useful to consider the proportionality principle as a rationality test consisting of three components[149]. One of which is the 'suitability test', which refers to the appropriateness of a chosen measure in achieving a proposed aim. Second is the 'necessity test', which aims to assess whether a chosen measure to achieve a proposed goal is the least restrictive in terms of a chosen norm. Third is '*stricto sensu*', where a measure is considered disproportionate even if it is found to be suitable and necessary, if the said measure imposes an excessive burden on the individual. Given this understanding, this thesis argues that the same tests could be used in guiding the data controllers. For example, if regulators impose burdensome measures for assessing privacy risks on health and wellbeing apps, Courts may view the same as *stricto sensu* and thereby rule against its implementation. Similarly, if a data controller for a health and wellbeing app decides to use a method that may not reflect the true nature of the data being processed, the Courts may hold such measures as inappropriate within the meaning of the proportionality principle.

---

[147] Nicholas Emiliou. *The Principle of Proportionality in European Law: A Comparative Study,* Zuidpoolsingel, (Kluwer Law International) 1996.p.115.
[148] Tor-Inge Harbo. *The Function of the Proportionality Principle in EU Law*.In:European Law Journal. Vol. 16(2010). pp. 158–185
[149] Mathias Kumm. *Political Liberalism and the Structure of Rights: On the Place and Limits of the Proportionality Requirement*. In:Law, Rights and Discourse:The Legal Philosophy of Robert Alexy (Hart) 2007.

Thus, scalability and proportionality could guide the data controllers in performing a privacy risk assessment and cater to their interest of innovation by minimizing the harm to the data subjects privacy.

6.3. Accountability beyond borders

In terms of health and wellbeing apps, the role played by cloud computing cannot be undermined. However, conflicts arise as a result of cloud computing being a mode of reducing the direct control of data while the regulators in the EU via the DPD is keen on keeping control of the same data[150]. Thus, cloud computing does pose a significant legal uncertainty in terms of identifying the controller, determining the applicable law, and with regard to transfer of personal data outside of the EU.

As discussed in chapter 3, determining the data controller for a health and wellbeing app is not an easy task. There are many entities such as the app developers, device manufacturers, app deployers and even third party data processors, who may play the role of the data controller at different points. In a complex scenario such as this, utilizing cloud computing would add to the dilemma as cloud computing itself would give rise to an uncertainty in identifying the data controller. From a privacy risk assessment point of view, this would mean that the responsibility and accountability towards carrying out such an assessment might also become unclear.

An inevitable result of using cloud computing is that the data collected through health and wellbeing apps may be transferred across borders to different member states or even to locations outside of the EU. According to the DPD Article 25, personal data cannot be transferred to countries outside of the EU, which do not offer adequate level of protection unless the data subject has given his or her consent unambiguously[151]. From the point of view of cloud technology or the mobile app industry, data portability is a key factor that drives innovation and developments in

[150] Menon, Gowri. *Regulatory Issues in Cloud Computing-An Indian Perspective*. In:Journal of Engineering Computers & Applied Sciences. Vol.2(2013).pp.18-22.
[151] DPD, Article 26

cloud-based technology[152]. Thus, it may be possible that the data controllers would avoid assessing the risks pertaining to a cloud service, which takes over the processing of personal data.

However, it was enumerated in chapter 3 that a data controller who may become a cloud client should conduct a thorough risk assessment in the light of full disclosure from such cloud service providers[153]. In the absence of a regulatory obligation for the data controllers however, it is unlikely that every health and wellbeing app developer or data controller would undertake such an assessment or all cloud service providers would provide clear descriptions as to where the actual data processing takes place.

Apart from these considerations, health and wellbeing app users may themselves use cloud services to store their data away from their own devices. Based on the Article 3 of the DPD, such actions would be considered the 'household exception' and therefore any such data may not be covered by the DPD. The risk here is that any processing that is undertaken on these data by third parties may also not be covered by the DPD[154]. However, if privacy risk assessments are to move beyond a mere compliance check with the DPD, data controllers or the app developers should assess such risks as the data subjects or the app users may not be in a position to foresee the potential harm.

When considering these challenges, it is clear that privacy risks emanating from the cloud may not be remediable completely. At the same time, uncertainty has been created by cloud computing as the existing laws are not necessarily adaptable to the intricacies of cloud computing.

However, this thesis sees an opportunity to minimize this uncertainty by implementing legal obligations on the part of the data controllers or app developers, on accountability towards the data that they collect and process. In fact, the notion of a single accountable entity has been suggested

---

[152] Opinion 05/2012, *Supra*, note 96
[153] *Supra*, note 96
[154] Article 29 Working Party. *Opinion 168 on The Future of Privacy*.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf [Visited 12th October 2015].

in the event of cloud computing or any other technology that introduces multiple data controllers[155]. In this model, privacy of the data subjects escalates through contractual terms between different data controllers and the data processors in the cloud. From the point of view of the data subjects and the regulators, they have to deal with only one entity, which is the initial data controller for the collected data.

Similar to cloud computing, big data and profiling techniques are also seen as essential elements of future innovations around health and wellbeing apps. As discussed in chapter 3, these technologies have the potential to create new information from seemingly harmless data, which may even become new sensitive data. Therefore, this thesis sees big data and profiling as a special category within privacy risk assessments around health and wellbeing apps. However, the challenge as perceived by this thesis is to perform a balanced risk assessment, which not only look into the risks, but also into the benefits of profiling.

In fact, ICO has endorsed this view by indicating that big data projects need to be clear and truthful from the onset about the benefits of such projects not only in terms of organizational benefits but also in terms of individual and societal benefits[156]. However, unless the data controllers or app developers are responsible and accountable, economic benefits of big data and profiling may overwhelm the need for a transparent disclosure of true benefits and its beneficiaries. Thus, even in terms of big data projects and profiling, there is a case to make data controllers or app developers accountable through appropriate legal obligations towards performing a truthful privacy risk assessment from the onset of such projects.

Based on these discussions, this thesis asserts that in a privacy risk assessment, accountability of the data controllers or the app developers or both are fundamental in the pursuit of upholding the user and regulatory interests.

---

[155] Pearson Siani and Andrew Charlesworth. *Accountability as a way forward for privacy protection in the cloud*. In:Cloud computing. Berlin, (Springer Berlin Heidelberg) 2009.pp.131-144.
[156] ICO. *Big Data and Data Protection*. https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf [Visited 14th October 2015].

7. Conclusions and recommendations

This thesis aimed to respond three research questions formed around privacy risk assessment of health and wellbeing apps. Therefore, the conclusions and the recommendations will be made in relation to the areas referred to by the research questions.

7.1. Contribution to privacy risks by mobile health and wellbeing apps

As perceived by this thesis, there are several instances where legal uncertainty may manifest in relation to health and wellbeing apps with privacy implications. These include the inherent difficulty in determining the personal and sensitive nature of the collected data, difficulty in determining the data controller and the data processor, and the potential for the industry to overlook the privacy rights of the app users. The first two instances are largely the result of cloud computing, big data and profiling technologies, which creates a legal uncertainty. The third instance manifests as a result of the enormity and the lucrativeness of the health and wellbeing apps market and due to the app users lack of understanding regarding privacy implications.

One implication of this understanding is that there is an immediate necessity to assign responsibility and make data controllers accountable towards a privacy risk assessment of health and wellbeing apps. In this regard, the thesis recognizes app developers to be in a position to better foresee and identify the potential privacy risks pertaining to such apps. However, the thesis does not see an equivalence between app developers and the ‘producers’ as perceived by the proposed GDPR given that the latter seems merely to perform the role of a data processor. Diluting the responsibility and the accountability of an app developer to a mere data processor may not serve the purpose of protecting the privacy rights as it again would create uncertainty about who the data controller would be. Therefore, this thesis recommends to identify app developers as having similar responsibilities and obligations to that of the data controllers through appropriate legislation.

7.2. The state of privacy risk assessment approaches relevant to mobile apps

In answering this question, the thesis compared three privacy risk assessments embedded within the RFID, CNIL and ICO PIA approaches. Before the comparison, the thesis adopted the stand that risk-based approaches should provide clarity in terms of the obligations of the data controller, provide an objective assessment of the risks, harms and the benefits, and not all privacy risk assessments need to have the same degree of rigor.

Based on this understanding, the thesis was able to deduce the following under several relevant themes.

Link between data protection principles and privacy risk assessments: Introduction of new technologies such as big data and profiling expands the scope of privacy. Therefore, limiting privacy risk assessments to the fundamental principles of data protection and information privacy may not be adequate.

Consent and privacy risks: The data controllers of health and wellbeing apps may have to consider consent in a more granular manner. This would mean that privacy risk assessment have to consider special groups of people such as children as well as the path taken by a particular set of data throughout its lifecycle in assessing the risks. Such a mechanism would enable more control for the data subjects and give more opportunities to minimize the need of non-anonymized data for the data controllers.

The need for accountability: There is a need to implement methodologies not only to recognize the data controller and the data processor, but also to recognize those who are responsible to undertake privacy risk assessment to improve responsibility and accountability. Given the complimentary roles played by the app developer and the potential data controller, the thesis recommends considering both as partly responsible towards the privacy risk assessment.

Scalability: The thesis does not agree with the proposed GDPR in its acceptance of pseudoanonymization carrying less strict data protection regime. The understanding gathered through this

thesis was that scalability of privacy risk assessments while appropriate in most instances; it should not in any way scale the data controllers obligations to data protection and privacy laws.

Likelihood of risk, threats and the degree of harm: The thesis recognized reasonable expectations of the data subjects, proportionality principle and reasonable terms as vital components of privacy risk assessments around health and wellbeing apps and therefore would recommend the same for future privacy risk assessments.

Implementing privacy risk assessments: There is a necessity to impart legal obligations on recording and reporting the outcomes of a privacy risk assessment at least when it comes to apps handling sensitive data. However, given the costs and the expertise necessary in reporting, the thesis recommends such obligations to be scaled in line with the overall scaling of the privacy risk assessment process.

Privacy-by-design and privacy-by-default: These concepts were recognized as a means of motivating the industry to minimize its liabilities and to ease the burden of having to flood the consumers with privacy notices and requests for consent at regular intervals. However, in order to achieve privacy-by-design or privacy-by-default, it is vital that data controllers oblige with the need to perform a privacy risk assessment as the first step.

7.3. Harmonizing the EU laws, industry interests and actual privacy expectations of the users of health and wellbeing apps

In responding to the third research question, the thesis recognized three focus areas under which it was able to make several recommendations.

Privacy beyond compliance: This thesis reiterates the need for privacy risk assessments to be more than a mere compliance check with the DPD. In doing so, adherence with the ECHR and the insights afforded through ECtHR cases were emphasized. The thesis also highlighted the States obligations under the ECHR to implementing legal guidance towards conducting an ap-

propriate privacy risk assessment by the data controllers. Therefore, it is recommended that such guidance ought to be more sensitive towards the qualitative requirements such as legality, legitimacy and proportionality while maintain the compliance requirements with the DPD.

Scalability and proportionality instead of stringency: This thesis enumerated the importance of privacy risk assessments to be scalable in order to motivate the data controllers and to promote innovation. In this regard, the thesis recommends adopting proportionality principle in harmonizing the different interests within the privacy risk assessment and facilitate innovation with minimum harm to data subjects privacy.

Accountability beyond borders: While acknowledging the legal dilemma posed by cloud computing, this thesis recognizes the importance of data portability in terms of innovation and cost effectiveness. Similarly, the benefits afforded to the individual and to the society through big data and profiling technologies were also acknowledged. However, unregulated use of any of these technologies may harm the privacy of health and wellbeing app users and therefore this thesis recommends the adaptation of 'single accountable entity'. Such an entity would better serve in promoting the undertaking of privacy risk assessments and for such assessments to be transparent.

7.4. Final remark

Health and wellbeing apps are set to become an everyday part of life and would require its users to provide more and more data to perform its tasks. While the benefits often outweigh the privacy risks imposed by such apps, there is an immediate requirement to ease the legal uncertainty that could facilitate exploitation of personal and sensitive data in mass scale. A scalable and a transparent privacy risk assessment obligation is seen by this thesis as a way to remedy this situation. However, in order to implement the same, the EU laws (the proposed GDPR) ought to provide guidance on methodologies to identify the relevant data controller among many entities and the obligatory party to the privacy risk assessment. The national regulators on the other hand ought to implement desirable standards fitting to its context for privacy risk assessments that take into account the reasonable expectations of the app users, principles of proportionality, reasonable terms and qualitative parameters of privacy rights.

8. References

EC Directives/Treaties

Charter of Fundamental Rights of the European Union (2000/C 364/01)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive)

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 25 Jan. 2012

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.

List of judgements/decisions

Bernstein ao v. Bester NO AO 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC)

Bodil Lindqvist v. Division of the office of public prosecutor in Jönköping (Case C-101/01), Court of Justice of the European Union, Luxembourg, 6 November 2003.

MS v. Sweden, The European Court of Human Rights, Strasbourg, 27 August 1997.

Refah Partisi (the Welfare Party) v. Turkey, ECtHR, Strasbourg, 13 February 2003.

P.G. and J.H. v. The United Kingdom, ECtHR, Strasbourg, 25 December 2001.

Z v. Finland (9/1996/627/811), ECtHR, Strasbourg, 25 February 1997

CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 48.

Liberty and Others v. United Kingdom, ECtHR, Strasbourg, 1 July 2008.

Heinz Huber v. Germany, CJEU (C524-06), Luxembourg, 16 December 2008

Luordo v. Italy, ECtHR, Strasbourg, 17 October 2003

COPLAND v. The United Kingdom, ECtHR, Strasbourg, 3 July 2007

Oluic v. Croatia, ECtHR, Strasbourg, 5 May 2009

Article 29 Working Party

Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks - 14/EN WP 218*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf [visited 28th September 2015]

Article 29 Working Party. *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation.* Brussels. 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf [Visited 16th October 2015].

Article 29 Working Party. Clarification of the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps - Annex - health data in apps and devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [Visited 12th September 2015].

Article 29 Working Party. *Opinion 02/2013 on apps on smart devices – WP202*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [visited 2nd October 2015].

Article 29 Working Party. *Opinion 03/2013 on purpose limitation*. http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf [Visited 12th October 2015].

Article 29 Working Party. *Opinion 05/2012 on Cloud Computing*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Visited 13th October 2015].

Article 29 Working Party. *Opinion 05/2014 on Anonymisation Techniques, and annex mobile devices.* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Visited 1st November 2015].

Article 29 Working Party. *Opinion 168 on The Future of Privacy*. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf [Visited 12th October 2015].

Other EU official documents

Committee of Ministers. *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*. https://wcd.coe.int/ViewDoc.jsp?id=1710949 [Visited 11th October 2015].

European Commission. *Digital Agenda for Europe*. 2015. http://ec.europa.eu/digital-agenda/en/news/mhealth-green-paper-next-steps [Visited 11th October 2015].

European Commission. *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century*. Brussels, 2012. http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf [Visited 14th October 2015].

European Commission. *Green paper on mobile health ("mHealth")*. Brussels, (European Commission) 2014.

European Commission. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. 2011. http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf [Visited 14th October 2015].

European Data Protection Supervisor. *Opinion 1/2015 on Mobile Health - Reconciling technological innovation with data protection.* Brussels. 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf [Visited 12th September 2015].

Organisation for Economic Co-operation and Development. *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 2013. http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [Visited 13th November 2015].

National guidelines/regulations

CNIL. Privacy Impact Assessment (PIA) Methodology (How to carry out a PIA). http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf [Visited 15th October 2015].

Information Commissioner's Office. *Privacy Impact Assessment Handbook Version 2.0.* 2009. Cheshire. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Visited 12th October 2015]

Books

Bennett, Colin. *The accountability approach to privacy and data protection: Assumptions and caveats*. In:Managing privacy through accountability. London, (Palgrave Macmillan) 2012. pp.33-48.

European Union Agency for Fundamental Rights. *Handbook on European data protection law*. Belgium. 2014. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [Visited 14th October 2015].

Lee Bygrave. *Data privacy Law: an international perspective.* Oxford (Oxford University Press) 2014.

Mathias Kumm. *Political Liberalism and the Structure of Rights: On the Place and Limits of the Proportionality Requirement*. In: Law, Rights and Discourse: The Legal Philosophy of Robert Alexy (Hart) 2007.

Mylonas, Alexios, Marianthi Theoharidou, and Dimitris Gritzalis. *Assessing privacy risks in Android: A user-centric approach*. Geneva, Springer International Publishing, 2014. (Lecture notes in Computer Science Series; 8418/2014)

Nicholas Emiliou. *The Principle of Proportionality in European Law: A Comparative Study*, Zuidpoolsingel, (Kluwer Law International) 1996.p.115.

Pearson Siani and Andrew Charlesworth. *Accountability as a way forward for privacy protection in the cloud*. In:Cloud computing. Berlin, (Springer Berlin Heidelberg) 2009.pp.131-144.

Principles of European contract law and Italian law (Vol. 2). Edited by Veneziano, A (Kluwer Law International) 2005.

Privacy impact assessment. Edited by Wright, David and Paul De, Hert. Houten, (Springer Science & Business Media) 2011.

The Oxford handbook of empirical legal research. Edited by Cane, Peter and Herbert, Kritzer. Oxford, (University Press) 2010.

Wright, David and Paul De, Hert (Ed.) *Privacy impact assessment*. Edited by. Houten, (Springer Science & Business Media) 2011.

Other secondary literature

A Privacy Impact Assessment Framework for data protection and privacy rights. Edited by David Wright, Kush Wadhwa, Paul De Hert and Dariusz Kloza. Seventh Framework Program. http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf [Visited 28th September 2015]

Cavoukian, Ann. *Creation of a Global Privacy Standard*. Ontario. 2006. www.ipc.on.ca/images/Resources/gps.pdf [Visited 3rd November 2015].

Centre for Information Policy Leadership. *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*. 2014. https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/A_Risk-based_Approach_to_Privacy_Improving_Effectiveness_in_Practice.pdf [Visited 17th October 2015].

Crawford Kate and Jason Schultz. Big data and due process: Toward a framework to redress predictive privacy harms. In:*BCL Rev.* 55 (2014). p.93.

David Wright. *Should privacy impact assessments be mandatory?* In: Communications of the ACM. Vol. 54 (2011).

Deloitte center for health solutions. *Connected Health: How digital technology is transforming health and social care*. 2015. http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf [Visited 20th October 2015].

Dennison, Laura...[et al.]. *Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study*. In:Journal of medical Internet research. Vol.15(2013).

Felt, A, Ha, E, Egelman, S, Haney, A, Chin, E and Wagner, D. *Android permissions: user attention, comprehension, and behavior*. In: Proceedings of the 8th Symposium on Usable Privacy and Security. ACM (2012).

Greenaway, Kathleen, Susan Zabolotniuk, and Avner Levin. *Privacy as a Risk Management Challenge for Corporate Practice*. 2012. Ted Rogers School of Management. http://ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf [Visited 11th November 2015].

Hasan, Osman...[et al.]. *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case*. In: 2013 IEEE International Congress on Big data. IEEE (2013)

ICO. *Big Data and Data Protection*. https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf [Visited 14th October 2015].

Information Technology and Moral Philosophy. Edited by Weckert, J and Hoven, Jvd. London, (Cambridge University Press) 2008, p. 311.

International Association for Public Transport. *Position on European Commission consultation on "Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)*. 2008. http://www.uitp.org/sites/default/files/Position_Papers/ [Visited 2nd November 2015].

Kay, Misha, Jonathan, Santos and Marina, Takane. *mHealth – New horizons for health through mobile technologies*. Geneva, World Health Organisation, 2011. (Global Observatory for eHealth series – 3/2011).

Lupton, Deborah. *M-health and health promotion: The digital cyborg and surveillance society*. In: Social Theory & Health. Vol.10 (2012), pp. 229-244.

Marie Oetzel, Sarah Spiekermann, Ingrid Grüning, Harald Kelter, Sabine Mull. *Privacy Impact Assessment Guideline for RFID Applications*. Bonn (Bundesamt für Sicherheit in der Informationstechnik) 2011.

Martin, Hansen...(et al.). *Shaping the Future of Electronic Identity Privacy Requirements*. http://futureid.eu/data/deliverables/year1/Public/FutureID_D22.03_WP22_v1.0_PrivacyRequirements.pdf [Visited 20th October 2015].

Menon, Gowri. *Regulatory Issues in Cloud Computing-An Indian Perspective*. In:Journal of Engineering Computers & Applied Sciences. Vol.2(2013).pp.18-22.

Milošević, Mladen, Michael T. Shrove, and Emil Jovanov. *Applications of smartphones for ubiquitous health monitoring and wellbeing management*. In: *JITA-Journal of Information Technology and Applications (Banja Luka)-APEIRON* 1.1 (2011).

Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri. *Review of the European Data Protection Directive*. 2009. https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf [Visited 14th November 2015].

PA Consulting, *Policy and regulation for innovation in mobile health*. London. 2012. http://www.gsma.com/connectedwomen/wp-content/uploads/2012/04/policyandregulationforinnovationinmobilehealth.pdf [Visited 14th October 2015].

Paintsil, Ebenezer and Lothar, Fritsch. *Towards Legal Privacy Risk Assessment Automation in Social Media*. erschienen im Tagungsband der INFORMATIK 2011. http://www.user.tu-berlin.de/komm/CD/paper/090221.pdf [Visited 17th November 2015].

Peter Mell and Timothy Grance. *The NIST Definition of Cloud Computing*. 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Visited 12th October 2015]

PWC. *Emerging mHealth: Paths for growth*. 2014. https://www.pwc.com/gx/en/healthcare/mhealth/assets/pwc-emerging-mhealth-full.pdf [Visited 12th October 2015]

Sarah Spiekermann. *The RFID PIA – Developed by Industry, Endorsed by Regulators*. In: Privacy impact assessment. Houten, (Springer Science & Business Media) 2011. pp. 323-346

Slaughter and May. *ICO publishes new privacy impact assessments code of practice – Briefing*. 2014. https://www.slaughterandmay.com/media/2090383/ico-publishes-new-privacy-impact-assessments-code-of-practice.pdf [Visited 3rd November 2015].

Terje, Aven. *A semi-quantitative approach to risk analysis, as an alternative to QRAs*. In: Reliability Engineering & System Safety. Vol.93(2008), pp.790 – 797.

Tor-Inge Harbo. *The Function of the Proportionality Principle in EU Law*. In:European Law Journal. Vol. 16(2010). pp. 158–185

Van Der Sype, Yung Shin, and Wiem Maalej. *On lawful disclosure of personal user data: What should app developers do?.* In:Requirements Engineering and Law (RELAW), 2014 IEEE 7th International Workshop on. (2014)

Vanhaecht K, De Witte K, Sermeus W. *The impact of clinical pathways on the organisation of care processes*. Belgium, (KU Leuven) 2007.

Walshe Kieran...[et al.]. *Health systems and policy research in Europe: Horizon 2020.* In: The Lancet . Vol. 382(2013).pp.668-669.

West, DM. *Improving health care through mobile medical devices and sensors*. *Brookings Institution Policy Report*. 2013. http://www.brookings.edu/~/media/research/files/papers/2013/10/22-mobile-medical-devices-west/west_mobile-medical-devices_v06.pdf [Visited 23rd October 2015].