İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

IS GOOGLE AT ODDS WITH THE GDPR? EVALUATION OF GOOGLE'S PERSONAL DATA COLLECTION ON MOBILE OPERATING SYSTEMS IN LIGHT OF THE PRINCIPLES OF DATA MINIMISATION, PURPOSE LIMITATION, AND ACCOUNTABILITY

Ayça ATABEY
117692010

Dr. Öğr. Üyesi Mehmet Bedii KAYA

İSTANBUL
2019

Is Google at Odds with the GDPR? Evaluation of Google's Personal Data Collection on Mobile Operating System in Light of Principles of Data Minimisation, Purpose Limitation and Accountability

Google Avrupa Birliği Genel Veri Koruma Tüzüğü ile Uyumlu mudur? Google'ın Mobil Cihazlarda Topladığı Verinin Amaç ile Sınırlılık ve Veri Minimizasyonu İlkeleri ve Hesap Sorulabilirlik Kapsamında Değerlendirilmesi

Ayça ATABEY
117692010

Tez Danışmanı : **Dr. Öğr. Üyesi Mehmet Bedii KAYA** (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Doç. Dr. Leyla KESER BERBER** (İmza) .....
İstanbul Bilgi Üniversitesi

Dr. Öğr. Üyesi Kadir BAŞ (İmza) .....
Marmara Üniversitesi

Tezin Onaylandığı Tarih : 16 Eylül 2019
Toplam Sayfa Sayısı : .....

Anahtar Kelimeler (Türkçe)
1) Veri Koruması ve Toplanması
2) Mobil Gizlilik
3) Kişiselleştirilmiş Reklamcılık
4) Veri Sahiplerinin Hakları
5) Hesap Sorulabilirlik İlkesi

Anahtar Kelimeler (İngilizce)
1) Data Protection and Collection
2) Mobile Privacy
3) Personalised Advertising
4) Data Subjects' Rights
5) Accountability

TABLE OF CONTENTS

ABBREVIATIONS

CNIL	Commission Nationale de L'informatique et des Libertés
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
Et. al.	Et alia
EU	European Union
FRA	European Union Agency for Fundamental Rights
OECD	Organisation for Economic Cooperation and Development
OS	Mobile Operating Systems
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
UNICEF	United Nations Children's Fund
USA	United Stated of America
Working Party 29	The Article 29 Data Protection Working Party

LIST OF FIGURES

ABSTRACT

The mobile technologies are rapidly advancing; smartphones are becoming increasingly ubiquitous in our lives while Google hoovers up personal data any possible way benefiting from the omnipresence of smartphone platforms. The GDPR with its bedrock principles set out in Article 5 has become a soaring topic globally, creating awareness, and enhancing the status of data protection as a fundamental right. However, the legal implications of Google's data collection through manifold ways create confusion regarding the scope and legality of such data collection. This thesis aims to evaluate personal data collection with a thorough discussion focusing on Google's responsibilities and compliance with the GDPR, more specifically, with the principles of purpose limitation, data minimisation, and accountability, which is then followed by a comprehensive analysis of Google's Privacy Policy and data subjects' rights.

Keywords: Data Protection and Collection, Mobile Privacy and Operating Systems, Personalised Advertising, Data Subjects' Rights, Accountability

ÖZET

Akıllı telefonlar, mobil teknolojilerin gelişmesi ile yaşantımızdaki önemi her geçen gün artırmaktadır. Apple'ın iOS işletim sistemi ile Google'un Android işletim sistemi en yaygın kullanılan mobil işletim sistemleri olarak bu dönüşüme öncülük etmektedir. Google, Kişiselleştirilmiş Reklamcılık iş modeli başta olmak üzere birçok nedenden dolayı dünyanın en yaygın mobil işletim sistemi Android'i kullanarak, cihazlar ile paylaştığımız kişisel verileri toplayabilmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü ile beraber getirilen ilke ve kurallar Google'un veri toplamasının kapsamı, yasallığı ve sonuçları hakkında belirsizlik yaratmaktadır. Bu çalışma ile birlikte Google'un Gizlilik Politikası ve veri toplama faaliyetinin Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ortaya konan ilke ve kuralları ile uyumluluğu analiz edilecektir.

Anahtar Kelimeler: Veri Koruması ve Toplanması, Mobil Gizlilik ve İşletim Sistemleri, Kişiselleştirilmiş Reklamcılık, Veri Sahiplerinin Hakları, Hesap Sorulabilirlik İlkesi

INTRODUCTION

In today's rapidly changing world, smartphones have become increasingly ubiquitous in our daily lives; however, the protections they offer are yet to evolve. The legal notions of privacy and data protection and their intersection with ever-developing technologies have become soaring topics globally. Following the enforcement of "the General Data Protection Regulation"[1] ("GDPR"), a new battlefield was created, where policymakers, mobile operating systems ("OS") and global IT giants such as Google, face legal challenges concerning privacy and data protection rights. The GDPR became the catalyst multiplying the probing questions concerning personal data collection on smartphones and the protection the mobile technologies provide for users' privacy and security, especially for the risks related to installed apps and the information shared with third parties. Article 5 of the GDPR ("Article 5") stipulates principles relating to processing of personal data, such as purpose limitation and data minimisation. Although the EU law was familiar with these concepts from "the Data Protection Directive"[2] ("DPD"), the GDPR introduced accountability, and required the controller to be responsible for and to demonstrate compliance with the principles. These developments affect the scope of the relationship between the rights to privacy and data protection: two interlinked, yet, separate fundamental rights already distinguished under the European Union ("EU") Charter of Fundamental Rights, and put the burden of these rights' implications on the shoulders of data processors and controllers. The gap

[1] EU Regulation 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119/1.

[2] EU Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ 1L 281/31.

created among the essences lying at the heart of these rights, the legal implications of the core principles set out under Article 5, and the lack of guidance on these principles' practical implementation creates confusion for different stakeholders involved in the various components of the smartphone ecosystem, including Google. A clarification is necessary in order to provide the desired protections for the purposes of the general data protection regime, which is possible by providing a better understanding of both technical and legal aspects of personal data collection.

This research presents a different aspect of the complex, yet strong relationship between the legal notions of "data protection" and "privacy," and ever-advancing technologies with a focus on the personal data Google collects on smartphones. To do so, it delves into the personal data collection methods used by Google on two different mobile platforms: Android and iOS, and zooms into the inner workings of the mobile ecosystem to simplify the myriad of technological details underscoring the importance of Google's business model in its personal data collection motives. After identifying the scope of the personal data collected, with or without users' consent, combining first-hand experience and valuing the latest technical research reports, this thesis refers to the essences of data protection to question Google's latest Privacy Policy's compliance with data subjects' rights under the GDPR.

RESEARCH METHODOLOGY

This thesis aims to evaluate the personal data collected by Google on Android and iOS platforms in scope of the GDPR. The data collection methods carried out on these two distinct platforms can be traced back to the different business models of Google and Apple. Regarding the legal implications of Google's personal data collection, although a cross-platform approach is intended, the Android ecosystem is the predominant focal point. The observations provided in this thesis are inclined

to concentrate on Android OS due to the availability of empirical research since Android OS is highly conducive to pursuing such detailed examination; whereas for iOS, there is no comprehensive research due to its closed system.

Technology

Today, it is proven that most of Google's data collection takes place when a data subject is not even using any of its products or services.[3] The amount of data Google collects is noteworthy, especially on Android mobile devices, arguably increased with booming Huawei sales in 2018-19[4], the most popular personal smartphone now used in the world[5]. This thesis focuses on the technology and the GDPR involved in the protection of personal data on smartphones and aims to understand how they overlap to provide the necessary protections to data subjects, by looking into personal data collection methods used by Google on two different mobile platforms: Android[6] and iOS.

This thesis particularly zooms into the inner workings of the mobile ecosystem to simplify the myriad of technological details looking from the perspective of a user

[3] Douglas Schmidt, 'Google Data Collection' (*FTC*, 15 August 2018) <https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0074-d-0018-155525.pdf> accessed 15 October 2018.

[4] Note that this research was conducted before Google's decision regarding Huawei handsets in May 2019. Also, check the latest updates on Huawei and Google relations 'What Does the Google Block Mean for Huawei Phone Owners?' (*Evening Standard*, 2019) <https://www.standard.co.uk/tech/huawei-google-ban-latest-what-does-block-mean-for-phone-users-a4156301.html> accessed 1 June 2019.

[5] 'Gartner Says Global Smartphone Sales Stalled in the Fourth Quarter of 2018' (*Gartner*, 21 February 2019) <https://www.gartner.com/en/newsroom/press-releases/2019-02-21-gartner-says-global-smartphone-sales-stalled-in-the-fourth-quart> accessed 1 May 2019.

[6] "Android is widely recognised as Europe's most popular mobile operating system. To developers, it is over 12m lines of open source code, providing a robust foundation for further development and experimentation. To device makers, it is an industry standard and royalty-free platform, ensuring compatible devices access to a wide ecosystem of apps and services straight out of the box." 'Android in Europe Benefits To Consumers And Business - Prepared For Google' (*Oxera.com*, 2018) <https://www.oxera.com/wp-content/uploads/2018/10/Android-in-Europe-1.pdf> accessed 4 May 2019.

outside of the professional IT industry, setting up Google accounts on four different smartphones, namely, Huawei P Smart 2019, Samsung Galaxy A10 2019, Huawei P20 and iPhone 7 – both Huawei P Smart 2019, Samsung Galaxy A10 2019 (Android OS) mobile devices were factory-reset and the experiments were carried out without inserting a SIM card; whereas for Huawei P20 and iPhone 7 – both devices were observed with a SIM card. However, it should be noted that there is not sufficiently detailed information based on recognised research regarding personal data collection on iOS platforms by either Apple or Google. Nevertheless, data collection performed on iOS platforms is referred to, for the purposes of comparison where necessary, based on the limited information that respective academically recognised reports and researches provide. In addition, although this thesis does not focus on other mobile platforms where Google's services can be used, such as mobile tablets, the analysis and information provided throughout this thesis is relevant for them as well.

In terms of the academic basis of this thesis, below analyses focus on a few landmark research studies, such as the following: First, MIT's research conducted by Yerukhimovich *et al*[7], where privacy-preserving technology available on the two dominant smartphone platforms, namely, Google's Android and Apple's iOS, was evaluated is taken into consideration. Second, research by Binns *et al*[8], which was peer-reviewed and funded by the British Government's Engineering and Physical

[7] Arkady Yerukhimovich, Rebecca Balebako, Anne E. Boustead, Robert K. Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D. Stanley, Jeffrey Stewart, Ari Trachtenberg, and Zev Winkelman, 'Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices' (*RAND Corporation*, 2016) <https://www.rand.org/pubs/research_reports/RR1393.html> accessed 26 February 2019.

[8] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert and Nigel Shadbolt, 'Third Party Tracking in the Mobile Ecosystem' (*ACM, 2018*) <https://arxiv.org/pdf/1804.03603.pdf> accessed 22 February 2019.

Sciences Research Council conducted by Oxford Internet Institute's recent research findings on third-party tracking allowing companies to identify users and track their behaviour across multiple digital services, with specific reference to its use for location services in order to assess how aligned the practices are with the statements in Google's Privacy Policy. Third, the source of arguably the most extensive media influence and academic debate, Schmidt's research[9] on the particular practices of Google's data collection and processing. These texts will be consistently referred to and built upon for the purposes of this thesis. Although much of the information given below and the discussions concerning data collection, such as location data, may be relevant for mobile applications used in other smart devices, such as cars[10], this thesis particularly focuses on mobile applications that run on smartphones, namely, on Android and iOS platforms.

Legal Framework

The evaluation carried out in this thesis is primarily based on the GDPR. However, as data protection and privacy rights are considered as "fundamental rights,"[11] and are thus protected in numerous jurisdictions and constitutions in different countries of the world, as well as in international human rights law, this thesis refers to other

[9] Schmidt (n 3).

[10] 'Google Give Keys of Android Automotive OS to Third Party Mobile App Developers' (*MobileAppDaily*, 2019) <https://www.mobileappdaily.com/google-opens-android-automotive-os-to-third-party-app-developers> accessed 5 May 2019.

[11] This thesis is mainly concerned with data protection and the GDPR, but privacy laws will be referred to where necessary for the discussion in the respective Chapters. "*As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring implementation of the International Covenant on Political and Civil Rights (ICCPR), recognised that there is a need for data protection laws to protect the fundamental right to privacy recognised under Article 17 of the ICCPR (International Covenant on Civil and Political Rights), see more in Office of the High Commissioner of Human Rights ("OHCHR"), 'Adopted and opened for signature, ratification and accession by General Assembly resolution of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49' OHCHR 4 – 98*"
<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 27 February 2019.

legal sources where necessary. The main legal principles to be taken into consideration are purpose limitation, data minimisation, and accountability set out under Article 5 and the interconnected Articles regarding data subject rights of the GDPR focusing on transparency. The additional legal sources include, but are not limited to, "the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981" as amended in 2018, the "ePrivacy Directive" (although it will soon be repealed and replaced by "ePrivacy Regulation")[12], and the relevant information provided by European authorities on "the upcoming ePrivacy Regulation" such as the "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)"[13], and "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR", specifically as regards "the competence, tasks, and powers of data protection authorities" which was adopted on 12 March 2019[14].

[12] "*In accordance with Article 94(2) of the GDPR, all references to Directive 95/46 in the ePrivacy Directive have been replaced with 'Regulation (EU) 2016/679' and references to the 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC' have been replaced with European Data Protection Board (EDPB) as of 12 March 2019*."
<https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 15 March 2019.

[13] The presidency of the Council of the European Union published a revised draft of the proposed ePrivacy Regulation. See more in Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 6467/19 (2019) 054357/EU <https://iapp.org/media/pdf/resource_center/ePR_2-15-19_draft.pdf> accessed 26 February 2019.

[14] EDPB, 'Opinion of the Board (Art. 64): Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (*EDPB*, 12 March 2019) < https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy-directive_en> accessed 26 April 2019.

In addition to these, this thesis will refer to case law and literature reviews that are related for the purposes of this thesis. Opinions of "the Article 29 Data Protection Working Party" ("Working Party 29")[15], the "European Data Protection Board" ("EDPB"), the "European Union Agency for Network and Information Security" ("ENISA"), "European Data Protection Supervisor" ("EDPS"), the "Commission Nationale de L'informatique et des Libertés" ("CNIL"), "the European Union Agency for Fundamental Rights" ("FRA") and other organisations and bodies engaged in the enforcement of data protection rights shall be taken into account. Such opinions shall be challenged by opinions criticising the GDPR's strictness and documents prepared by Google as well as other sources influenced by personal data-driven economy and advertising industry.

TERMINOLOGY USED

For the purposes of this thesis, "apps" and "mobile apps" will refer to the applications installed and used on smartphones. Moreover, the terms "mobile phone", "mobile device" and "smartphone" are used interchangeably.

This thesis majorly employs the terminology used in the GDPR. However, since Google is a US-based entity and vastly use terms like "information", "personally identifiable information" and "personal information" instead of "data" or "personal data", throughout the thesis the terms "information" and "data" are used interchangeably, especially in Chapters where relevant references to FTC decisions or to Google's Privacy Policy are made. In addition, the terms "data subject," "individual," "end user" are used interchangeably with the terms "user" and

[15] As of 25 May 2018, the Article 29 Working Party ceased to exist and is replaced by EDPB. See more in European Commission, 'The Article 29 Working Party Ceased to Exist as of 25 May 2018' (*EC*, 11 June 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492> accessed 27 February 2019.

"smartphone user."

LEGAL QUESTIONS

This thesis aims to evaluate the personal data collected by Google for the purposes of answering the following questions:

1 – To what extent Google's data collection practices on mobile platforms coincide with the requirements prescribed by the principles of data minimisation, purpose limitation and accountability?

2 – Does Google's Privacy Policy undermine data subjects' rights?

3 – Overall, is Google at odds with the GDPR?

In order to answer these questions, this thesis first elaborates on the definition and scope of "personal data" under the GDPR, and further discusses the personal data collected by Google on mobile operating systems. Secondly, a number of data collection methods used by Google are explained to prepare the discussion for the purposes of data collection before delving into the relevant principles. Thirdly, this thesis assesses Google's practices in scope of its latest "Privacy Policy" and the tensions they create with "data subjects' rights," and mainly the notion of "transparency" with a focus on location and activity data collected through Google's products and services on mobile platforms. Lastly, this research concludes by discussing the responsibilities of IT giants such as Google, and underscores the key role they play in enhancing "rights to privacy and data protection" by providing further guidance and clarification to different stakeholders of the mobile ecosystem.

CHAPTER ONE

1. PERSONAL DATA COLLECTED BY GOOGLE

The GDPR tries to balance "being resilient enough to provide individuals clear and tangible protection" and "being flexible enough to allow for the legitimate interests of businesses and fundamental rights of the data subjects."[16] However, this task is challenging because it concerns balancing different rights and interests of distinct parties whose priorities and concerns are different.

As mobile platforms are arguably one of the most frequent places where these two parties interact due to their "always on"[17] nature with a variety of sensors collecting a myriad of data (for example, GPS, digital compass, and humidity), this balancing task is even more challenging in smartphone ecosystems where torrent of personal data is pouring every second.

Even though the GDPR brought considerable attention to data protection laws and undeniably created an invaluable awareness globally, it also left the pioneer of the "personal data-driven economy", Google, to struggle.

There are still some concerns regarding the implementation of the GDPR, one of which is that it requires an understanding of both technical and legal aspects, to at least a certain extent[18] despite the fact that the fundamental notions relating to key

[16] 'Legitimate Interests' (*ICO*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 2 May 2019.
[17] EDPS, 'Guidelines on the Protection of Personal Data in Mobile Devices Used by European Institutions' (2015) 22 <https://edps.europa.eu/sites/edp/files/publication/15-12-17_mobile_devices_en.pdf> accessed 1 May 2019.
[18] ENISA, 'Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR' (2017) 57 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> accessed 15 January 2019.

principles and requirements covered under the GDPR are generally accepted and supported. Corporate entities hold a key role in resolving the way personal data is treated under legal provisions, as well as reconciling with the costs of enforcing the new requirements prescribed by the GDPR to strike a balance between the rights of businesses and data subjects. As part of this balancing act, the GDPR goes to great lengths to define what is and is not personal data.[19]

The purpose of this Chapter is to identify and outline the scope of the personal data collected by Google on mobile operating systems. This Chapter starts with explaining the importance of understanding what constitutes personal data and continues by discussing the scope of "personal data" based on its definition under the GDPR. Lastly, this Chapter concludes by specifying the personal data collected by Google on mobile operating systems, namely, Android and iOS.

1.1. UNDERSTANDING PERSONAL DATA

The GDPR requires entities wishing to deal with "personal data" that pertain to 512 million people residing in Europe to comply with rules prescribed in the GDPR, and hold them accountable for such compliance under Article 5. "Personal data" is a key notion that shapes the "material scope" of the GDPR, as Purtova states

[19] 'What Is Considered Personal Data Under The EU GDPR?' (*GDPR.eu*, 2019) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 6 February 2019; Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 'Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions' (2018) 4 Journal of Cybersecurity 1 <https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056> accessed 3 May 2019.

> *"Only when personal data is processed do the data protection principles, rights and obligations apply, under Article 3(1) DPD and Article 2(1) GDPR."*[20]

Understanding the scope of the "personal data" is important in order to ascertain what exactly is being protected for what purposes. This can help stakeholders internalise the reasons for personal data protection. Moreover, such a thorough understanding could render compliance a "must" for the essence of data protection as a fundamental human right, rather than a "must" to avoid getting caught and facing large fines.

Furthermore, the scope of personal data could be determinant in affecting court decisions.[21] This is because the reasoning employed by the judges would be built upon the scope of the definition recognised by the courts. Therefore, since the definition could affect the outcome of a case, clarifying the scope could equally affect other rights different from data protection, depending on the facts of a case. For many cases concerning data protection, the starting point is the statutory definition of personal data. This task can be distressing, and even make judges "anxious"[22] when interpreting the definition of personal data. Consequently, the understanding of what personal data is and is not, in a general context, is necessary before identifying what data Google collects. This Chapter further discusses the

[20] Nadezhda Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 43 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 15 February 2019.

[21] A perfect example to observe this is "*Secretary of State for the Home Department v TLU* [2018] EWCA Civ 2217.

[22] In Secretary of State for the Home Department v TLU [2018] EWCA Civ 2217; [2018] 4 W.L.R. 101; [2018] 6 WLUK 287 (CA (Civ Div)), Lord Justice Gross stated that Auld LJ in *Durant v Financial Services Authority* [2003] EWCA Civ 1746 had been anxious to establish a narrow meaning for 'personal data'.

legal implications of ever-advancing mobile technologies for the purposes of this thesis.

1.2. DEFINITION

Under EU law, just as under "Council of Europe" ("CoE") law, for the purposes of the GDPR and "Modernised Convention 108 Article 2 (a)"[23],

> *"'Personal data' is information relating to an identified or identifiable natural person. It concerns information about a person whose identity is either manifestly clear, or can be established from additional information."*[24]

As such, pursuant to "Article 4 (1) of the GDPR"[25], which closely follows the DPD[26], "personal data" means:

---

[23] "*The Convention was modernised to be able to better address emerging privacy challenges as a result of the increasing use of new information and communication technologies, recognising the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism*" in CoE, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Treaty Series - No. 223)' (2018) 1 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 14 January 2019.

[24] European Union Agency for Fundamental Rights (FRA), 'Handbook on European Data Protection Law - 2018 Edition' (2018) 83 <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 15 February 2019.

[25] "*The GDPR only applies to personal data processed in one of two ways: (1) the processing of personal data that is done wholly or partly by automated means (or, information in electronic form); and (2) personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (or, written records in a manual filing system)"* in 'What Is Personal Data?' (*ICO*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/> accessed 3 May 2019.

[26] Under the DPD, personal data had a similar, yet more "ambiguous" definition. See Article 2 (a).

> *"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

By personal data, what is meant is the data of "actual" or "potential" relevance to data subjects, whether collected from them or from other data subjects or things.[27]

The Article 4 definition of personal data must be broken down into elements, which are of utmost importance, since they constitute the foundation of personal data and play a great role to help determine and identify whether the data collected by Google on smartphones falls under the scope of these elements. This is important because, only if the data collected on mobile platforms constitute "personal data," then the data collected by Google would be worth being evaluated in light of the Article 5 principles and data subjects' rights for the purposes of this thesis.

Below, the terms referred to in this definition will be further elaborated on:

1 - "**<u>any information</u>**": This element is very inclusive and not limited to any particular format. It includes "objective information", such as an "individual's age" and "subjective information", like "employment evaluations." Since there is no limitation in terms of format, a video taken in an engagement party, audio messages

[27] Nick Couldry and Ulises Mejias, 'Data Colonialism: Rethinking Big Data's Relation to The Contemporary Subject' (2018) 20 Television & New Media 339 <https://journals.sagepub.com/doi/abs/10.1177/1527476418796632?journalCode=tvna> accessed 7 May 2019.

sent via mobile apps, such as WhatsApp or Viber, as well as any numerical, graphical, and photographic data can all potentially contain personal data.

Smartphone users usually process personal data of other people, for example, when taking a photo of someone, checking one's contact lists, or sending or receiving e-mails. All data subjects with any connection to the mobile phone are potentially affected, since data collection agents have tentacles with access to almost all information when the data subject uses its products or services.

Although the exact same data could be "anonymous" when being collected, it could transform into being "personal" data later, as Purtova states "simply by virtue of technological progress."[28] Anonymous data is not covered under the scope of the Article 5. However, for the purposes of this thesis, the anonymous data Google collects will be treated as personal data as well since in smartphone ecosystems not all concepts are set in stone. More specifically, "anonymised" may not necessarily mean, "anonymised" in the literal and practical sense since, as Schmidt contends,

> *"Google has the ability to connect the anonymous data collected through passive means with the personal information of the user."*[29]

A similar example could be photos of others, from which their mood can be determined by facial recognition and emotion software such as Microsoft's mood assessor[30]. In terms of inaccurate information, the information that is inaccurately

[28] Purtova (n 20).
[29] Schmidt (n 3) 4.
[30] Facial recognition has become a heated debate topic; see Raquel Aragon, 'How Should We Regulate Facial-Recognition Technology?' (*IAPP*, 29 January 2019) <https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/> accessed 1 April 2019.

attributed to a specific individual be it factually incorrect or information that in reality is related to another individual is nevertheless considered "personal data" as it "relates" to that specific data subject.[31] If data are inaccurate to the point that no data subject can be identified, then the information does not constitute personal data under the GDPR.

2 - "**relating to**": This element is important as it relates to the content of the data, which could be regarded as "personal data" that "relate to" a data subject who can be identified ("identifiable"). Information that identifies a data subject, even without a specific name attached to it, could constitute "personal data," if it is being collected to learn or form an opinion about that data subject, or if this information collection (processing) will have an impact on that person.

Records consisting of explicit information that "relates to" a distinct individual are interpreted as associated with that individual, examples of which are "criminal record"[32] or "medical history." Similarly, other types of records that comprise of an individual's activity and movement can also be considered as such. Put differently, any type of data that is linked with an identifiable individual is considered as personal data. For example, an application, which allows students to keep their schedules (courses and exam dates) and deadlines in one place, can involve personal

[31] GDPR.eu (n 19).

[32] "*It is important to note that the concept of "Sensitive Personal Data" in the GDPR leaves out the category of actual or alleged criminal offences and criminal convictions—data in those categories are addressed separately. This was also the position under the Directive. However, Member States may create additional categories of Sensitive Personal Data, and many Member States have historically opted to treat these data as Sensitive Personal Data*"; See more in Tim Hickman and Detlev Gabel, 'Chapter 5: Key Definitions – Unlocking The EU General Data Protection Regulation' (*White & Case*, 5 April 2019) <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation> accessed 1 May 2019.

information[33], insofar as this app reveals information relating to the student.[34]

Another example could be the data that are used for learning or making decisions about a data subject are personal data as well. However, the collected information should 'relate to the identifiable individual' to constitute and be recognised as 'personal data'. In other words, such data requires being more than merely identifying an individual, it must relate in "some way" to the user.

Information that, when processed, could have an impact on an individual, even without an intention to do so, is considered to be personal data. For example, Uber tracks all of its drivers, so that it can find the nearest available car to assign to an Uber request. However, this data could also be used to monitor whether Uber drivers follow the rules of the road and to measure their productivity rate. This processing of the data relates to the individuals in some way; therefore, it should be subject to data protection rules.[35]

Although currently embedded into Google's other services, another example for such use can be "Google Now", which is Google's news and updates platform. The application acquired location-based data from the mobile phone itself, without the user's explicit permission to acquire that very information, to be able to provide personalised and customised latest news and updates to the user. Although the data collected is told to be merely to provide a better service, nonetheless the user is not

[33] This example is inspired and originated from Karolina Baras, Luisa Soares, Carla Vale Lucas, Filipa Oliviera, Norberto Pinto and Regina Barros, 'Supporting Students' Mental Health and Academic Success Through Mobile App and IoT' (2018) 9(1) International Journal of E-Health and Medical Communications <https://www.researchgate.net/publication/320895755_Supporting_Students'_Mental_Health_and_Academic_Success_Through_Mobile_App_and_IoT> accessed 6 May 2019.
[34] GDPR.eu (n 19). Another example is a child's drawing of their family scenario: See ibid. *"The events from the student's calendar and his or her mood indicators, the application sends notifications accordingly."*
[35] EDPB (n 14).

consulted in giving that permission.

Sometimes, data can address an identifiable data subject and still not be classified as personal data about that data subject. Such a situation can occur when the data does not really relate to the data subject in question. Additionally, inaccurate information can be recognised as being "personal data" if it "relates to" an "identifiable" data subject. This may be the case in instances of giving nicknames or fake names, for example, when creating an account on an app or a website.

Therefore, understanding what the term 'relate to' involves is important, as it raises an evaluation that is contextual. In order to establish "the status" or "category" of information as a type of personal data, it needs to be clarified primarily if this information relates to an individual, before evaluating identifiability at all. Information "relating to" an actual individual could be understood in a wide context or not, much like "identifiability". This calls for an analysis of the type and extent of the information in relation to that individual, and the specific conditions under which this relationship applies.

There are no guidelines provided by the DPD or the GDPR on how to interpret "relating to" in a general context. The Recitals that outline and clarify even the personal data definition are "non-binding," in that EU Member States are not required to implement them as part of their national practices. As such, it is not yet clear whether the option of a regulation being imposed as a legislative instrument will lead to the personal data definition of the GDPR to be consistently applied throughout EU member states.[36]

3 - "**identified or identifiable**": Simply put, whenever one individual can be differentiated from other individuals, that person who can make the differentiation

[36] Purtova (n 20) 40-81.

can be considered to be identifying that data subject. Put differently, any data subject who can be distinguished from others should considered being identifiable.

Direct identification involves direct identifiers that can be used not only in the identification of individuals, but can also have an impact on the manner in which these data subjects are treated. Similarly, indirect identification is also considered a crucial component involved in defining what constitutes personal data. In this golden age of data association, data "de-anonymization" and data interpretation with the extensive powers of artificial intelligence, concerns arise regarding "what types of data" will be treated as "personal data", since what becomes part of that definition will open the way for individuals to be uniquely identifiable and identified.

To decide if an individual is identifiable, a controller, processor or another individual dealing with personal data who is "processing" personal data[37] must take into consideration the reasonable ways that are likely to be used to "directly or indirectly identify" the data subject like "singling out", deeming it possible to treat one person in a different way from another for the purposes of Recital 26 of the GDPR.

"Recital 26 of the GDPR"[38] elaborates on the scope of the definition of personal

[37] Such processing should fall under the scope of Article 4 (2) of the GDPR, which states as follows: *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*

[38] See Recital 26 of the GDPR, which provides as follows: *"The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data, which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by*

data, providing very useful details in terms of implementation. As Purtova[39] re-affirms, Schwartz and Solove highlight, Recital 26 GDPR shapes the GDPR notion of personal data suit for "a tailored, context-specific analysis for deciding whether or not personal data is present."[40]

Calling someone by his or her name[41] is the most common way of identifying that person, but it is often context-dependent. There are millions of people named Robert in the world, but when the name "Robert" is said, generally the point is to catch the attention of the person being faced. By adding another data point to a data subject's name, which in this case is proximity, enough information is acquired to identify one specific individual. These data points are identifiers.

Similarly, going back to the GDPR's definition, it could be seen that, in the definition, there are different types of identifiers: "a name, an identification number, location data, and an online identifier." Biometric data[42] is also very important to

---

another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

[39] Purtova (n 20) 44.

[40] The scope of the personal information is criticised comprehensively in Paul Schwartz and Daniel Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102 California Law Review 9.

[41] See Paragraph 24 of the Opinion of Advocate General Tizzano in the Lindqvist case (*Bodil Lindqvist v Aklagarkammaren i Jonkoping* – Case Commissioner-101/01 – European Court of Justice) delivered on 19 September 2002. See 'The Matter Ofpolyðore International. Inc. Case No. 9327' (*FTC*, 24 December 2008) <https://www.ftc.gov/sites/default/files/documents/cases/2009/01/090114variousarticles.pdf> accessed 15 March 2019.

[42] Kartikay Mehrotra, 'Google Aims at Privacy Law after Facebook Lobbying Failed' (*Bloomberg*, 24 April 2018) <https://www.bloomberg.com/news/articles/2018-04-24/google-takes-aim-at-privacy-law-after-facebook-lobbying-failed> accessed 6 May 2019.

point out since it is highly relevant in mobile ecosystems[43], such as data that includes device fingerprints or face recognition[44], which can also work as identifiers.

Although most of these can be seen clear enough and are pretty much straightforward, online identifiers could be more complicated. To shed some light, "Recital 30 of the GDPR" gives numerous examples that are highly related to the smartphone ecosystem; these include online identifiers[45] and location data, which are prescribed by the GDPR to be treated as personal and must be protected as such. "Recital 30" further clarifies "Article 4 (1)"[46] by providing details that are relevant for mobile ecosystem, and therefore, for the purposes of this thesis.

These examples include IP addresses, cookie identifiers, and other identifiers, which refer to information that is related to an individual's tools, apps, or devices, such as their Android phone or iPhone. This is not an exhaustive list, and 'any information' that could identify a specific device is recognised as an 'identifier'.[47]

---

[43] See *Rivera v Google, Inc*., Case No. 1:16-cv-02714 (N.D. Ill. Dec. 29, 2018); Sam Rutherford and Tegan Jones, 'Google Has Lawsuit in Illinois over Facial Recognition Scanning in Google Photos Dismissed' (*Gizmodo Australia*, 2019) <https://www.gizmodo.com.au/2019/01/google-has-lawsuit-in-illinois-over-facial-recognition-scanning-in-google-photos-dismissed/> accessed 4 May 2019.

[44] Laurie Sullivan, 'Watching Ads Verified by Facial Recognition Earns Moviegoers Free Ticket' (*MediaPost*, 23 April 2019) <https://www.mediapost.com/publications/article/334864/watching-ads-verified-by-facial-recognition-earns.html> accessed 3 May 2019.

[45] 'Guide to The General Data Protection Regulation (GDPR)' (*ICO*, 2018) 9-10 <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> accessed 2 May 2019.

[46] See Recital 30 of the GDPR, which clarifies Article 4(1) and further provides as follows: *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

[47] Els J Kindt, *Privacy and Data Protection Issues of Biometric Applications* (Springer 2013).

4 - "**natural person**": By using "natural person," the GDPR is saying that data about companies or organisations that are considered as "*legal persona*" are not personal data. Also, this element delimits the scope to individuals who are alive. Data related to the deceased are not considered personal data as Recital 27 of the GDPR clarifies[48].

There are also special categories of data, namely "sensitive data"[49], provided in "Article 6 of the Modernised Convention 108" and "Article 9 of the GDPR." The processing of such data requires enhanced protection since it could constitute a threat to individuals, menacing data subjects' rights and their protection.[50]

Making this distinction is significant: some personal data categories are often differentiated according to whether they are sensitive, or whether they are a special category of data that needs further protection when having undergone processing. The latter requires safeguards of a "broader extent, which involve limiting the permitted grounds for processing the data."[51] Concerning "health data," prior to the enactment of the GDPR, data relating to an individual's health condition was

[48] 'Answer to Question No E-007611/17' (*Europarl,* 2018) <http://www.europarl.europa.eu/doceo/document/E-8-2017-007611-ASW_EN.html> accessed 5 May 2019.

[49] See Privacy International's report for further information regarding sensitive data in a global context; Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (2018) 26 <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> accessed 2 January 2019. See also Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, Opinion of Advocate General Kokott.

[50] See Ioulia Konstantinou, Paul Quinn and Paul De Hert, 'Cloud Deliverable 3.1: Overview of applicable legal framework and general legal requirements' (2016) LSTS – Vrije Universiteit Brussel <https://cris.vub.be/files/28383754/D3.1_SeCloud.pdf> accessed 31 March 2019.

[51] European Court of Human Rights ("ECHR"), 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (2018) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 1 March 2019.

considered as "personal data concerning health." For example in *Bodil Lindqvist*[52], a case concerning the online reference to people by their information, such as their names or by other means including their contact details or information on their hobbies.

The Court of Justice of the European Union ("CJEU") stated as follows, regarding a reference made on an internet page grounding their statement on former DPD, Article 8 (1)[53]:

> *"Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health."*

A definition of "sensitive personal data" is not found in most countries' statutory laws; however, they do provide a list of what can be considered as such, or they outline a list of "special categories of personal data."[54] Although it might not be directly relevant for the purposes of this thesis, an interesting point worth mentioning concerns criminal offences, there is not a widely accepted "general approach" regarding such data; accordingly, different countries have different rules

[52] Case C-101/01 *Bodil Lindqvist* [2003] CJEU para 51 <http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30d5f6e5241847894902b867dc13431149fa.e34KaxiLc3qMb40Rch0SaxuNbxr0?doclang=EN&text=&pageIndex=0&docid=48382&cid=21701> accessed 20 February 2019.
[53] Now under Article 9 (1) of the GDPR.
[54] Privacy International (n 49) 26; Hickman and Gabel (n 32).

whether to classify it as "sensitive" or not.[55] This shows that countries actually reflect their legal culture and perception of personal data into their laws.[56] Understanding this point is important to observe different approaches and could help stakeholders understand why some countries find the GDPR and EU data protection laws too rigid.[57]

Commonly, data categories that are recognised as "sensitive" can be associated with discriminatory acts tackled in constitutional measures and human rights

[55] See for definition and the scope of sensitive data see "*ICO v Colenso-Dunne* [2015] UKUT 471 *(AAC) this case confirmed that, under English law, information relating to actual or alleged criminal offences, or criminal convictions, is not 'less sensitive' merely because the category is not listed as Sensitive Personal Data in the Directive. Another example is in Denmark, information relating to actual or alleged criminal offences or criminal convictions, is treated as semi-sensitive data. These data are subject to some, but not all, of the protections afforded to Sensitive Personal Data.*"

[56] For a comparison of European and American approaches to data protection and privacy, see Kimberly Houser and Gregory Voss, 'Can Facebook and Google Survive the GDPR?' (*Oxford Law Faculty*, 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr> accessed 3 May 2019. "*The American ideology behind data privacy is the balancing of an entity's ability to monetize data that it collects (thus encouraging innovation) with a user's expectation of privacy (with those expectations apparently being quite low in the U.S.). In the EU, the focus is on protecting a users' privacy. A great example of this dichotomy is the Google Spain case. A Spanish citizen sought to have certain information removed from a Google search as permitted under EU law. Google objected to this in court. On the one hand was freedom of speech (paramount in the U.S.) and the public right to know asserted by Google, and on the other, the European's right to privacy and to be forgotten argued by the European plaintiff. The European Court of Justice ruled that the balancing of interests tipped in favour of privacy for the Spaniard*."

[57] See Noam Kolt, 'Return On Data' (2019) 38 Yale Law & Policy Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362880> accessed 7 May 2019; Andrea Matwyshyn and Sinan Aral, 'What The EU's GDPR Rules Mean for U.S. Consumers' (*Knowledge@Wharton*, 2018) <https://knowledge.wharton.upenn.edu/article/how-the-gdpr-rules-will-impact-data-protection/> accessed 6 May 2019. See also Matilde Ratti, 'Personal-Data and Consumer Protection: What Do They Have in Common?' in Bakhoum et al., *Personal Data in Competition, Consumer Protection, and Intellectual Property Law* (Springer 2018) 377-393.

mechanisms, promoting the "right to non-discrimination."[58]

The GDPR does not provide an exhaustive list stating what is considered sensitive personal data. Other categories of data that can be related must also be taken into account, such as data regarding children. Although there is, a great potential of the addition of different categories of data that call for further protection is considered resulting from the variable points of sensitivity on a national scale. An example from of a locally meaningful context could be the treatment of "caste information" in India as "sensitive personal data."[59] Nevertheless, "data related to the types of information such as information revealing the ethnicity, religion, political stance, biometric[60] and genetic data[61] as well as health data are generally recognised as constituting sensitive personal data."[62]

Google states that it does not process sensitive data; however, recently[63], new evidence was filed in Ireland, Poland, and the UK, in January 2019 with the national authorities of the respective countries revealing how Google as well as other ad auction companies unlawfully profile Internet users' religious beliefs, ethnicity,

[58] UN Committee on Economic, Social and Cultural Rights ("CESCR"), 'General comment No. 20: Non-discrimination in economic, social and cultural rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights) E/C.12/GC/20' (2009) <http://www.refworld.org/docid/4a60961f2.html> accessed 27 April 2019. "*As a scarce example, there are jurisdictions like Colombia where provisions on sensitive personal data specifies data that has an effect on individuals' privacy or the undue use of which can lead to the discrimination of individuals (Article 5 of the Law 1581 of 2012 of Colombia).*"

[59] B.N. Srikrishna, Aruna Sundararajan, Ajay Bhushan Pandey, Ajay Kumar, Rajat Moona, Gulshan Rai, Rishikesha Krishnan, Arghya Sengupta and Rama Vedashree, 'White Paper of the Committee of Experts on a Data Protection Framework for India' (2018) (4)3 Ministry of Electronics and Information Technology 43 <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_in dia_18122017_final_v2.1.pdf> accessed 20 February 2019.

[60] See Article (4) (14) of the GDPR.

[61] See Article (4) (13) of the GDPR.

[62] Privacy International (n 49) 26.

[63] Johnny Ryan, 'Update On GDPR Complaint (RTB Ad Auctions)' (*Brave*, 28 January 2019) <https://brave.com/update-rtb-ad-auction-gdpr> accessed 14 February 2019.

diseases, disabilities, and sexual orientation.[64] It is safe to assume that, the unstoppable benefits of a data-driven economy, the resulting data flows and technological advancement making the world "limitless," hopefully the double-standardized implementation of the relevant nationalized data protection will come to an end. This will potentially contribute to combating discrimination and profiling in respect of the essences of the rights of data protection and privacy.

Although some of the information given in this thesis does not directly concern or relate to EU citizens, if one truly believes data protection to be a fundamental human right, it seems hypocritical to treat EU citizens' data along with data collected globally from other countries in the world, where the rule of law is questionable. This context is believed to contribute to a thorough understanding of the scope of "personal data," and can encourage and promote contemplation regarding data protection rules in the world, while possibly urging to find a middle ground with other countries, where the balance of interests and rights will be of paramount importance.

1.2.1. What are the 'identifiers' and related factors?

The combination of a piece of data with another data can also enable identifying an individual. The Regulation does not provide any definitive list giving further information on what is or is not personal data. Therefore, understanding the definition given under the Article 4 (1) is of utmost importance, since only its interpretation can shed light into what constitutes personal data.

As mentioned above, personal data means any information relating to a data subject, or in other words, any information that is clearly about a particular person. At first

[64] See for example 'Request for an Assessment Notice/Invitation to Issue Good Practice Guidance Re "Behavioural Advertising"' (*ICO*, 2019) <https://brave.com/ICO-Complaint-.pdf> accessed 15 May 2019.

glance, this definition may be considered as too broad and vague. However, certainly after the DPD, Article 4 (1) of the GDPR is what elaborates this definition, and clarifies it to a certain extent, albeit not giving any specific list explaining what falls under the scope of this definition and what does not.

In addition to the examples given above, in certain circumstances, someone's IP address, eye colour, vocation, social status, or political views may be considered as personal data. "Personal data" should be considered in the context in which data collection is carried out, since one piece of data, carrying a specific information might not individuate a person, while it can be relevant when combined with other data collected.

For example, "collecting information on users who download products from websites (reached on browsers including Chrome)"[65] might ask them to state their age range, whether they are students or more commonly, and their country of origin. It could be contended that none of these does fall under the GDPR's scope of personal data, since many people have the same age, occupation, or origin. Similarly, if a data subject is asked which university he/she studies at, the name of the university cannot be used to identify an individual (unless there is only one student at the university).

This is a hypothetical example. However, in real life, knowing that someone is a student at "X" university does not really help identify someone. In that case, the data would need to be combined with more information, such as the maiden name. A data subject's name cannot always be considered as personal data, however, in its combination with other data, and then the name will have a part in individuating

[65] ENISA (n 18).

that person[66].

1.2.2. Pseudonymisation & anonymisation

The new thresholds are high and rules are strict about the purposes for which data may be used. When organisations such as Google collect names and addresses in order to open an account for users to use its products/services or credit card details to process payments, Google is prohibited from putting the data in question to any other use. How about collecting data, but having it be 'pretended' and not real[67]?

The GDPR allows this way of veiling the collected personal data. However, the GDPR comes with an escape hatch. This is pseudonymisation, describing, "*the processing of personal data in a manner that the data can no longer be linked to a specific data subject without the use of additional information*" under Article 4 (5)[68] of the GDPR.

This means replacing "identifying information," such as names, dates of birth, payment details, or addresses, with data that look the same, but do not reveal details about a real person.

Pseudonymisation is utilized especially for data collection performed for statistical purposes, which can be an escape hatch that helps entities not to fall foul of the

[66] 'What Are Identifiers and Related Factors?' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/> accessed 15 February 2019.
[67] 'Pseudo' (*Cambridge Dictionary*) <http://dictionary.cambridge.org/dictionary/english/pseudo> accessed 1 January 2019.
[68] As defined in Article 4(5): *"means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".*

GDPR.[69] Also, to conclude whether a natural person is identifiable, all reasonable means that can be used, such as singling out, to directly or indirectly identify the natural person should be taken into account pursuant to Recital 26.[70]

1.2.3. Through such processes, can "personal data" become "non-personal data"?

Metaphorically speaking, pseudonymisation is a "mask"[71], a "veil" protecting the data, or a lock, and its key enables "re-identification of data subjects," which should "be kept separate and secure"[72]. However, does utilising the measure of the pseudonymisation liberate the personal data collected? In other terms, if personal data is pseudonymised or, encrypted, can such processing transform personal data to non-personal data? Does it free the data from being "personal," so to speak? This question is often contemplated. The answer is *no*. Therefore, it can be concluded that data that have "undergone a pseudonymisation process remain personal data."[73] "Pseudonymised data" is not treated separately nor is un-alienated from the personal data concept, and is therefore not excluded from the general definition of "personal data" under EU law.[74] However, "it does remove the ability for the data to identify a person."[75] In addition, encryption by itself does not transform personal

[69] 'Pseudonymisation Is Helping Firms Comply with A New EU Privacy Law' (*The Economist*, 5 April 2018) <https://www.economist.com/science-and-technology/2018/04/05/pseudonymisation-is-helping-firms-comply-with-a-new-eu-privacy-law> accessed 15 November 2018.
[70] ENISA, 'Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation' (2018) 4 <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions/at_download/fullReport> accessed 15 January 2019.
[71] 'Data Masking: Anonymisation or Pseudonymisation?' (*GDPR Report*, 7 November 2017) <https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/> accessed 15 March 2019.
[72] ICO (n 25).
[73] ibid.
[74] GDPR.eu (n 19).
[75] Josh Gresham, 'Is Encrypted Data Personal Data under the GDPR?' (*IAPP*, 6 March 2019) <https://iapp.org/news/a/is-encrypted-data-personal-data-under-the-gdpr/> accessed 15 April 2019.

data to non-personal data, it just puts a mask on it, and the data behind the mask remains the same.

On the other hand, clearly distinct from "pseudonymised data," the principles and rules of data protection do not apply to anonymised data. Anonymization refers to the process by which the data can no longer relate to an identified or identifiable individual, in other words, the type of data is exactly opposite of personal data.

As pseudonymised data cannot be used in order to identify a person, the organisation using the technical measure to pseudonymise the personal data can be considered to have genuinely respected the essence of data protection right and have taken reasonable steps for the purposes of data subjects' protection. Hence, as stated in ENISA's report such organisations are "*often afforded some regulation leniency, particularly, with regards to data breach notification requirements."* [76] The report further elaborates that such flexibility is offered bearing in mind the reduced risk that data subjects' are being expected to face and the organisation's efforts in taking the reasonable step of using the technical measure of pseudonymisation in breach cases. This is because, despite the breach, the collected and pseudonymised data cannot be used to identify any specific individual.[77]

Through technologies that "encrypt the data or make it pseudonymised"[78], businesses could meet the requirements for conforming with prescribed responsibilities, achieving an enhanced coping with potential threats despite the fact that security risks still do not vanish. Although data that is pseudonymised is less likely to result in risk or harm for the data subject, it is proven that with the ever-

[76] ENISA (n 70).
[77] ibid.
[78] ibid.

advancing mobile technologies security remains to be a concern.[79]

In today's world, now is the pivotal time for increasingly generated personal data, in other words, today more personal data exists than ever existed before. The data that was not considered as "personal" such as IP address now is. The scope has expanded more than ever before in parallel with the increase in the "personal data" itself. This is why GDPR left no room for data processors to hide behind discrepancies under a definition. It is significant to note that the GDPR's personal data concept sheds light on the definition by providing more information than the DPD, which is seen to be encapsulating more than the American definition of personally identifying information ("PII").[80]

In addition, it is significant to note that notwithstanding of "the intrinsic nature", or in other words, "type" of the data and the method through which it is being collected, when data that relate to one another or that are collected together, these pieces of information could be used, in combination, to narrow down the number of individuals to such an extent that, in many instances, the individual's identity could be practically found.

1.2.4. Data relating to other data?

Looking from a wider perspective, what provides greater wisdom to the definition and the elements of the definition of personal data, such as being 'identifiable', is Aristotle's[81] famous quote:

---

[79] ibid.
[80] '2 CFR § 200.79 - Personally Identifiable Information (PII)' (*Cornell Law School Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/2/200.79> accessed 15 March 2019.
[81] For a discussion of data protection, data collection, use value, and exchange value notions (personal data), see Giovanni Comandé, 'Opinions · The Rotting Meat Error: From Galileo to Aristotle in Data Mining? (2018) 4 European Data Protection Law Review

"The whole is more than the sum of its parts."

This quote explains how Google's data collection – despite being anonymised[82] – can be utilized to identify a data subject. In fact, Google's Privacy Policy slightly implies it if the user can read between the lines. For a comparison of Google's May 2018 Privacy Policy and January 2019 (following the new features introduced in May 2019); see Figures 7.9 and 7.10 in Chapter 7. Excerpts shown in the left boxes imply and for a user who has some background information, in fact, arguably "openly" say that "Google may associate data from its services and tools with a smartphone user's personal information" as demonstrated in Schmidt's research. Google's Privacy Policy will be further discussed and evaluated in detail in Chapter 7.

1.3. RELEVANCE IN THE MOBILE ECOSYSTEM

In the framework of the GDPR, the definition and scope of "personal data" is vital for the purposes of this thesis, and the mobile ecosystem presents an overwhelming dominance wherein this data is gathered. It is precisely mobile OSs and the applications they run that collect terrific amounts of data for numerous purposes.[83]

As discussed above, location data is specifically underlined in "Article 4 (1) of the GDPR" as a factor with respect to which an individual is either "directly or

<https://edpl.lexxion.eu/article/EDPL/2018/3/4> accessed 2 May 2019.

[82] "*Data is to be considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort, or resources, taking into consideration the available technology at the time of the processing and technological developments. Page 4 Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol), 10.X.2018"* in CoE (n 23).

[83] Shakila Bu-Pasha, Anette Alén-Savikko, Jenna Mäkinen, Robert Guinness, and Päivi Korpisaari, 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' (2016) 2 European Data Protection Law Review <https://edpl.lexxion.eu/article/edpl/2016/3/7> accessed 5 April 2019.

indirectly identifiable". As an example, the term "location data" is commonly referred to as involving any information that corresponds to a geographic or geospatial position, either implicitly or explicitly[84]. It is noteworthy to point out the difference between the following cases to comprehend the role of location data as per several legal frameworks: cases in which location data are recognised as "personal or sensitive data," and cases in which the data are practically anonymised and is therefore not seen as "personal or sensitive data."

For the purposes of the latter case, it is crucial to note that personal data from which identifiers are taken out become anonymised[85]. However, taking the *"The whole is more than the sum of its parts"* saying into account, location data can be put to use to infer different and highly prevalent personal data[86], through which it can be seen as sensitive data. As it was mentioned in the beginning of this section, location data constitutes personal data, while it can also become a type of sensitive data. It is due to this definition that location data are accepted as identifiers of personal data. Thus, this thesis focuses on location data and considers it to constitute personal and/or sensitive data.

It is noteworthy to mention that the new ePrivacy Regulation Proposal states as follows:

[84] Location Forum, 'Location Data Privacy: Guidelines, Assessments and Recommendations' (2013) 2(3) 7 <https://docplayer.net/9241139-Location-data-privacy-guidelines-assessment-recommendations.html> accessed 23 February 2019.
[85] "*There are scholars who argue that a distinction between personal data and sensitive personal data does not hold in the new age of big data. Instead they suggest that all personal data should be considered as possibly sensitive personal data"* in Purtova (n 20).
[86] Atle Årnes and Catharina Nes, 'What does your app know about you?' (*Datatilsynet*, 2011) 14 <http://www.datatilsynet.no/Global/english/APPrapp_english.pdf> accessed 5 April 2019.

> *"(17aa) Metadata such as location data can provide valuable information, such as insights in human movement patterns and traffic patterns."*[87]

The Proposal also requires to genuinely anonymising the result before sharing the analysis with third parties. The definition of the term "personal data" must be further developed and expanded[88], too, to involve any data that can potentially allow the direct or indirect identification of individuals. With the increased effect of technology, these various sorts of identifiers will evolve as well, as IP addresses are now commonly accepted to be a type of personal data.[89]

Overall, the existing definition of personal data is "broad, flexible and adaptable to technological context" [90] of the mobile ecosystem. As Purtova puts it, the mentions of "identifiable natural person" and "information relating to a natural person" are open to interpretation, and in fact, call for clarification as to what actually constitutes a "relevant possibility of identification" and a "relevant" relationship between data collected and the data subject.[91]

The interpretation of "the European Court of Justice" ("ECJ") in *Breyer* helps fit the definition in the context of the mobile ecosystem better in terms of "additional

[87] ePrivacy Regulation Proposal (n 12).
[88] See Miranda Mourby, Elaine Mackey, Mark Elliot, Heather Gowans, Susan E. Wallace, Jessica Bell, Hannah Smith, Stergios Aidinlis and Jane Kaye, 'Are 'Pseudonymised' Data Always Personal Data? Implications of The GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review <https://www.sciencedirect.com/science/article/pii/S0267364918300153> accessed 15 February 2019.
[89] 'What is personal data?' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> accessed 10 February 2019.
[90] For a criticism, see Schwartz and Solove (n 40) 9.
[91] Purtova (n 20) 44.

data"[92] and combining data. Also, user signature, including activity and movement as in Google Web & App Activity, and other device identifiers, also involving behavioural choices in device use, are associable as part of transactions that are both sensitive and non-sensitive. Therefore, it is important that legislation defining the term must bear in mind that personal data can be exposed from other forms of data, by which its derivation, implication, and prediction are possible. As such, Purtova argues, moving forward, there is a need to address the broader context, in the sense that all the data categories and their specific requirements to type, storage, collection, and processing are increasingly relevant.[93]

Overall, ENISA's report[94] provides a generalised approach towards the nature of data collected on smartphones, whether it constitutes "personal data" or not. In other words, the report states that almost everything, as in, all data or information related to the smartphone or data subject's use of smartphone, can fall under the definition of personal data for the purposes of the GDPR. Although Purtova's comments on the concept of personal data are not directly linked to the smartphone ecosystem, it would not be wrong to say that ENISA's approach overlaps with Purtova's outstanding analysis bringing an inclusive and all-encompassing perspective. She argues that, when the "hyper connected," in Floridi's words,

[92] "The European Court of Justice" ("ECJ"), *Breyer*, in its October 2016 verdict, decided that "personal data" *"must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."* See Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.
[93] Purtova (n 20) 44.
[94] ENISA (n 18) 15.

"onlife"[95] world of data-driven agency comes, "the intensive compliance regime" of the GDPR will soon become "the law of everything," well-intentioned but unmanageable, extremely challenging to maintain. She further adds that the separation of "personal" from "non-personal" data is not ideal and in fact must be abandoned. Purtova gives a compelling reason and solution for this: the principle that all the data processing should prompt protection should be welcomed, or in her words "embraced" and "welcomed" by all means, and how this protection can be scalable should be comprehended.

Looking from another perspective, another recently debated issue related to data protection concerns data ownership, here also, the distinction between personal and non-personal data appears to be a questionable and blurring issue as Zech also supports by referring to ECJ judgment in the *BHB vs Hill* case.[96] Zech prefers not to differentiate "personal" and "non-personal" data for the purposes of clarity and avoiding confusion.[97]

1.4. PROCESSING

Various means of defining processing will be insufficient to cover the extent and comprehensiveness of the term and are particular to collection. The definition of processing must be inclusive and extensive, as opposed to exhaustive. As such,

---

[95] "*The term 'onlife' was coined by Luciano Floridi and refers to 'the new experience of a hyper connected reality within which it is no longer sensible to ask whether one may be online or offline' in Luciano Floridi"* in 'The Onlife Manifesto: Being Human in A Hyper connected Era' (2015) 64 Library Review <https://www.emeraldinsight.com/doi/abs/10.1108/LR-04-2015-0034> accessed 3 January 2019.

[96] Herbert Zech, 'Data as a tradeable commodity' in Alberto De Franceschi, *New Features of European Contract Law: Towards a Digital Single Market* (Intersentia 2016) 51–79.

[97] See also Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) GRUR Int. 989, 997 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> accessed 4 April 2019.

countries are urged to consider technological growth in methods of data analysis in a more inventive and forward-looking manner. In addition, the full, end-to-end lifecycle of data must be encompassed in processing, covering its entirety from creation to deletion, including the potential use of data to uncover other data.[98]

In view of this, it is offered by Privacy International to explicitly incorporate data generation into the 'processing' definition. Data protection law thus far does not expressly undertake the act of processing, which is key. It requires regulation and supervision, together with which individuals must be allowed protection. Privacy International examines the issues around the concept of 'data exploitation', which it observes as having arisen from the excessive generation of data, because the prerequisite for further processing is generation. The proposal to have processing further regulated and supervised rests on this analysis.[99] Privacy International puts it eloquently by referring to the bedrock principles and underscoring the importance of the intersection with the concept of "processing" as follows:

> *"An absence of transparency, a lack of accountability, combined with low awareness regarding how data is collected and handled, exacerbate the problem created by the far-reaching scope of data generation by the products, services and platforms available. In today's data-based realm, this problem causes major disproportion in the distribution of power. Extending the definition of 'processing' to include this evaluation will eventually*

[98] See also Andrew Hilts, Christopher Parsons and Masashi Crete-Nishihata, 'Approaching Access: A look at consumer personal data requests in Canada' (*CitizenLab*, 12 February 2018) <https://citizenlab.ca/2018/02/approaching-access-look-consumerpersonal-data-requests-canada> accessed 22 March 2019.
[99] FRA (n 24).

uphold the principles of 'use limitation' and 'data minimisation'."[100]

These concepts will be discussed in the following Chapters.

1.5. GOOGLE'S TENTACLES

The GDPR requires the organisations that collect, use or store the personal data of people in the EU to comply with the GDPR's requirements, and holds them accountable in case of non-compliance or a failure to comply, by making such organisations face large fines. Google clearly falls under this scope, not only because of its business model and its services used in profit-making, but also because in the mobile app environment, when data is collected through the use of a smartphone belonging to a natural persona, the "personal" or in other words "private" nature of the smartphone usage could imply that such data needs to be considered as personal data under the GDPR.[101]

Also, Google has updated terms and contractual protections, and explicitly stated that the company is a "processor of personal data", and that they make available data processing terms, mirroring the relationship between the controller and processor, where required.[102] Products where Google acts as a processor include, but are not limited to, Android Enterprise, Google Analytics for Firebase[103] and G

[100] Privacy International (n 49) 27.
[101] See ENISA (n 18) 15.
[102] 'Compliance | How Google Complies with Data Protection Laws' (*Google*) <https://privacy.google.com/businesses/compliance/#!?modal_active=none> accessed 2 May 2019.
[103] Google Firebase is a part of Google Marketing Platform which also includes Display & Video 360, Campaign Manager, Search Ads 360, Google Analytics, Tag Manager, Optimize, Data Studio, Attribution; 'Data Collection - Analytics Help' (*Google*) <https://support.google.com/analytics/answer/6318039?hl=en> accessed 15 April 2019.

Suite.[104] However, on the other hand, it must be noted that Google also states that it acts as "the controller" for its publisher products, since it often makes "decisions on the data to deliver and improve the product."[105]

As Google stealthily and silently became the "Big Brother" of today's world as well as the mobile ecosystem, particularly involving Android users, it currently holds data on users more than many could even imagine. This raises the following question: "Why Google collects so much data?"

The answer is simple, yet, it requires a true understanding of the company's ways of profitmaking. Put differently, the answer lies at the heart of Google's business model and its profit-making mechanisms. Firstly, the data collected could be utilised by the IT giant to sell targeted advertising. Google collects data and target consumers to show them ads in which they are more likely to be interested.

Secondly, Google also uses that data to track consumers and direct them to buy more products and services, by consuming the advertised content, either online or in-store.[106] This commercial aspect of Google's business model and the way it uses personal data collected will be discussed in Chapter 3 in detail.

Going into the data collection of Google's specific services, Android is a Google product, but it supplies Google with much more than merely serving as a product

[104] Other products are Google Cloud Platform, Ads Data Hub, Google Ads Customer Match, Google Ads Store sales (direct upload).
[105] 'Why Is Google A "Controller" Under The GDPR as Opposed to A "Processor" Of Data? GDPR FAQs - Google Ad Manager Help' (*Google*) <https://support.google.com/admanager/answer/9035987?hl=en> accessed 10 May 2019.
[106] Google merely gives information on online-to-store conversions as aggregated figures; 'Google Help' (*Google*) <https://support.google.com/google> accessed 15 April 2019.

to be consumed. If an individual uses an Android device with the Chrome[107] browser running, or through the apps, the user installed on his/her phone, Google knows whether that person is traveling by foot or car, where he/she shops, how often he/she uses TripAdvisor app.

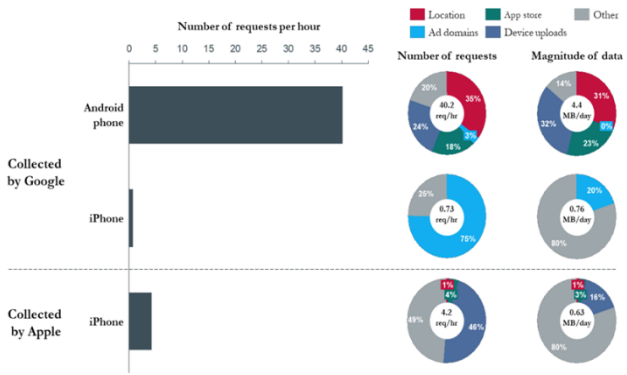
Google's tentacles have been increasingly reaching out to more users with the development of technological methods and tools enabled on data subjects' mobile phones[108].

In his landmark research, Schmidt studied Google's data collection practices and detailed "data mining in a 24-hour period from a stationary Android phone with Chrome running in the background."[109] The idle - dormant smartphone running on the background Android OS and Chrome are found to be sending data to the IT giant's servers an average of 14 times an hour, 24 hours a day.[110]

Also, one of the most striking conclusions is that "a major part of Google's data collection takes place while a user is not directly engaged with any of its products or services".[111]

[107] For further detail, see Schmidt (n 3). Also, note that Safari has recently been limiting tracking considerably. However, Chrome acquires basic information on the type of device and type of OS etc., as well as general device information to the extent that the OS allows. However, with regard to web and other apps activity, it does acquire quite an extensive amount of data. Generally, this depends on how much the OS allows, and which permissions are asked for.
[108] 'Smartphone Solutions for Smarter, Greener Urban Mobility' (*Horizon 2020 - European Commission*, 18 May 2017) <https://ec.europa.eu/programmes/horizon2020/en/news/smartphone-solutions-smarter-greener-urban-mobility> accessed 15 April 2019.
[109] Schmidt (n 3) 3.
[110] ibid.
[111] 'How Google Uses Information from Sites or Apps That Use Our Services' (*Google*) <https://policies.google.com/technologies/partner-sites> accessed 15 April 2019.

Figure 1.1 Traffic Data Sent from Idle iPhone and Android Mobile Phones



Source: Schmidt (2018) at 14

One of the dismal conclusions of this research is that, even if Google makes attempts and tries to be more transparent, naming the methods of data collection through "Google products," in Schmidt opines that technical ways, which these products use for data collection "may not be easily graspable by a general user."[112]

The technical and "complicated" nature of these practices deems the transparency principle, as a high threshold, more difficult to achieve. However, as legal design,[113] thinking exists as a method for people from legal professions to explain legal concepts by using more creative and simple ways, Google should be able to find a way to do it as well, of course, in technical terms. Google should seek to deliver a Privacy Policy or Privacy and Terms statements on its website, explaining the most complex data processing matters in a easily graspable and unambiguous way so that

[112] ibid 36.
[113] 'What Is Legal Design Thinking - Visual Contracts, A Strategic Business Advantage' (*Visual Contracts*) <https://www.visualcontracts.eu/community/what-is-legal-design-thinking> accessed 15 March 2019.

an individual who is not coming from a technical background, but who is also keen to find out about how his/her data is being processed can be fully satisfied with the explanations and examples Google provides. The simplicity and clarity should be in Google's DNA if it wants to gain its users' trust[114]. Although there are mounting privacy concerns after the incidents such as Cambridge Analytica[115], the study comes amid rising questions regarding the methods used by Google for data collection purposes, including disputes concerning consumer protection. In such cases, consumers gave rise to highly debated questions by claiming the tech-giant misled them over its conducts and practices in "incognito"[116] mode.[117] These privacy concerns, incidents denouncing, and revealing Google's defects are escalating into a greater dispute and heated debate about digital privacy in the world today.

Can Google identify a data subject directly from the information it has?

Without encountering any difficulty, Google can "distinguish" a data subject from other data subjects merely through the information it collects. Therefore, it could be concluded that data subject can be identified. Google does not have to know someone's name for him or her to be directly identifiable – though ironically, Google does know it automatically as soon as a data subject signs up for an account

[114] See World Economic Forum, 'Unlocking the Value of Personal Data: From Collection to Usage' (2013) 4 <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf> accessed 15 April 2019.
[115] 'Cambridge Analytica Controversy Must Spur Researchers to Update Data Ethics' (*Nature*, 27 March 2018) <https://www.nature.com/articles/d41586-018-03856-4> accessed 15 April 2019.
[116] "*Incognito mode in Chrome allows you to browse the web without recording webpages and files in your browser or Account history (unless you choose to sign in). Cookies are deleted after you have closed all of your incognito windows and tabs, and your bookmarks and settings are stored until you delete them. It is important to note that the incognito mode previously Google to track, know and remember details that the mode normally should not be able to do*." See in 'Browse in Private - Computer - Google Chrome Help' (*Google*) <https://support.google.com/chrome/answer/95464> accessed 15 April 2019.
[117] Schmidt (n 3).

using his/her real name. Even if the data subject does not do this, a "blend" or "combination" of other identifiers can easily be enough to identify the user; and since that individual is "directly identifiable" from the information collected by Google, it could be inferred that this constitutes "personal data".

Can Google identify an individual indirectly from the information it has (when combined with other available information)?

It is important to recall the indirect component of the "personal data" definition given under the GDPR. Even if additional information might be needed to be able to identify someone, the user may still be identifiable regardless. The additional information may already be available, or it may be information that Google needs to get from a different source. This is especially the case, not for Google as it is the leading hub of global data, but for third party apps or websites, running on the data subject's smartphone.

As Schmidt's research re-affirms, the smartphone users' collected data can be "reconstructed to be able to identify them." However, this does not mean that the user would be "identifiable under the GDPR." Google should "particularly be careful in relying on the anonymised[118] of the data it collects especially in certain circumstances." Regarding the anonymous data, Schmidt found that Google actually can "identify smartphone users by combining "user-anonymous" advertiser data with its own collected data."[119]

[118] "*Anonymization is just one process we use to maintain our commitment to user privacy. Other processes include strict controls on user data access, policies to control and limit joining of data sets that may identify users, and the centralized review of anonymization and data governance strategies to ensure a consistent level of protection across all of Google*." See also, 'Two of the Techniques We Use to Protect Your Data' (*Google*) <https://policies.google.com/technologies/anonymization?hl=en-US> accessed 15 May 2019.
[119] Schmidt (n 3).

GOOGLE LOCATION SERVICES

Google is the network location provider on its mobile platform, where it has a location service[120] called Google Location Services ("GLS"), also known as Google Location Accuracy. GLS is built with the purpose of offering better accuracy in device location.[121] Smartphones today already have Global Positioning System ("GPS"), the service that makes use of satellite signals to establish the location of a device. However, GLS can gather more information from Wi-Fi, mobile networks and device sensors to find the location of the smartphone. Location data is regularly collected from the device, which is put to use anonymously to gain improved location accuracy. A data subject's location can be identified with different degrees of accuracy by varying ways.[122]

The permissions that smartphone users provide to Android settings determine the specificity of the smartphone tracking the data subject's location. Also, it is worthy to note that the data subject's smartphone's location[123] continues to work even if

[120] 'How Google Uses Location Information?' (*Google*) <https://policies.google.com/technologies/location-data> accessed 15 May 2019.

[121] Google does have reasons to access location data, outside of GoogleAds and other than providing better services. It needs this information to track where the device is, whether it is lost, strengthening issues about operators and Google itself etc. Opting out of ads, however, is not an option. If it cannot acquire location data, it will keep showing personalised ads without location data-context, in case it cannot access location data. Therefore, for personalised services, location data is not a must. Each permissions site includes an "Others" tab, which generally includes the following options to prevent device from sleeping etc.

[122] Some of these ways are *"GPS, IP address, sensor data from the device, information about things near the device, such as Wi-Fi access points, cell towers and Bluetooth-enabled devices."* See 'How Does Google Know My Location?' (*Google*) <https://policies.google.com/technologies/location-data?hl=en#how-find> accessed 4 May 2019.

[123] ibid; *"It is not possible to withhold the information of general location from the device's location settings in terms of setting the region etc. In the worst case, the device identifies as 'worldwide' or 'international'. Therefore, all content that is shown based on location initially receive that information from IP-geolocation, which refers to the location/country the device recognises the user is in at that time. Therefore, this issue relates more to copyright issues (i.e. When showing Netflix content that is according to the country the user is in, etc.) rather than personalisation. These types of features can be tested with a VPN connection. Also, since*

GLS is turned off[124]; yet, the smartphone will rely only on GPS "to estimate device location for apps with the necessary permission".[125] Thus, it could be concluded that GLS is distinct from the device's location setting.[126]

Location data can be used by Google like other tech companies in order to offer basic products/services ("even if the precise location is not being collected from the device"[127]). As an example, such information can allow Google to understand the country in which the user is making use of their services, and if there is a sign-in from an unexpected location, Google can detect unusual account activity, which uses data collection to improve the service in hardening user access security.[128]

'localisation' is one of the main factors of relevant algorithms, the current region on the smartphone is default picked by the device itself. However, by following the general menu progression of Search Settings -> Search Results -> Region Settings, the region can be changed by the user."

[124] It is crucial to note the following most recent development by Google regarding of use of 'location data': *"The latest version of Google's Android phone software will also alert users when apps may be exploiting access to phone location data... Android Q, as the new operating system is currently known, will also let users restrict apps' access to location more generally — for instance, by only allowing apps currently in use to gather the data."* See more in Rachel Lerman and Matt O'Brien, 'Experts Aren't Impressed with Google's New Privacy Tools' (*Time*, 8 May 2019) <http://time.com/5585676/google-new-privacy-tools/> accessed 10 May 2019.

[125] See Schmidt (n 3).

[126] 'Manage Your Android Device's Location Settings - Google Account Help' (*Google*) <https://support.google.com/accounts/answer/3467281?hl=en> accessed 15 May 2019.

[127] According to the report, accessing apps from different devices or browsers changes user agent information. For example, Samsung Galaxy Note 4 Android 8.0 Chrome v25, or Apple iPhone XS Plus iOS 12.0.4 Safari 12.04 However, even if the user's IP is different, in an IP-geolocation query, if the user is accessing from a trustable IP-geolocation database, the result the device would product with regard to location data would be similar. The app can detect that you are in a certain country, for example, when logging in from different devices. The same applies for city information, but locations smaller than cities might be difficult to detect (since this depends on queries based on data updates regarding the IP location with respect to an ISP, rather than momentary sensor information like GPS). Also note that: "*Going into further detail on one source of location information, IP addresses are part of the fabric of the internet, and are assigned to a device whenever that device connects online. When a website needs to send something to a computer (like Google search results), it needs the computer's IP address to send it to the right computer. IP addresses are roughly based on geography, and as such, may be used to approximate the general location of a device."* See Google (n 102).

[128] 'Detecting suspicious activity on your account Google' (*Google*) <https://support.google.com/accounts/answer/140921?hl=en> accessed 15 May 2019.

LOCATION HISTORY

In 2009, exactly a decade ago, Google launched Google Latitude, an app allowing data subjects to share their location. Most of the users are familiar with ‘Location History’ because it can be considered as “a long-time Google product” as Quartz describes, with origins in the currently out-dated Google Latitude.

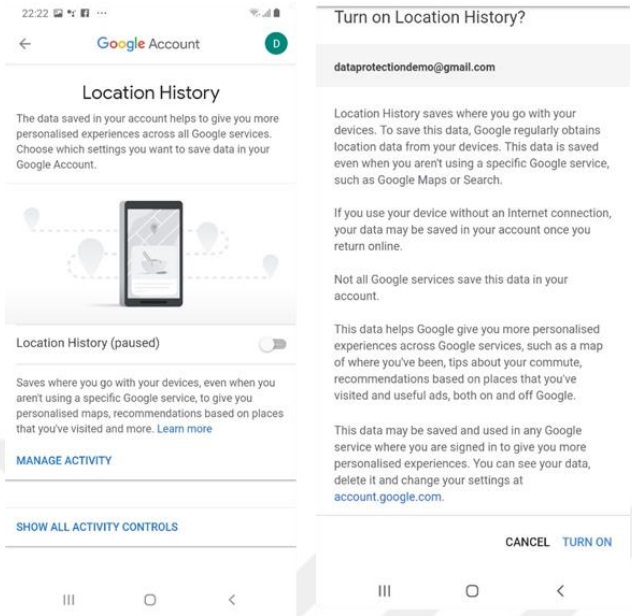
Today, the key features include the popular Location History that are used for purposes like making café, pub recommendations to smartphone users.

Google states the following as regards the Location History when starting the phone:

> *“Location History is not enabled on an Android phone by default, nor does the Android phone suggest it to be turned on when starting a new phone for the first time and setting the phone up.”*

However, it must be added that although what Google says is true, and Android phones do not suggest or nudge the smartphone users to turn on the location history when starting up the phone and opening a Google account; later, while the phone is in use the reminders begin to show up.

Figure 1.2: Google Location History



Source: Samsung Galaxy A10 2019 Screenshots

Google employs such features with its "Location History" tracking and record-keeping abilities. Google recently introduced an auto-delete function[129] that will allow users to delete data about their search and location.[130] The new tool automatically deletes a person's 'Location History', as well as 'Web and App Activity' after a specific time period. However, Android is fed information from various different sources, from not only search history, but also location data, offline credit card expenses, correspondence, websites liked and pursued, videos watched etc. Therefore, Google's practice is unfortunately disproportionate to its

[129] 'Introducing Auto-Delete Controls for Your Location History and Activity Data' (*Google*) <https://www.blog.google/technology/safety-security/automatically-delete-data/> accessed 1 May 2019.
[130] 'Google's Allowing Users to Automatically Delete Location and Activity Data' (*Android Central*, 2 May 2019) <https://www.androidcentral.com/google-auto-delete-feature-announced> accessed 3 May 2019.

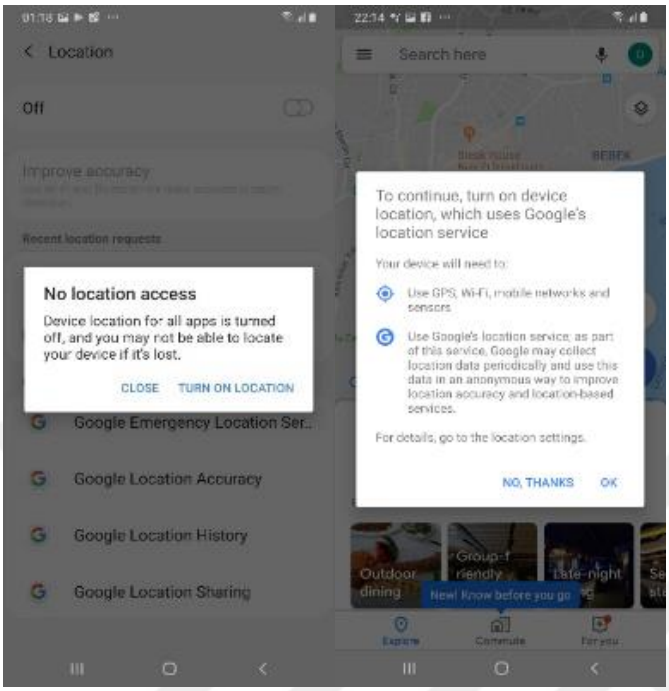
statements.

Data subjects can choose to delete the data after either 3 or 18 months. The function will then continue to delete the data over time. In addition, Google states that data subjects already can access their account for “simple on and off controls for Location History and Web & App Activity, and if they choose, they can delete all or part of that data manually.”

Last year, a Google revised help page attempted to clarify how Google tracks mobile phones on certain apps even when the location history is off, which is called ‘electronic tracking.’ Google went under fire after the Associated Press released findings from a three-day investigation, which revealed that Google apps track the phone’s location even when the Location History in the phone is turned off, as mentioned above.

In addition, the “Location History” feature is embedded into the start of commonly used apps, such as Google Maps, Photos, “the Google Assistant,” and “the primary Google app”, whereby “the app continuously reminds the user to change the setting from ‘off’ to ‘on’”.

Figure 1.3: Location History Turn On Reminders



Source: Samsung Galaxy A10 2019 Screenshots

Also, it was proven that with Android smartphones, when the user buys and starts the phone, pre-installed apps[131] coming by default with phone start to process data without asking the data subject's consent. Ironically, even if Google states that "Location History" and "Sharing Location information" are left to the data subject's consent, in practice, it was proven that Google can reach data subjects' location without the need of a data subject's consent or approval for turning "on" the location history feature.

[131] Apple made some developments about pre-installed apps, whereby some apps that used to be part of the pre-installed set were removed, and only basic services remain. Also, users could previously not erase pre-installed apps, which they now can. Android now supports a similar feature.

The research conducted by Quartz discovered that there was no common language used by the apps, explaining what occurs when the notorious "Location History" is enabled. The report adds, "None of those apps explicitly inform that activation will allow every single Google app, not just the one seeking permission, to access "Location History" data" (See Figure 1.2).

Quartz's findings can be considered to show a clear misrepresentation as CNIL's recent decision re-affirms[132]. According to Quartz's analysis and Schmidt's research of the phones' transmissions, the below given list shows the data that is regularly transmitted to Google once the Location History is turned on:

> *"A list of types of movements that user's phone thinks the user could be doing, by likelihood (like walking: 51%, on Bicycle: 4%, in Rail Vehicle: 3%); the barometric pressure; whether or not the user is connected to Wi-Fi; the MAC address which is a unique identifier of the Wi-Fi access point the user's phone is connected to[133]; the MAC address, signal strength, and frequency of every nearby Wi-Fi access point; the MAC address, identifier, type, and two measures of signal strength of every nearby Bluetooth beacon; the charge level of user's phone battery and whether or not user's phone is charging; the voltage of the user's battery; the GPS coordinates of user's phone and the accuracy of*

[132] 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC' (*CNIL*, 21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 10 February 2019.
[133] Laura Hautala, 'These Android apps have been tracking you, even when you say stop' (*CNET*, 14 February 2019) <https://www.cnet.com/news/these-android-apps-have-been-tracking-you-even-when-you-say-stop/> accessed 23 February 2019.

> *those coordinates; the GPS elevation and the accuracy of that."*

Budington opines that this list goes far beyond what a smartphone user would expect for "Location History".[134] Google claims that Location History is entirely opt-in and used for delivering better a better service to users. As explained above, Google informs on its Google Account Help support platform that

> *"The Location History is turned off by default for data subject's Google Account and can only be turned on if the user opts in."*[135]

However, the details given on its support website are overall not sufficient for a regular user to understand the scope and the amount of data it collects. Google fails to provide accurate and clear information to users[136], as the interaction between Google and the OS is not made clear.

The only information given focuses on the deletion and request of the data collected, while it does not specify what it means by "opt-in", and the scope of this "opting in". In the case of Android, a user can only opt-in for one app, such as Google Maps, while Google does not specify that opting in for one app may mean opting in for all apps as it was proven true.[137]

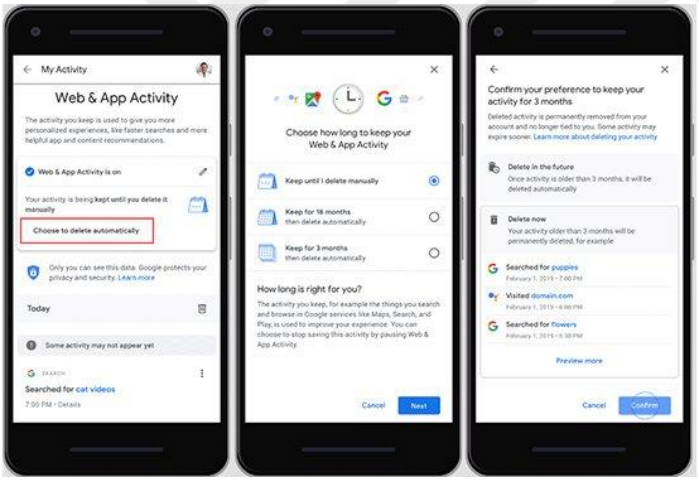
---

[134] See David Yanofsky, 'If you're using an Android phone, Google may be tracking every move you make' (*Quartz*, 24 January 2018) <https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/> accessed 4 March 2019.
[135] 'Manage Your Location History - Google Account Help' (*Google*) <https://support.google.com/accounts/answer/3118687?hl=en> accessed 15 May 2019.
[136] Jack Cohen, 'Your iPhone has a Hidden List of Every Location You've Been' (OneZero, 25 February 2019) <https://onezero.medium.com/your-iphone-has-a-hidden-tracking-list-of-every-location-youve-been-c227a84bc4fc> accessed 20 March 2019.
[137] Schmidt (n 3) 11.

For example, a user can get traffic congestion related suggestions for his/her regular week-end trips, photos and videos organised by locations, suggestions according to favourite meeting spots, and find a lost smartphone without opting in for "Location History".

To sum up, according to Schmidt's research and the Quartz report, the "Location History" is not entirely opt-in, as Google claims it is, and although the user can edit, delete[138] history or turn the history off at any time, the tracking does not stop.[139] As discussed above, when the user is asked to opt in, the full extent of enabling "Location History" is not entirely made clear.

Figure 1.4: Web-based Google Account Web & App Activity – New Delete History Feature (as of May 1, 2019)



Source: Samsung Galaxy A10 2019 Screenshots

[138] Laurie Sullivan, 'Transparency for Leads in Open Exchange Boosts Publisher Count Past 500' (*Mediapost*, 2019) <https://www.mediapost.com/publications/article/334821/transparency-for-leads-in-open-exchange-boosts-pub.html> accessed 15 May 2019.

[139] When asked to opt in, however, the full implications of enabling Location History are rarely made clear. Here are some of the ways Google apps ask users to enable Location History; see Nicole Kobie, 'How to Delete Your Google Search History and Stop Tracking' (*Wired*, 2 April 2019) <https://www.wired.co.uk/article/how-to-delete-google-search-history-tracking> accessed 15 May 2019.

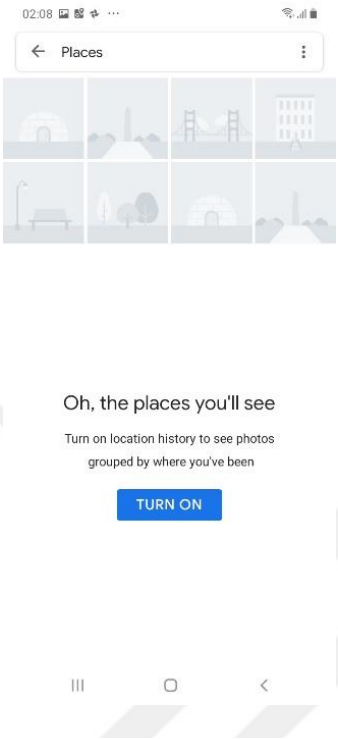
GOOGLE PHOTOS

In the context of Google Photos, both the app's own features and their relationship with "Location History" will be discussed.

If the user chooses the places album, he/she is requested to turn the location history on. The notification shows that the user will be able to group his/her photos according to location; however, it neglects to mention that this information can be used for different purposes such as tracking data about user's favourite entertainment spots. Therefore, the user is not provided the chance "to restrict the permission" they give to the extent of allowing "Location History".[140]

[140] See Schmidt (n 3); Binns et al (n 8); Andy Meek, 'Google Tracking Is Even Creepier Than You Thought, Study Finds' (*NYPost*, 2019) <https://nypost.com/2018/08/21/google-tracking-is-even-creepier-than-you-thought-study-finds/> accessed 3 May 2019; Hayley Tsukayama, 'Don't want Google tracking you? You have almost no choice, according to a study' (*The Washington Post*, 21 August 2018) <https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.1de6726f6450> accessed 13 April 2019.

Figure 1.5: Google Photos Location History Turn On Reminder



Source: Samsung Galaxy A10 2019 Screenshot

Also, for the purposes of the GDPR and as clarified in report,[141] the context of the processing of images is relevant to the determination of the sensitive nature of the data. The processing of images will not generally involve processing of sensitive data as the images will merely be covered under the definition of "biometric data" when being processed through a specific technical mean which permits the unique "identification" or "authentication" of an individual.[142]

Authentication is described as "being able to prove that a certain individual

[141] CoE (n 23).
[142] ibid.

possesses a certain identity and/or is authorised to carry out certain activities.[143]

Moreover, where processing of images is intended to reveal racial, ethnic or health data, such processing would be regarded as "processing sensitive data"; whereas, images processed by a video surveillance system only for security purposes, for instance, in a school area, or CCTV as in the UK would most probably not categorized and fall under the scope of "processing sensitive data".

GOOGLE MAPS[144]

Similarly, in the context of Google Maps, both the app's own features and their relationship with "Location History" will be discussed. In Google Maps, users are invited to "Get the most from Google Maps" by enabling "Location History". "Google needs to periodically store users' location to improve route recommendations, search suggestions and more" is shown on the screen. These recommendations are provided by Google as a response to learning about user's behaviour.

Even after the CNIL decision[145], this information (Google's tracking of users) is not being communicated to the user directly as the user turns on "Location History".

---

[143] ibid.

[144] 'Business Redressal Complaint Form' (*Google*) <https://support.google.com/business/contact/business_redressal_form> accessed 6 May 2019; Google Maps has become a tool of necessity when it comes to connecting businesses with potential and existing customers looking for directions and other information about services. A newly launched forum with the Business Redressal Complaint Form will let people who come across fraudulent activity report issues with business listings in Google Maps: *"These suggestions come in exchange for Google knowing how often the user goes for a run and how often the user charges his/her battery"*. Also see Jennifer Valentino-DeVries and others, 'Your Apps Know Where You Were Last Night, And They'Re Not Keeping It Secret' (*Nytimes.com*, 2018) <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> accessed 11 May 2019.

[145] See CNIL (n 132).

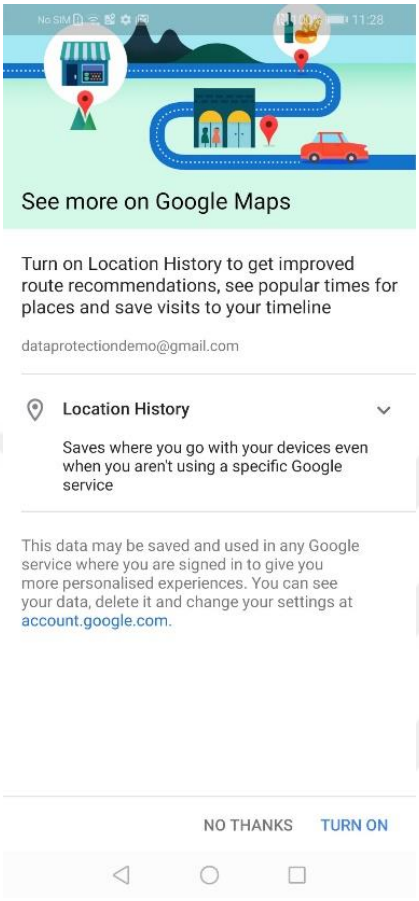
However, there is a general statement in the Google's Privacy Policy saying the following:

> *"We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low."* [146]

As per the updated terms and the data collection information Google provides specifically for Google Maps, there is absolutely no mention of tracking the data subject's smartphone's battery.

[146] 'Google Maps/Earth Additional Terms of Service – Google' (*Google*) <https://www.google.com/help/terms_maps/> accessed 10 May 2019; Laurie Sullivan, 'Google Maps Opens Fraud Complaint Forum' (*Mediapost*, 28 February 2019) <https://www.mediapost.com/publications/article/332582/google-maps-opens-fraud-complaint-forum.html> accessed 13 May 2019, wherein the link leads to a form that Google will review in accordance with its guidelines but completing and submitting this form does not guarantee the company will take action based on the request; 'Guidelines for Representing Your Business On Google - Google My Business Help (*Google*) <https://support.google.com/business/answer/3038177> accessed 4 May 2019.

Figure 1.6: Google Maps Location History Turn On Reminder



Source: Huawei P Smart 2019 Screenshot

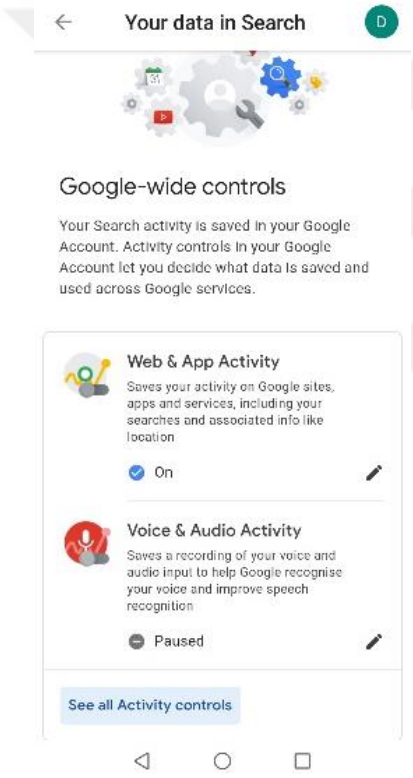
GOOGLE APP

Also in the context of the original Google App, both the app's own features and their relationship with "Location History" will be discussed. According to Quartz's research, in the Google App, an immediate request of consent pops up as soon as the user clicks on the app. Though it is important to note that for the second pilot user this notification merely comes up when the user accesses information on traffic congestion. Clicking "Learn More" shows Google's aim to make use of this data

not only to help the user on the way (concerning the traffic, directions etc.), but also to offer the data subject “more useful ads on and off Google.”

It is important to add that on a current Android smartphone, in the Google App, the general settings do not have a Location History part of its own. When clicked on All App Activity as seen in Figure 1.7, it leads the user to general Google Location History site.

Figure 1.7: Google App All Activity Settings



Source: Huawei P Smart 2019 Screenshot

GOOGLE ASSISTANT[147]

Lastly, in the context of Google Assistant, both the app's own features and their relationship with 'Location History' will be discussed.

Google Assistant's previous activation screen shows "The Assistant depends on these settings in order to work," the screen shows "Location History" as creating a "private map of where you go with your signed-in devices."[148] It does not make any statements regarding the Google's sharing of the user's Wi-Fi information. It merely states that Google will "regularly obtain location data from this device, including when you aren't using a specific Google product."

On the one hand, Google informs the users that location history is a "must" for Google Assistant's proper functioning.[149] However, it is important to note that, on the other hand, as seen in Figure 1.8, Google Assistant's setup page does not include a separate section for Location History; it shows "information on Device Information and Voice & Audio Activity." Therefore, it gives the impression that it is automatically affected by "the consent the user gives to the general Location History settings for the device".

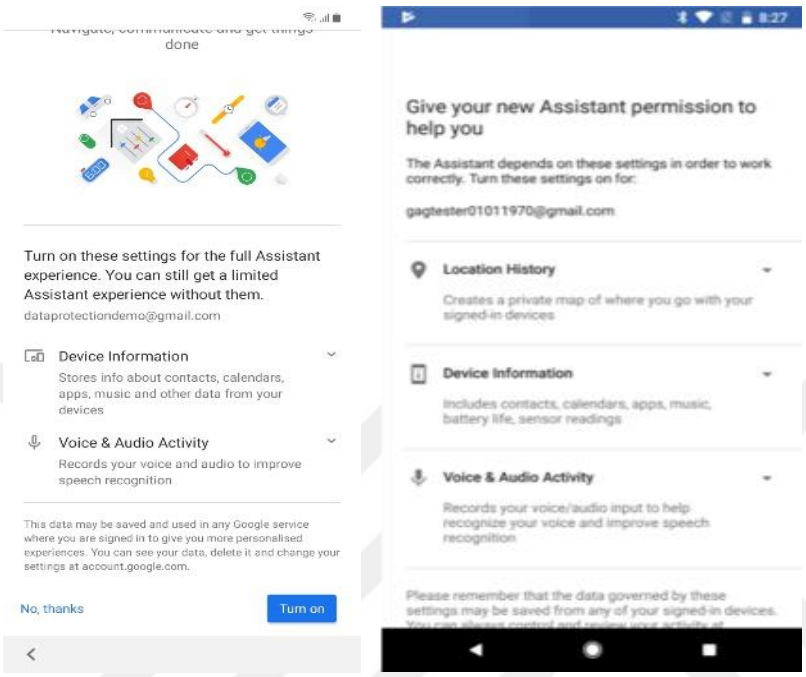
---

[147] Google Assistant has a strategic importance for Android Phones since it is a product comparable to the similar products of other tech giants such as Apple and Amazon.

[148] "In fact, that map cannot be categorised to be a fully private map for all means. Google provides Location data to advertisers based on the user's activity and it further states that these ads are "more useful" than those shown without using this information.

[149] *"Allowing these permissions is required to activate Google Assistant. Although if 'Location History' is disabled after Google Assistant is set up, the assistant will still function and does not seem to prompt for it to be re-enabled". "Android users can check some of the information Google has collected about them by looking at 'Your timeline' in Google Maps."* See 'Google Maps Timeline - Computer - Google Maps Help' (*Google*) <https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en> accessed 15 April 2019.

Figure 1.8: Google Assistant- On the Right, Screenshot from the Previous Setting Set, and On the Left, the Current Google Assistant Setup Settings



Source: Samsung Galaxy A10 2019 Screenshots

1.6. PERSONAL DATA COLLECTED BY APPS

As explained in the previous sections, although the GDPR clarified by adding a number of details to the definition of "personal data," the scope of it is still broad and ambiguous, and the question whether a specific data type qualifies as personal data may ask for a detailed analysis.

According to ENISA's report, "the personal nature of mobile device usage entails that such data has to be considered as personal data as in the meaning of the GDPR."[150] Accordingly, data on the smartphone itself is considered "private" or

[150] ENISA (n 18).

"personal" by its intrinsic nature like WhatsApp content and additionally, data that is associated with the smartphone including "environmental aspects" like smartphone's location as well as the unique identifiers are seen as private and personal as well. When the collected data is completely anonymised, the legal rules are not applicable and relevant since anonymised personal data becomes indistinguishable from other data.

The GDPR introduced the already known pseudonymous data "in a legal sense as a new subset of personal data."[151] Pseudonymisation, as a type of data processing, is referenced as both a security and data protection by design mechanism. As a result, in the GDPR context, "pseudonymisation can motivate the relaxation to a certain degree of data controllers' legal obligations, if appropriately applied."

As for the access to sensitive data, as it can be expected, stricter requirements apply under Article 9 of the GDPR. This is highly relevant for example for health-relevant apps or online dating apps, wherein explicit user consent for the data collection must be taken by the controller specifying the original purpose and the scope and amount of the data necessary to carry out the functionalities of the app.

Also, in the mobile context elements such as images can constitute sensitive data since they can reveal information that falls under the scope of Article 9. However, it is a fact that hardware providers are progressively enhancing their products with various "types of sensors"[152], such as the "NFC (Near-Field Communication)", "heart rate," and "iris scan" that are interconnected through Internet of Things (IoT).

[151] ibid 15.
[152] iOS asks for permissions when accessing sensors. These permissions either support an 'always' option or a 'when the app is in use/open' option. App-based settings can be managed in the Settings menu, in terms of what each app can address in what way. There is also a visual information system regarding which sensor is being used actively.

Meryem *et al*. observed that around 10 new sensors have now become popular in mainstream mobile devices in less than two years, bringing the number of mobile sensors to more than 30 sensors[153]. More examples of these include FaceID, active edge, depth camera (using infra-red), thermal camera, air sensor, laser sensor, haptic sensor, iris scan, heart rate and body sensors.

Sensors increase the intelligence of smartphones and are used in prevalent apps such as fitness apps.[154] However, these sensors are also provided for security purposes, like "authentication"[155], "authorization"[156], "device pairing"[157]and ensure the security of "contactless payment"[158]. Researchers have shown that "user PINs and passwords can be disclosed through sensors, such as the camera and

[153] Maryam Mehrnezhad and Ehsan Toreini, 'What Is This Sensor and Does This App Need Access to It?' (2019) Informatics 6 (1) 7 <https://www.researchgate.net/publication/330606893_What_Is_This_Sensor_and_Does_This_App_Need_Access_to_It> accessed 4 May 2019.
[154] Maryam Mehrnezhad, Ehsan Toreini and Sami Alajrami, 'Making Sense of Sensors: Mobile sensor security awareness and education' (2017) Technical Report Series No. CS-TR- 1510 <https://www.ncl.ac.uk/media/wwwnclacuk/schoolofcomputingscience/files/trs/1510.pdf> accessed 20 April 2019.
[155] Er De Luca, Alina Hang, Frederik Brudy, Christian Lindner and Heinrich Hussmann, 'Touch Me Once and I Know It's You! Implicit Authentication Based On Touch Screen Patterns' (*Core*, 10 May 2012) <https://core.ac.uk/display/22192389> accessed 15 May 2019.
[156] Ankita Jain and Vivek Kanhangad, 'Exploring Orientation and Accelerometer Sensor Data for Personal Authentication in Smartphones Using Touchscreen Gestures' (2015) Pattern Recognition Letters 68(2) 351-360 <https://www.sciencedirect.com/science/article/abs/pii/S0167865515002056> accessed 8 March 2019.
[157] Ying Zhao, Xing Liang, Xiaoping Fan, Yiwen Wang, Mengjie Yang and Fangfang Zhou, 'Mvsec: Multi-Perspective and Deductive Visual Analytics on Heterogeneous Network Security Data' (2014) Journal of Visualization 17(3) 181-196 <https://netsec.ethz.ch/publications/papers/mvsec-tr-2014.pdf> accessed 9 April 2019.
[158] Maryam Mehrnezhad, Feng Hao and Siamak F. Shahandashti, 'Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment' (2015) International Conference on Research in Security Standardisation 21-39 <https://www.researchgate.net/publication/300132931_Tap-Tap_and_Pay_TTP_Preventing_the_Mafia_Attack_in_NFC_Payment> accessed 18 April 2019.

microphone[159], the ambient light sensor[160] and the gyroscope[161].”[162] Maryam et al. also points out that “sensors such as NFC can also be misused to attack financial payments”[163]. Overall, it could be said, “sensitive data are undoubtedly being processed in apps, and create a paradox between the exception of ‘consent’ for the purposes of Article 9”.

A study conducted by Binns *et al*. say, “almost 9 in 10 Android apps are able to share data with Google”[164]. This landmark peer-reviewed study of almost 1 million Android apps complements Schmidt’s study, with its wide-range of apps and particular analysis on the app environment. This study sheds light on how data from smartphones are collected and further shared with “almost 90% of apps set up to transfer information back to Google”.[165] This research expanded to journals and magazines initiating significant debate upon its publishing.[166]

Images are not generally considered as sensitive data; however, images of data

[159] Laurent Simon and Ross Anderson, ‘PIN Skimmer: Inferring PINs through the Camera and Microphone’ (2013) 3rd ACM Workshop on Security and Privacy in Smartphones Mobile Devices 67–78 <https://www.cl.cam.ac.uk/~rja14/Papers/pinskimmer_spsm13.pdf> accessed 13 April 2019.
[160] Raphael Spreitzer, ‘PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices’ (2014) 4th ACM Workshop on Security and Privacy in Smartphones Mobile Devices <https://graz.pure.elsevier.com/en/publications/pin-skimming-exploiting-the-ambient-light-sensor-in-mobile-device> accessed 19 April 2019.
[161] Zhi Zu, Kun Bai and Sencun Zhu, ‘TapLogger: Inferring User Inputs on Smartphone Touchscreens Using On-board Motion Sensors’ (2012) 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks <http://www.cse.psu.edu/~sxz16/papers/taplogger.pdf> accessed 19 April 2019.
[162] ibid.
[163] Maryam Mehrnezhad, Mohammed Aamir Ali, Feng Hao and Aad van Moorsel, ‘NFC Payment Spy: Privacy attacks on contactless payments using NFC-enabled mobile’ (2016) 3rd International Conference on Research in Security Standardisation <https://www.researchgate.net/publication/309611581_NFC_Payment_Spy_A_Privacy_Attack_on_Contactless_Payments> accessed 19 April 2019.
[164] Binns et al (n 8).
[165] ibid.
[166] Aliya Ram, Aleksandra Wisniewska, Joanna S. Kao, Ændrew Rininsland and Caroline Nevitt, ‘How smartphone apps track users and share data’ (*Financial Times,* 23 October 2018) <https://ig.ft.com/mobile-app-data-trackers/> accessed 3 January 2019.

subjects can expose the racial make-up, which implies sensitive data processing under Article 9. Similarly, for example, in WhatsApp messages one's political views or a private information revealing a health condition, or mental health condition can be subject to third party malicious access which may pose a security issue in addition to privacy related risks. For mobile platforms, hosting apps that collecting or dealing with sensitive data requires additional measures to be taken.

Location data is not categorised as sensitive data; however, as ENISA underlines in its report

> *"The processing of location data on mobile platforms is generally considered to require special attention to the question of necessity and proportionality."*[167]

In addition to the GDPR, in the case of "over-the-top service providers of interpersonal communication services", the new ePrivacy Regulation Proposal has[168] novel directions for the legitimacy of the processing of "metadata" and "content" that are more rigid than the GDPR provisions. However, these rules will not be evaluated as thoroughly as the GDPR provisions as per the topic and objectives of this thesis.

Now that the definition and the scope of personal data have been discussed, the next Chapter discusses the methods that are used to collect the above listed data.

---

[167] ENISA (n 18).

[168] 'EDPB Releases Opinion on Interplay Between the ePrivacy Directive and The GDPR and A Statement On the ePrivacy Regulation' (*Hunton Privacy Blog*, 19 March 2019) <https://www.huntonprivacyblog.com/2019/03/19/edpb-releases-opinion-on-interplay-between-the-eprivacy-directive-and-the-gdpr-and-a-statement-on-the-eprivacy-regulation/> accessed 15 April 2019.

CHAPTER TWO

2. PERSONAL DATA COLLECTION METHODS USED BY GOOGLE

Today, "mobile internet constitutes the majority of global internet traffic".[169] The use of mobile internet and the ubiquity of the smartphones in people's daily routines changed the lives of data subjects in many ways. The victory of the mobile ecosystem is interconnected with data collection methods, data intelligence, and high quality of information (in terms of accuracy) that can be collected on data subjects. Everyone knows that IT giants, like Google, as well as mobile phones themselves collect data. However, the most-wondered question is "How? What methods are used to collect mobile data?"; although this Chapter does not aim to explore the technical details lying behind the available data collection methods, it briefly presents Google's data collection methods on mobile operating systems in a general way, and gives concise information when explaining the relevant features and means through which Google carries out data collection.

The aim is to portray data collection methods in a clear way by using plain language when explaining the technical background with the help of screenshots and illustration when necessary. This Chapter will start with a brief introduction giving a short background on the smartphone market, and then explore data collection methods by dividing them into passive and active categories, both using software and hardware technologies. This Chapter also delineates 'Web and App Activity' and 'Location History' collection methods, along with a description of the general collection methods used on smartphones by referring to different Google products and services where applicable.

---

[169] 'Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine' (*European Commission*, 18 July 2018) <http://europa.eu/rapid/press-release_IP-18-4581_en.htm> accessed 2 February 2019.

2.1. GOOGLE AND THE DUOPOLY IN THE SMARTPHONE MARKET

Android and iOS have created a duopoly resulting from their undeniable dominance in the mobile phone market. Both Android and iOS are in necessity to select apps with good, in fact, high quality from a great number of readily available app developers in order to make reasonable suggestions to their app users. In general, terms, "when the market is small, platforms like Android and iOS can allocate resources to manually test app quality for selection; but as the market size increases, the required resource for selection is also increased, and so challenges the platforms' capability, which thus faces the selection difficulty."[170]

Shao explains Android's use of open strategy in the game against its rival iOS.[171] Shao also points out the drawbacks of this clever yet in some way-questionable strategy by listing some of the unintended results triggered through its adaptation such as "fragmentation" matters, "weakened governance power", "entry of non-competent developers" and scrutinising the quality of "apps and developers".[172]

Android and iOS have substantial differences, which can be rooted in the business models of their parent companies. However, Yerukhimovich et al. point out that the platforms' approaches to data protection and privacy seem to be converging.[173] For instance, "Android is adopting run-time permissions requests, which iOS has used for years, while both are incorporating stronger encryption".[174] The greatest difference between the Android and iOS platforms stems from the fact that Apple

[170] Jianhua Shao, 'Strategic Signals in The App Economy: An Empirical Study of Google Play Store' (PhD, Nottingham University 2016) <http://eprints.nottingham.ac.uk/32742/> accessed 8 February 2019.
[171] ibid.
[172] ibid; see also Privacy International, 'How Apps on Android Share Data with Facebook' (2018) <https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report> accessed 15 April 2019.
[173] Yerukhimovich et al (n 7).
[174] ibid.

is the only manufacturer of the iPhone, on which a substantial portion of Apple's commercial profitability depends. Google, on the other hand, allows different hardware manufacturers to produce devices that run the Android, which shows Google's focus on being primarily a software provider. This marks several important differences in their personal data collection methods affecting the scope of user data and privacy protection.

The Google ecosystem while allowing many vendors to make hardware, it also complicates to patch existing systems, since there are multiple versions to be patched and many parties responsible for applying the patches, resulting in slow patching processes to occur.[175] This affects user privacy, as known "potential vulnerabilities exposing private data are likely to remain available for a longer time with Google".[176]

Apple, in contrast, can, at any time, apply a global patch to all iOS devices.[177] Apple is the sole code provider for all iOS devices, minimising the variety of pre-installed apps and their sources.[178] However, as Vidas et al points out Apple's centralised ecosystem does not come without its cost.[179] Also, as Yerukhimovich et al

[175] ibid.
[176] In addition, as McDaniel puts it, "Google's distributed ecosystem means that different carriers can add their own apps to the base Android distribution, and force users" towards installing and use. Such apps, commonly called "bloatware," often allow providers to collect tremendous amounts of private user data to utilize for their own motives. See Patrick McDaniel, 'Bloatware Comes to the Smartphone' (2012) IEEE Security and Privacy 10(4) 85–87 <http://patrickmcdaniel.org/pubs/mcd12.pdf> accessed 2 March 2019.
[177] ibid.
[178] Timothy Vidas, Daniel Votipka and Nicolas Christin, 'All your droid are belong to us: A survey of current android attacks' (2011) 5th USENIX Conference on Offensive Technologies <https://www.researchgate.net/publication/262290609_All_your_droid_are_belong_to_us_A_survey_of_current_android_attacks> accessed 3 March 2019.
[179] ibid; specifically, "the homogeneous attack surface of all iOS devices means that a single exploit may be able to compromise private data on all such devices", whereas, "different versions of Android potentially avoid such shared vulnerability".

demonstrated the iOS's centralized model better controls patching and privacy-invasive bloatware, however is more at risk to world-wide exploits.[180] Additionally, depending on OS management, app standards can generally be used to increase users' privacy.[181]

For example, health apps have recently shown a move for more transparency and control in collecting and processing users' data, which some operating systems are requiring from app developers. This indicates that the processing of personal data is considered particularly sensitive (i.e. locational data), given the need for the data subject's explicit and open consent for collecting such data, or the mandatory request for renewal of consent when necessary.[182] Although app stores are widely used in industries like healthcare, helping the customisation and improvement of services, there are also reliability and security issues surrounding the use of app stores due to the sensitive data handled in such industries.[183] Browsers and mobile OSs provide development platforms that support blooming markets for third-party applications; yet, it is noteworthy to mention that this may create risks for the

[180] Yerukhimovich et al (n 7) 7.
[181] Virgilio Almeida, Danilo Doneda and Carolina Rossini, 'How Do App Stores Challenge the Global Internet Governance Ecosystem?' (2016) 20(6) IEEE Internet Computing 49-51 <https://ieeexplore.ieee.org/document/7781550> accessed 5 April 2019.
[182] Susan Crawford, Jonathan Zittrain and Lisa Brem, 'Game Changers: Mobile Gaming Apps and Data Privacy' (2012) Harvard Law School Case Studies <https://casestudies.law.harvard.edu/game-changers-mobile-gaming-apps-and-data-privacy/> accessed 3 April 2019.
[183] For example, see Carrie E. Pierce, Sieta T. de Vries, Stephanie Bodin-Parssinen, Linda Härmark, Phil Tregunno, David J. Lewis, Simon Maskell, Raphael Van Eemeren, Alicia Ptaszynska-Neophytou, Victoria Newbould, Nabarun Dasgupta, Antoni F. Z. Wisniewski, Sara Gama and Peter G. M. Mol, 'Recommendations on the Use of Mobile Applications for the Collection and Communication of Pharmaceutical Product Safety Information' (2019) US National Library of Medicine – Drug Safety 42(4) 477–489 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6450855/> accessed 3 April 2019.

user.[184]

As Cluley and Seriot[185] show that some "third-party authors are malicious running on different operating systems, including iOS, and further discuss how third-party code could bring vulnerabilities, resulting from the fact that the authors of third-party applications are usually not security experts"[186]. Going to into the issue of security, the new risks that arise along with the progress in technology must be recognised in the scope of the mobile ecosystem. Commodifying personal data collection and making the processes more transparent, regulating collection purposes and methods, and preventing excessive processing with the data minimisation principle are crucial for the security of the mobile ecosystem. Firmly protecting data processing and compliance with the GDPR will not only enhance data protection and privacy rights of individuals, but also help in coping with countless cyber threats in the mobile ecosystem, such as crypto jacking. Even though smartphones are not as powerful as laptops or other bigger devices in terms of processing, problems such as crypto mining are evolving with the increasing

[184] Adrienne Porter Felt, Kate Greenwood and David Wagner, 'The Effectiveness of Application Permissions' (2011) University of California, Berkeley – 2nd USENIX Conference on Web Application Development <https://people.eecs.berkeley.edu/~daw/papers/perms-webapps11.pdf> accessed 3 April 2019.

[185] Graham Cluley, 'Windows Mobile Terdial Trojan makes expensive phone calls' (*Naked Security by Sophos*, 10 April 2010) <https://nakedsecurity.sophos.com/2010/04/10/windows-mobile-terdial-trojan-expensive-phone-calls/> accessed 5 March 2019; Nicolas Seriot, 'iPhone Privacy' (2010) Black Hat DC <http://seriot.ch/resources/talks_papers/iPhonePrivacySlides.pdf> accessed 5 March 2019.

[186] Roberto Suggi Liverani and Nick Freeman, 'Abusing Firefox Extensions' (*DefCon Security Assessment*, 2009) <https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-roberto_liverani-nick_freeman-abusing_firefox.pdf> accessed 6 April 2019; Simon Willison, 'Understanding the Greasemonkey vulnerability' (*Simon Willison*, 20 July 2005) <http://simonwillison.net/2005/Jul/ 20/vulnerability/> accessed 6 April 2019.

ubiquity of smartphones.[187] To provide some recent developments, crypto miners have managed to enter Google Play[188] and Apple's App Store[189], and thus subsequently banned by Google[190] and Apple[191]. ENISA reports[192] its observations on "malicious multi-featured mobile apps[193], having capabilities from DDoS, adware, banking Trojan to crypto mining that can brick mobile devices"[194]. According to ENISA's recent report in January 2019, "mobile miners' use percentage over the total threat incidents increased by 9,5% in Q1 2018."[195] The mobile malware landscape is steadily increasing, whereby threats increase annually and the continued use of older OS magnifies the problem.[196] Also, cyber criminals are increasingly getting involved with the use of mobile apps as a method to deliver

[187] Kaspersky Lab, 'KSN Report: Ransomware and malicious crypto miners 2016-2018' (*Kaspersky Content Hub,* October 2018) <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf> accessed 1 March 2019.
[188] Jason Gu, Veo Zhang and Seven Shen, 'Coin Miner Mobile Malware Returns, Hits Google Play' (*Trendmicro Security Intelligence Blog*, 30 October 2017) <https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/> accessed 1 March 2019.
[189] Chance Miller, 'Calendar 2 made $2K in 3 days mining cryptocurrency, but Apple says it violated Mac App Store guidelines' (*9to5Mac*, 13 March 2018) <https://9to5mac.com/2018/03/13/crypto-mining-calendar-app-ios/> accessed 1 March 2019.
[190] 'Google bans crypto-mining apps from Play Store' (*BBC Technology*, 27 July 2018) <https://www.bbc.com/news/technology-44980936> accessed 2 March 2019.
[191] Karissa Bell, 'Apple bans crypto-mining apps from App Store to protect your battery life' (*Mashable*, 12 June 2018) <https://mashable.com/2018/06/11/apple-bans-cryptocurrency-mining-apps> accessed 2 March 2019.
[192] ENISA, 'Threat Landscape Report 2018: 15 Top Cyber threats and Trends' (January 2019) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 2 March 2019.
[193] Kaspersky Lab, 'From Crypto Currency Mining to DDos Attacks: The New Multi-featured Mobile Trojan Loapi Discovered' (*Kaspersky Content Hub,* 18 December 2017) <https://www.kaspersky.com/about/press-releases/2017_new-multi-featured-mobile-trojan-loapi-discovered> accessed 2 March 2019.
[194] 'Monero-Mining HiddenMiner Android Malware Can Potentially Cause Device Failure' (*Trendmicro Security Intelligence Blog*, 28 March 2018) <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure/> accessed 2 March 2019.
[195] ENISA (n 192) 101.
[196] ibid 27.

crypto miners[197].[198]

Going back to Schmidt's study, he analysed data collection on and by all Google platforms and products including Android phones and Google Photos, in addition to Google's publishing and advertising (ads) services including Google Ad Manager (previously, DoubleClick). In this study, Schmidt signed up for a new Google Account as "Jane" and conducted research with a factory-reset Android phone. The research states, while riding the subway to work, she searched for cold medicine and later scheduled a doctor's appointment. From the appointment confirmation email, Google created a calendar event[199] without explicitly getting her consent to put the appointment in her schedule.

The below given Figure 2.1 outlines the activity history of that test user, where the grey 'pings' represent passive data collection during a typical day of an Android phone user.[200] The study further provides Jane's active engagement with Google products such as using YouTube and Google Maps.[201] This is a clear way to see how the study distinguishes "active data collection" and "passive data collection" – the latter occurs when the user is not using Google products directly.

[197] Pankaj Kohli, 'CoinMiner and other malicious cryptominers targeting Android' (*Sophos*, January 2018) <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-coinminer-and-other-malicious-cryptominers-tpna.pdf?la=en> accessed 2 March 2019.
[198] ENISA (n 192) 98.
[199] Schmidt (n 3) 37.
[200] Liz Entman, 'Study of Google data collection comes amid increased scrutiny over digital privacy' (*Physorg*, 2 November 2018) <https://phys.org/news/2018-11-google-scrutiny-digital-privacy.html> accessed 2 March 2019.
[201] Schmidt (n 3) 37.

Figure 2.1: Schmidt's Study of Subject Jane's "Day in the Life of an Android Phone

Source: Schmidt (n 3)

Provided that Chrome was "running" and "location enabled", an Android phone is 'pinged' throughout the day by other wireless networks, hot spots, cell towers, as well as Bluetooth beacons[202]. Also, for the duration of fifteen-minute walk around the neighbourhood the smartphone communicated with Google 9 times to send location requests to Google. These requests collected 100 unique identifiers from public and private Wi-Fi access points. It is noteworthy to recall that those unique identifiers constitute personal data – as they can be used to "identify" an individual as explained above in Chapter 1. Moreover, even when she does not use Google Maps, Google Search, Gmail, or YouTube, Google's publisher and ad products are found to be collecting data, as she visits web pages, uses apps and clicks ads. In this case, the number of passive data collection events was twice that of active ones.

2.1.1. Android and iPhone comparison

This landmark study also compared data collection from an idle Android phone

[202] For details provided on this page, see Schmidt (n 3) 2-10.

running Chrome[203], with an idle iPhone running Safari. The findings suggest, Google did not collect user location information during the 24-hour period. The Android phone, however, communicated with Google twice as often as the iPhone did. Accordingly, it was seen that an idle Android phone running Chrome sends back to Google nearly 50 times as many data requests per hour, as an idle iPhone running Safari.[204]

Even a better finding showing "the role of Android phones in Alphabet (Google's parent company) communicate with Google approximately ten times more frequently, as Apple devices do communicate with Apple servers".

These results highlight the fact that Android and Chrome platforms are critical vehicles for Google's passive data collection.[205] According to Quartz's report the Alphabet[206] subsidiary's "location-hungry tentacles are quietly lurking behind" and "creeping around" some of the most innovative features of its Android mobile OS.[207] In plain language, this is to say that Google silently reaches out to Android users' data through the use of innovative features. In its report, Quartz uses figurative language and depicts Android as an octopus, stating that once those tentacles latch on, phones using Android start silently transmitting data back to the servers of Google, including everything from GPS coordinates to nearby Wi-Fi

[203] Google takes Search business very seriously and recently announced its avid aspiration of ameliorating Google Search on mobile devices. See Laurie Sullivan, 'Page Load Times, Technology Are Major Ranking Factors in Google Search Results' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335987/page-load-times-technology-are-major-ranking-fact.html?edition=113918> accessed 15 May 2019.
[204] Schmidt (n 3) 2-10.
[205] ibid; also see John Thornhill, 'Should we think of Big Tech as Big Brother?' (*Financial Times*, 4 January 2019) <https://www.ft.com/content/43980f9c-0f5b-11e9-a3aa-118c761d2745> accessed 20 March 2019.
[206] Marziah Karch, 'What Is the Difference Between Google and Alphabet?' (*Lifewire*, 27 January 2019) <https://www.lifewire.com/understanding-google-and-alphabet-4116085> accessed 20 February 2019; also see Yanofsky (n 134); also see Alphabet's history and Larry Page's statement 'G is for Google' (*Alphabet*) <https://abc.xyz/> accessed 15 May 2019.
[207] ibid.

networks, barometric pressure, and even a guess at the phone-holder's current activity.

Some may argue that the product behind those transmissions is "opt-in" for Android users. However, this cannot be a solid reason for the supporters of this corrupted system, on which they can base their defence, showing that Android users are willingly opting to be a part of this system. This is because, as a widely accepted fact, this opt-in product could be difficult to avoid, even if a user can achieve to have the honour to understand this tricky system. "Opting in is also required to use several of Android's marquee features[208]".[209]

Most of the mobile apps require the user to create an account to be able to use the app. This is when the data subject types in their e-mail address and creates a password. Users could put the same password as their e-mail account password, while on the background; the app developer can see the password generated by the user. Even in cases when the app developer does not, when a new account is created on the mobile app, it means that the app developer, as well as other third parties, may reach your e-mail address in an easier way.

Who would think that providing very simple and basic information, such as an e-mail address, could result in such privacy risk? E-mail accounts are extremely rich data mines, in fact, due to which phishing attacks usually target e-mail accounts. For most of today's digital society, e-mail accounts often act as "de facto digital passports,"[210] as they connect data subjects to their social media accounts, bank accounts, and even services such as natural gas and electricity. Considering e-mail

[208] 'Android 1.1 Version Notes' (*Android Developers*, February 2009) <https://developer.android.com/about/versions/android-1.1> accessed 23 February 2019.
[209] Yanofsky (n 134).
[210] Bennett Cyphers and Jason Kelley, 'Facebook got Caught Phishing for Friends' (*Electronic Frontier Foundation*, 4 April 2019) <https://www.eff.org/deeplinks/2019/04/facebook-got-caught-phishing-friends> accessed 10 April 2019.

is the primary source of a user resetting their password, too, if a user's e-mail is compromised, then then all other information regarding the user's digital identity is exposed to risk.

2.2. ACTIVE AND PASSIVE DATA COLLECTION ON MOBILE PHONES

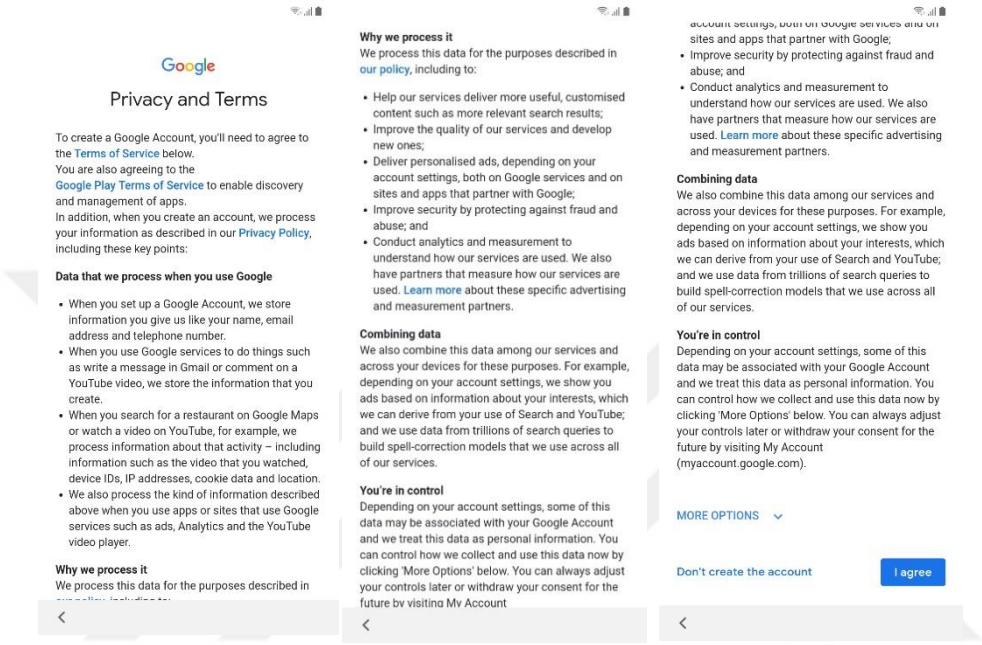
As briefly introduced above, although there are many different ways whereby Google collects data, in general, they can be divided into two: "active," the more obvious ways Google collects data, and "passive", which are the less obvious ways for data collection. The following section will focus on passive data collection methods for the purposes of this thesis, since active data collection is carried out with data subject's intentional sharing, and therefore is not problematic in terms of data subjects' rights and for the purposes of Article 5 principles.

Active data collection is used when the data subject directly and consciously communicates information to Google.[211] For instance, when the data subject signs into apps, such as YouTube or Gmail on his/her smartphone, and gives information, such as e-mail address, to be able to sign in. Another example is signing up to create a "Google Account". In order to sign up and use the services the account provides, the data subject needs to provide some "personal information", such as name and date of birth. A third example could be when a user searches for the Godfather's trailer, and writes the name of the movie on the search tool bar in the YouTube app on his/her smartphone. The search query is collected by Google, as this exchange of information between the data subject and YouTube can be seen as active data. These examples fit the definition of active data for the purposes of personal data collection. In scope of its definition, the information given in the examples, constitutes the type of information which is "directly exchanged" between the data

[211] Schmidt (n 3) 2.

subject and a Google product or service.

Figure 2.2: Google's Privacy and Terms Showing the Information Google Provides Regarding the Data It Collects



Source: Samsung Galaxy A10 – 2019 Screenshots

Google claims that it is being transparent about the data it uses. In fact, this is the case mostly for the active data collection it carries out. Google states that, basically, the information data subjects create or provide to Google are what is being collected, which is not big news. Above an example of active data collection was given for when data subjects sign up for a Google Account, after signing up, if a data subject is signed in to his/her account, Google collects and "protects" information the data subject creates when using its services. This can include the data subject's name, birthday and gender, data subject's password and mobile phone number, e-mails that the data subject writes, sends and receives on Gmail,

photos and videos which are saved, Docs that the data subject creates on Google Drive, comments the data subject makes on YouTube, as well as the contacts the data subject adds on the smartphone and calendar events.[212]

On the other hand, the second type of data, which is collected by "passive means, is defined as information exchanged in the background without any clear notification to the user."[213] Put differently, for instance, the "passive" means occur, "whereby an app is instrumented to collect data while it is running, probably without the data subject's knowledge".[214]

Going back to the example, when the user searches the Godfather trailer on the search tool bar, and the user's location is sent to Google as a result of the user's entering a search query, this information can be considered as passive data collected.

Google's passive data collection methods arise from platforms, such as Android and Chrome, applications such as Search, YouTube, Maps, and publisher tools such as Google Analytics. The below sections give a brief overview of Google's data collection methods on mobile phones: the first section focuses on the collection through Android and Chrome platforms, and the following sections present a concise overview of Google's data collection through publisher and advertiser technologies, then moving on to data collection through Google products and services, including the App Store, Google Play, and third-party data vendors.

---

[212] *"We collect data to make these services work better for you. This can include: Things you search for, Videos you watch, Ads you view or click, your location, Websites you visit, Apps, browsers, and devices you use to access Google services,"* in 'Making it easy to understand what data we collect and why' (*Google*) <https://safety.google/privacy/data/> accessed 19 April 2019.
[213] Schmidt (n 3) 2.
[214] ibid.

2.2.1. Data collection through Android and Chrome

Schmidt's research suggests, "The number of passive data collection events was twice much of the active events; in "day in a life" experiment, Google collected or inferred over two-thirds of the information through passive means. At the end of the day, Google identified user interests with remarkable accuracy." [215]

Once again, as mentioned in Chapter 1, according to ENISA's report, "the personal nature of mobile device usage implies that such data has to be considered as personal data as in the meaning of the GDPR".[216] Therefore, after connecting the dots, putting the personal data definition aside, even the fact that the smartphones are literally always with data subjects deems the data collected through those devices to be treated with diligence and caution. However, one of the main issues with such data collection stems from the lack of transparency and results in data subjects' lack of awareness and knowledge about the passive personal data collection methods, which are enabled through Google's far-reaching tentacles that are discretely hidden behind the innovative technologies, integrated in mobile ecosystems.

In this context, Schmidt has compelling arguments contending that the scope and amount of Google's "passive data collection has largely been overlooked by past studies".[217] Schmidt explains in detail how Google's passive data collection was, indeed, overlooked and further explores the passive ways used by Google. After his study, data collection methods on Android platforms have become a popular topic

[215] ibid 9.
[216] ENISA (n 18) 15.
[217] Schmidt (n 3) 2.

for newspapers[218] and online news platforms.

In addition to Android platforms, the Chrome browser contributes greatly to Google's data collection on smartphones, with over 2 billion active installs worldwide.[219] For instance, when the data subject completes an online form on his/her phone, the Chrome browser collects personal data and sends it to Google as part of the data synchronisation process. It also tracks webpage visits and sends user location coordinates to Google.[220] In addition, both Android and Chrome were found to be sharing data with Google, even via a dormant stationary Android phone, physically fixed in one place and not moving.[221]

When a data subject starts interacting with an Android phone (for example, when walks around or simply visits websites or uses apps), passive communications to Google server domains increase significantly, even in cases where the user did not use any key Google apps such as Google Maps. In the research, this significant increase is found be triggered principally by data activity from Google's publisher and advertiser products, namely Google Analytics, Google Ad Manager and Google Ads. According to Schmidt's research findings, such data constituted 46% of all

[218] See for example Rene Ritchie, 'Android sucks 10x more data than iPhone' (*iMore*, 31 August 2018) <https://www.imore.com/android-sucks-10x-more-data-iphone?_ga=2.98283034.426741244.1554988833-1448611976.1552437390> accessed 20 March 2019.
[219] Frederic Lardinois, 'Google says there are now 2 billion active Chrome installs' (*TechCrunch*, 10 November 2016) <https://techcrunch.com/2016/11/10/google-says-there-are-now-2-billion-active-chrome-installs/> accessed 20 March 2019.
[220] Schmidt (n 3) 3.
[221] ibid: *"The study compared both structures, and found that the idle Android phone, when Chrome is active in the background sent location information to Google 340 times during a 24-hour period, or at an average of 14 data communications per hour. In fact, location information constituted 35 percent of all the data samples sent to Google. This rate is shown to be significantly higher compared to the iOS."*

requests to Google servers from the Android phone.[222]

To sum up, the findings revealed the fact that, even if a user does not interact with any key Google applications, Google is still able to collect considerable information through its advertiser and publisher products[223] (See Figure 1.1 above for details).

Also, despite their differences (in terms of their parent companies' business models), the number of times an iOS phone communicated with Google services is "found to be similar to an Android phone".[224] Finally, it was found that if an iOS device user decides to decline using any Google product (as in, no Android, no Chrome, no Google applications etc.), and visits only non-Google webpages, the number of times data is communicated to Google servers still remains high. The communication between Google and iPhones as well as Android phones was found to be "driven purely by advertiser/publisher services.

2.2.2. Personal data and activity data collection

Google Play can only be benefited in order to download and use apps on one condition. First, the data subject must create (or must already have) a Google Account, which is described as being the key gateway through which Google collects personal information, including user name, e-mail and phone number. If a user registers for services such as Google Pay[225], Android furthermore, gathers the data subject's payment information as well as post code when asking the address, which becomes part of a user's personal information associated with their Google

[222] ibid.
[223] ibid 4.
[224] ibid.
[225] 'Google Chrome Privacy Whitepaper – Payments' (*Google*, 23 April 2019) <https://www.google.com/chrome/privacy/whitepaper.html#payments> accessed 30 April 2019.

account.[226]

The research adds that Chrome is capable of capturing such information in cases where it collects personal data through its form "autofill" feature, and such form fields typically include user name, address, phone number, login name, and passwords.[227] In such case, Chrome stores form-fill information on a user's local drive. Nevertheless, when a data subject logs in to Chrome using their Google Account, and enables its "Sync" feature, this information is sent to and stored on Google servers. Last but not least, Chrome as it is enabled by default, could also learn about the language(s) a person speaks during their interactions with its translate feature.[228]

In addition to personal data, Chrome and Android send Google information about a user's web browsing and mobile app activities. In fact, this can be seen on the Web & App Activity, as it will be discussed in Chapter 7.

2.2.3. Collecting location data through Android and iOS

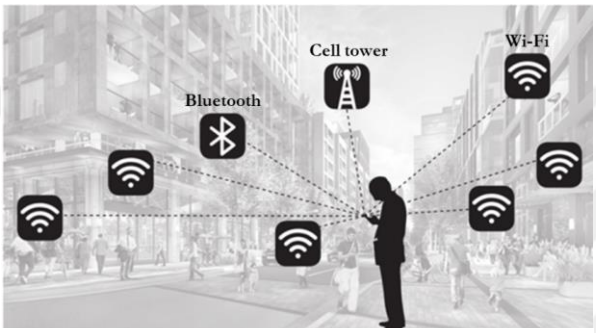
Android and Chrome platforms accurately collect location data of data subjects in different ways. For instance, a "coarse location" assessment can be done through GPS coordinates on an Android smartphone, or through a network's IP address on a desktop/laptop device. On the other hand, the data subject location accuracy can be enhanced further "fine location" through the use of nearby cell tower IDs, via scanning the device-specific BSSIDs, or basic service set identifiers, assigned to

[226] Schmidt (n 3) 3.
[227] 'Google Chrome Privacy Whitepaper – Autofill and Password Management' (*Google*, 23 April 2019) < https://www.google.com/chrome/privacy/whitepaper.html#autofill> accessed 30 April 2019.
[228] 'Google Chrome Privacy Whitepaper – Translate' (*Google*, 23 April 2019) <https://www.google.com/chrome/privacy/whitepaper.html#translate> accessed 30 April 2019.

the radio chipset used in nearby Wi-Fi access points.

As listed in Chapter 1, Android phones can also use information from the Bluetooth beacons registered with Google's Proximity Beacon API.[229] An even more astonishing finding is "these beacons not only provide user's geolocation coordinates, but can also pinpoint exact floor levels in buildings."[230]

Figure 2.3: Android and Chrome Use Multiple Ways to Locate a Mobile User

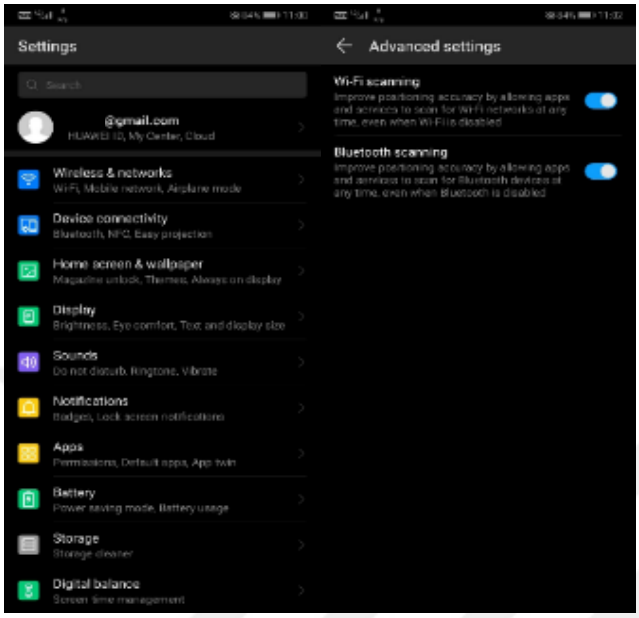


Source: Schmidt (n 3) 11.

It is burdensome for Android mobile users (in our case, Huawei and Samsung) to "opt out" of "location tracking." For instance, on an Android device, "even if a user turns off the Wi-Fi, the device's location is still tracked via its Wi-Fi signal." To circumvent such tracking, the only option left to the smartphone user is to disable the Wi-Fi scanning overtly by making an extra effort and taking an action, as shown in Figure 2.4 below.

[229] 'Proximity Beacon API – Overview' (*Google*, 9 February 2017) <https://developers.google.com/beacons/proximity/guides> accessed 20 March 2019.
[230] See also Schmidt (n 3).

Figure 2.4: Android Collects Data Even if Wi-Fi is Turned 'Off' by User (Wi-Fi 'Off' Can Be Seen in the Upper Tab of the Smartphone)



Source: Huawei Pro20 Screenshots

Schmidt shows that Google can easily understand whether a user is still, walking, and running, biking, jogging, or riding on a train or a car. Google does this via tracking of an Android mobile user's location coordinates at frequent time intervals, in combination with the data from on-board sensors (such as an accelerometer) on smartphones.[231]

The study states that a main part of Google's data collection takes place while a data subject is not directly engaged with any of its products, and that the magnitude of such collection is significant, especially on Android mobile devices.[232] An

[231] Schmidt (n 3) 12.
[232] ibid 23.

investigation carried out by the Associated Press found many Google-run services to continue to store location data[233], even when the user selects a privacy setting which explicitly states that it will prevent Google from collecting and storing this data[234].[235] An advocacy group took legal action against Google on behalf of UK iPhone users, claiming that the company illegally collected data from their iPhones while they used Apple's Safari browser[236]. [237]

As briefly mentioned in Chapter 1, the recently introduced auto-delete function that Google introduced does allow users to delete data about their search and location,[238] which automatically deletes a person's 'Location History', as well as 'Web and App Activity' after a specific time period. Users can choose to delete the data after either 3 or 18 months. The function will then continue to delete the data over time. Google also adds, "Users can access their account to manage their tracked history, by stating that on and off controls are available for 'Location History' and 'Web &

[233] 'Google tracks user location even when forbidden, investigation finds' (*Engineering and Technology*, 14 August 2018) <https://eandt.theiet.org/content/articles/2018/08/google-tracks-user-location-even-when-forbidden-investigation-finds/> accessed 21 March 2019.
[234] It is crucial to note the following most recent development by Google regarding of use of 'location data': *"The latest version of Google's Android phone software will also alert users when apps may be exploiting access to phone location data... Android Q, as the new operating system is currently known, will also let users restrict apps' access to location more generally — for instance, by only allowing apps currently in use to gather the data (some apps record location data continuously in the background)"*, see Lerman and O'Brien (n 124).
[235] Ryan Nakashima, 'AP Exclusive: Google tracks your movements, like it or not' (*Associated Press*, 14 August 2018) <https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb> accessed 22 March 2019.
[236] 'Google taken to court in UK over claims of improper data collection' (*Engineering and Technology*, 22 May 2018) <https://eandt.theiet.org/content/articles/2018/05/google-taken-to-uk-court-over-claims-of-improper-data-collection/> accessed 22 March 2019.
[237] Siobhan Doyle, 'Android smartphones collect ten times more data than iOS phones, study reveals' (*Engineering and Technology*, 4 September 2018) <https://eandt.theiet.org/content/articles/2018/09/android-smartphones-collecting-ten-times-more-data-than-ios-phones-study-reveals/> accessed 22 March 2019.
[238] Laurie Sullivan, 'Google To Let Users Delete Mobile Auto-Tracking Data' (*MediaPost*, 1 May 2019) <https://www.mediapost.com/publications/article/335301/google-to-let-users-delete-mobile-auto-tracking-da.html> accessed 5 May 2019.

App Activity', upon user consent, the data can be manually either partially or fully be deleted. Google, in trying to clarify its help resources, revised its statements regarding its tracking of mobile phones on certain apps even when the location history is off, which is called 'electronic tracking'.[239]

2.3. PUBLISHER AND ADVERTISING TECHNOLOGIES

This section talks about Google's data collection carried out through publisher and advertiser technologies. Google's data subject activity data collection mostly lives on "its publisher and advertiser-focused tools" such as AdSense.

These tools, which are also a great source enabling Google's data collection, have their own tentacles with an incredible reach. For instance, over 1 million mobile apps use AdMob, over 1 million advertisers use AdWords, over 15 million websites use AdSense, and over 30 million websites use Google Analytics.[240] Also, the latest statistics show that YouTube is the most popular mobile app in the US. [241] YouTube also relies on advertising, last year it made substantial changes in its ads model, and recently announced that the ads are getting longer[242].

Google offers the use of the Analytics SDKs to collect data from mobile apps, and uses the Measurement Protocol to collect data from other digital devices, like ticket

[239] Google, 'Manage Your Location History - Google Account Help' (n 135).
[240] 'Google Ads Vs Google Marketing Platform: which is best for your display ads?' (*Bannerflow*, 2018) <https://blog.bannerflow.com/google-ads-vs-google-marketing-platform/> accessed 24 March 2019.
[241] 'Mobile Apps: U.S. Smartphone Audience Reach 2019 | Statistic' (*Statista*, 2019) <https://www.statista.com/statistics/281605/reach-of-leading-us-smartphone-apps/> accessed 14 May 2019.
[242] Alex Weprin, 'Youtube Ads Are Getting Longer' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335989/youtube-ads-are-getting-longer.html?edition=113918> accessed 17 May 2019.

kiosks and game consoles.[243] To be able to do this, the developer should set up the SDKs and the Measurement Protocol[244].

One particular privacy issue pointed out by the researcher was the prevalent use of third-party libraries (or SDKs) within the pre-installed apps on Android phones. In general, SDKs are very popular within the mobile developer world, because they make it possible to build apps much more quickly than if the developer had to 'reinvent the wheel', so to speak. So the issue, say the researchers, is not that they found these third-party libraries within Android apps. The issue is that so many of these libraries seem to be related to advertising and user tracking. For example, of the 82,000+ apps examined by the researchers, 12,000 of them had a total of more than 164 different advertising-related SDKs.[245] Google announced that in October 2019, they will establish Google Analytics' mobile apps reporting to be based on the Google Analytics Services SDKs for Android and iOS. If users have properties that receive app data (no web, no Measurement Protocol) only from those SDKs, data collection and processing for those properties will stop on October 31, 2019. No data after that date will be available in any of those properties. They further added that access to the historical data in those properties via the Analytics interface

[243] 'Analytics Help – SDKs' (*Google*) <https://support.google.com/analytics/answer/7373305?hl=en> accessed 24 March 2019.

[244] *"The Google Analytics Measurement Protocol allows developers to make HTTP requests to send raw user interaction data directly to Google Analytics servers. This allows developers to measure how users interact with their business from almost any environment. Developers can then use the Measurement Protocol to: Measure user activity in new environments. Tie online to offline behaviour. Send data from both the client and server. Note: The Measurement Protocol only allows developers to collect user-interaction (event/hit) data. It does not allow developers to upload aggregated data like tables."* See more in 'Google Analytics – Measurement Protocol Overview' (*Google*) <https://developers.google.com/analytics/devguides/collection/protocol/v1/> accessed 26 March 2019.

[245] Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador and Narseo Vallina-Rodriguez, 'An Analysis of Pre-installed Android Software' (*IMDEA Networks Institute*, 2019) 4 <http://eprints.networks.imdea.org/1959/1/An_Analysis_of_Pre-installed_Android_Software_2019_EN.pdf> accessed 30 March 2019.

or the API will remain available until January 31, 2020[246].

Another angle is the kind of data streams handled in advertising operations via Google's mobile development. The information collected by Google's publisher and advertiser-focused tools comprises a "non-personal identifier that Google can use to send targeted advertisements without identifying the unique individual's personal information."[247] However, this proves to be useless in most cases, since when this data is combined with others, in fact, they could identify an individual. For example, while "AdSense collects data on mobile devices, they have a limited capacity of acquiring user information from mobile devices".[248] This is because, cookie data is not shared between mobile apps, the isolative method of "sandboxing" makes user tracking by advertisers quite difficult across these apps. Companies, including Google, make us of mobile ad libraries, like AdMob, which their app developers then embed into their mobile apps in order to serve ads and address the above cookie-related issue. Said libraries gather data when the apps are in use, and share that data with Google respective to the particular app, which they are part of. Example of such data can be GPS data, device model and so on, in case the relevant permissions are acquired for the app. Schmidt further elaborates that, these ad libraries are capable of sharing user-personal data like age and gender with Google, as confirmed by Google's own online statements[249].

In sum, Google uses advertising identifiers for mobile apps to serve ads in services where cookie technology may not be available. Google may utilize technologies that have similar functions to cookies.

---

[246] 'Analytics Help - Sun setting the Google Analytics Services SDKs' (*Google*) <https://support.google.com/analytics/answer/9167112?hl=en> accessed 30 March 2019.
[247] Schmidt (n 3) 16.
[248] ibid 18.
[249] ibid.

In some circumstances, Google links the identifier used for advertising on mobile applications to an advertising cookie on the same device, in order to coordinate ads across the data subject's apps and browsers, for instance, when the data subject sees an ad within an app that launches a web page in his/her mobile browser. Furthermore, it aids Google to improve the reports provided to advertisers on the effectiveness of advertisers' campaigns.[250]

2.4. GOOGLE'S APPLICATIONS AIMED AT DATA SUBJECTS

Google collects data from mobile apps, as it openly tells in its Privacy Policy that it gathers

> *"information about the apps, browsers and smartphones*[251] *its users utilise in accessing Google services, which helps Google provide features like automatic product updates and dimming user's screen if his/her battery runs low. The information Google collects includes unique identifiers*[252]*, browser type and settings, device type and settings, operating system, mobile network information including*

[250] See 'Types of Cookies Used by Google' (*Policies.google.com*, 2019) <https://policies.google.com/technologies/types?hl=en-US> accessed 16 May 2019.
[251] "But cell phone location data can reveal that same highly personal information to anyone with means and motivation," see Woodrow Hartzog and Evan Selinger, 'Why You Can No Longer Get Lost in the Crowd' (*The New York Times*, 17 April 2019) <https://www.nytimes.com/2019/04/17/opinion/data-privacy.html> accessed 20 April 2019.
[252] See more in 'Key Terms' (*Google*) <https://policies.google.com/privacy/key-terms#toc-terms-unique-id> accessed 24 March 2019.

carrier name and phone number, and application version number."

Google further informs that it collects,

> *"information about the interaction of smartphone users' apps, browsers and devices with its services, including IP address, crash reports, system activity, and the date, time and referrer URL of user's request when a Google service on the user's device contacts its servers"*.[253]

Google collects data about the smartphone user's activity in its services, which Google states it uses to do things like recommend a YouTube video the user might like. The activity information Google collects may include: terms the user searches for, videos the user watches, views and interactions with content and ads[254], voice and audio information when the user uses audio features, purchase activity, people with whom the user communicates or shares content, activity on third-party sites and apps that use Google's services, or Chrome browsing history that the user synchronised with his/her Google account[255].

---

[253] "*For example, when the user installs an app from the Play Store, or when a service checks for automatic updates. If the user is using an Android device with Google apps, then that device periodically contacts Google servers to provide information about the device and connection to Google's services. This information includes things like data subject's device type, carrier name, crash reports and which apps the user installed."* See more in 'Google Privacy Policy - When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control' (*Google*) <https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en_eu.pdf > accessed 30 March 2019.

[254] "*For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears."* See more in 'Views and Interactions with Content and Ads' (*Google*) <https://policies.google.com/privacy#footnote-content-views> accessed 15 May 2019.

[255] 'Synced with Your Google Account' (*Google*) <https://policies.google.com/privacy#footnote-chrome-sync> accessed 15 May 2019.

2.4.1. Google apps and services

As Google states on its Help website, it addresses the user to show user control and consent in the use of Google apps and services: "You're in control of what information you share with Google when you search. To browse the web more privately, you can use private browsing, sign out of your account, change your custom results settings, or delete past activity."

Under the notion of "Search and Browse Privately," the following are possible according to this web source. For Android, user search and site visits are not recorded in the browsing and download histories, while for iOS, user search, and site visits are not recorded in past activity, which is the term equivalent for iOS. As for cookies, for Android, cookies are deleted after the private browsing window is closed, and similarly for iOS, cookies are deleted after Incognito mode is exited.[256] If the user is using a browser (for which only Chrome and Firefox are supported) on their mobile device, they can thus search the web more privately, the tips for which will be detailed below. However, it is important to note that these tips do not work on the Google app for Android phones. Whereas for iOS, the website states that the user can search on Google and browse the web without saving their past activity by using the Incognito mode on the Google app on iOS.

The tips provided to ensure that Google's app and services are used in a more private manner are offered on the website as well. The user can benefit from any of these topics for tips, either for Android or iOS: "'Open private browsing mode',

[256] "It is crucial to note the following most recent development regarding "incognito" use: "the company said it will extend an "incognito mode" feature to its Google Maps and search apps. When activated, the app won't record user searches or movements, analogous to how the same feature works in its Chrome browser and YouTube now." See more in Lerman and O'Brien (n 124).

'Sign out of your Google Account', 'Remove all custom results', 'Delete past searches or stop saving them', or 'Delete your browser history'."[257] The methods behind these tips are explained, whereby a user can "browse the web without saving their past searches or other activity, by turning on private browsing in a mobile browser," or can "remove the results the user sees when tapping on links of customised content created by user's search and ad results data," since if not turned off, ads personalisation is active even if the user is signed out of their account.

For the purposes of this Chapter, since data collection methods by Google are key, it must be discussed that these statements, although useful in creating user awareness about what is and is not possible to do, as well as give users a guide showing how to take action, the website still does not include any further information – precise explanation - about what data Google collects and exactly how. When it states, for Android or iOS, that ad personalisation can be turned off and results can be removed, it is unclear whether either the user will merely stop future ads personalisation or past data will be cleared as well. Same applies for the private browsing mode or incognito mode: simply logging out of a Google account and opening a private browsing tab do not necessarily mean that all data tracking and collection by Google will be ceased. Whether it is or is not as such must be communicated to the user, explaining the following: *what/how much* data are acquired both with and without the user's consent, *from where* the data are acquired, *for what purposes* the data are acquired, and what precisely happens if the user *actively rejects* to give permission for collection of data. To install trust in Google's data collection methods and its mobile ecosystem, clarifying and demonstrating these facts is important.

[257] 'Search & Browse Privately - Android - Google Search Help' (*Google*) <https://support.google.com/websearch/answer/4540094?authuser=0&co=GENIE.Platform%3DAndroid&oco=1> accessed 5 May 2019.

2.5. CONCLUSION

2018 was a bewildering and hectic year for many smartphone users, especially for Android users, since they discovered that they are basically being 'spied on' by their smartphones, after the Pandora's box of personal data collection was opened. Following the emergence of media reports about how Google continues to track information about users, even such features are off created significant unease about the methods employed by its products and services. Google came under fire after the released findings of a research led by Schmidt, which revealed and showed that Google apps track the phone's location even while the "Location History" in the phone is turned off. In his research, Schmidt delved into the less noticeable methods for Google's data collection. One of the most debated findings of the research stated that even if data subjects avoid Google apps and Android phones, Google can still collect a large amount of data through the use of the digital advertising tools it offers to advertisers and publishers.

Fully understanding the ways through which personal data is collected is a must in today's world where ubiquity of mobile phones for the erosion of privacy and data protection is blamed for the excessive data collection practices of leading IT organisations.[258] Therefore, personal data collection through mobile phones has become a sensational topic, putting IT giants like Google and Facebook in the spotlight, as these service providers, app developers and mobile service providers are criticised for both collection methods, as well as the lack of clarity on these methods shown to the owners of the very data they collect.

With the booming effect of the GDPR, now combined with the long-expected

[258] Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing 2017).

ePrivacy[259] Regulation[260],[261] is expected have a complementary effect in establishing which methods are appropriate and necessary, and which are not, according to the stipulations under the GDPR. As part of the combat for the awareness and enhancement of data protection and privacy rights, Google has an immense role in showing good faith and clean practice.[262] Because despite its challenges mentioned above, the ubiquity of mobile phones and the increasing use of mobile apps worldwide also offer a great opportunity.

As long as data collection methods and practices reflect an image of compliance and respect to individuals' rights in the context of the mobile platform, a repository of appropriate and consent-driven data can help take us to the next millennium. Raising bidirectional communication between users and researchers, data and its proper collection methods can cultivate invaluable fields like "self-report instruments" for psychology,[263] smartphone apps for real-time monitoring;[264]

[259] EDPB (n 14).
[260] Warwick Ashford, 'Mind the overlap between GDPR and ePD, warns privacy lawyer' (*Computer Weekly*, 27 March 2019) <https://www.computerweekly.com/news/252460345/Mind-the-overlap-between-GDPR-and-ePD-warns-privacy-lawyer> accessed 4 April 2019.
[261] 'Apps/Mobile' (*ePrivacy*) <https://www.eprivacy.eu/en/industries/apps-mobile/> accessed 4 April 2019.
[262] Bart van der Sloot and Frederik Zuiderveen Borgesius, 'Google and Personal Data Collection' (2012) Google and the Law 75-111 <https://link.springer.com/chapter/10.1007%2F978-90-6704-846-0_4> accessed 5 April 2019.
[263] Erin I. Walsh and Jay K. Brinker, 'Is SMS appropriate? Comparative properties of SMS and apps for repeated measures data collection' (2016) European Journal of Psychological Assessment 35(1) 63-69 <https://econtent.hogrefe.com/doi/abs/10.1027/1015-5759/a000376> accessed 6 April 2019.
[264] John B. Torous, JP Onnela and Matcheri S. Keshavan, 'New dimensions and new tools to realize the potential of RDoC: digital phenotyping via smartphones and connected devices' (2017) Transnational Psychiatry 7(3) <https://www.ncbi.nlm.nih.gov/pubmed/28267146> accessed 6 April 2019.

mobile app use for improving health care,[265] prevention of suicide through apps,[266] and the list goes on. The possibilities are endless.

[265] Commission on the Future of Psychiatry, 'The WPA-Lancet Psychiatry Commission on the Future of Psychiatry' (2017) Lancet Psychiatry 4(10) 775-818 <https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(17)30333-4/fulltext> accessed 6 April 2019.

[266] Joseph Tighe, Fiona Shand, Rebecca Ridani, Andrew Mackinnon, Nicole De La Mata and Helen Christensen, 'ibobbly mobile health intervention for suicide prevention in Australian Indigenous youth: a pilot randomised controlled trial' (2017) BMJ Open 7(1) <https://bmjopen.bmj.com/content/7/1/e013518> accessed 6 April 2019.

CHAPTER THREE

3. PURPOSES OF PERSONAL DATA COLLECTION

The term "Infonomics" was coined in the late 1990s as commercial entities developed an interest in the value and turning data into money – "monetisability of data"; infonomics is a theory, the blend of information and economics, a relatively new discipline of asserting economic significance to information.[267] Today is the pivotal times to observe the infonomics theory.[268] Online advertising can be considered as an extension of today's infonomics theory based data driven economy.

As demonstrated in Chapter 2, companies, including Google, use tracking technologies to collect observed data, IP addresses[269], advertising identifiers for mobile apps[270], beacons, device fingerprinting in order to track across

[267] United States House of Representatives Committee on Energy and Commerce, 'Hearing entitled 'Algorithms: How Companies' Decisions About Data and Content Impact Consumers' (2017) 2 <http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf> accessed 10 April 2019.

[268] See LF Garifova, 'Infonomics and the Value of Information in the Digital Economy' (2015) Procedia Economics and Finance 23 738-743 <https://www.sciencedirect.com/science/article/pii/S2212567115004232> accessed 11 April 2019.

[269] "*Google's ad products may receive or infer information about your location from a variety of sources. For example, we may use the IP address to identify your general location; we may receive precise location from your mobile device; we may infer your location from your search queries; and websites or apps that you use may send information about your location to us. Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads you see, to measure ad performance and to report aggregate statistics to advertisers.*" See 'Advertising – How Google uses cookies in advertising' (*Google*) <https://policies.google.com/technologies/ads?hl=en-US> accessed 8 April 2019. Here, Google fails to specify all the means it uses to collect such data. In addition, it is noteworthy to mention that Google generally use "may" and gives very limited and shallow examples. See also David Nield and others, 'All the Ways Google Tracks You—And How to Stop It' (*WIRED*, 2019) <https://www.wired.com/story/google-tracks-you-privacy/> accessed 27 May 2019.

[270] ibid.

smartphones.[271] Meanwhile the proliferation of smart speakers[272] such as Google Assistant offers novelties and makes the observation of "real-time behaviour" possible[273] of data subjects. When messages and content targeted at a smartphone user is based on profiling prompts "a reaction," or in other words, "a response" from the data subject, as a result, the response of the data subject is monitored, creating extra data for processing and utilized to sharpen up the profile to be used in future targeting for advertising purposes.[274]

As per a report[275] by the Advertising Bureau and the PwC[276], digital advertising revenues in the US have passed $100 billion, with a total of $107.5 billion in 2018. As can be seen in Figure 3.1, this demonstrates an increase of 22% since 2017, a large portion of which was driven by digital video advertising, growing 37% year-over-year, and mobile advertising, growing 40% year-over-year. Overall, digital video on mobile devices makes up about 63% of the total revenue of digital ads, helping boom the mobile advertising business. Furthermore, it is noteworthy to mention that digital audio advertising (like ads on podcasts and Spotify etc.)

---

[271] Privacy International, 'Comments to the Article 29 Working Party Guidelines on Automated Individual Decision Making and Profiling' (2018) 5 <https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20submission%20on%20profiling%20guidance.pdf> accessed 6 April 2019.

[272] Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' (2016) IVIR 6(2) 3 <https://www.ivir.nl/publicaties/download/1747.pdf> accessed 6 April 2019.

[273] See 'Bringing You the Next-Generation Google Assistant' (*Google*, 2019) <https://www.blog.google/products/assistant/next-generation-google-assistant-io/> accessed 10 May 2019.

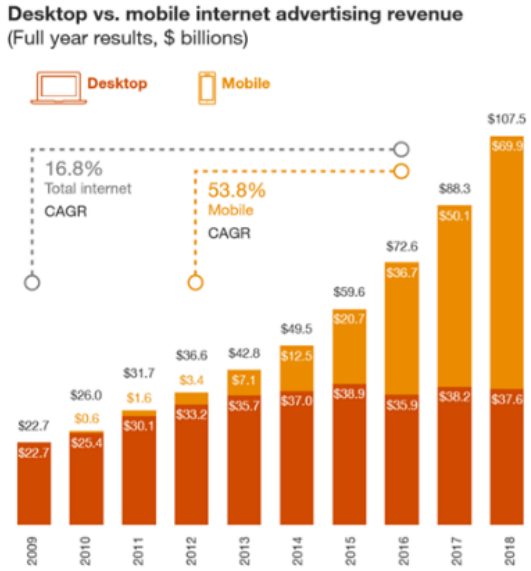
[274] EDPS, 'Opinion 3/2018 on online manipulation and personal data' (2018) 11 <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 10 April 2019.

[275] Kevin Kelly, *New rules for the new economy* (Penguin Books 2000) 240; Interactive Advertising Bureau (IAB), 'IAB internet advertising revenue report: 2018 full year results' (2019) <https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf> accessed 14 May 2019.

[276] Alex Weprin, 'U.S. Digital Ad Revenue Passes $100 Billion, Driven by Video, Mobile' (*Digital News Daily*, 7 May 2019) <https://www.mediapost.com/publications/article/335528/us-digital-ad-revenue-passes-100-billion-drive.html> accessed 10 May 2019.

enjoyed extensive growth with 23% year-over-year.

Figure 3.1: Desktop vs. Mobile Internet Advertising Revenue (Full Year Results, 100 $ Billions)

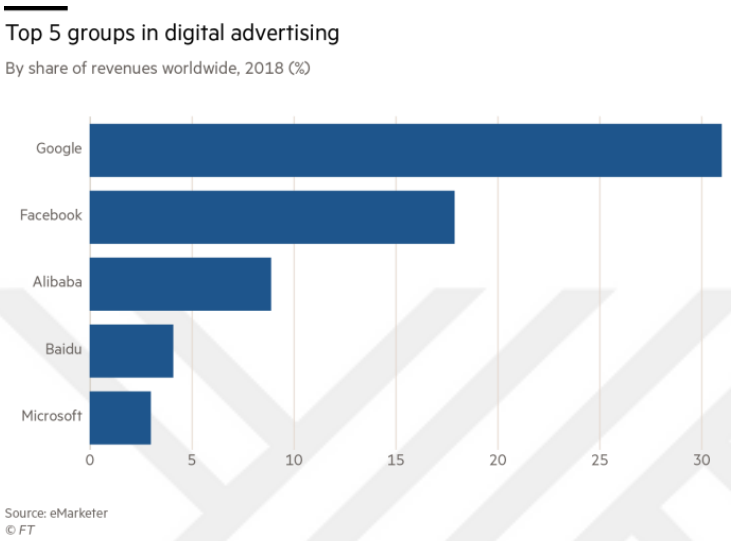


Source: Weprin (n 261).

Figure 3.2 below shows top 5 groups in digital advertising, where Google is the leader with the highest percentage of share of revenues worldwide.[277]

[277] Hannah Kuchler, 'Advertisers stick by Facebook despite privacy scandal' (*Financial Times*, 26 April 2018) <https://www.ft.com/content/eb6dac28-48e5-11e8-8ae9-4b5ddcca99b3> accessed 11 May 2019.

Figure 3.2: Top 5 Groups in Digital Advertising by Share of Revenues Worldwide, 2018 (%)



Source: Kuchler (n 277).

With regard to purposes of data collection, the answer lies at the heart of Google's business model. As previously mentioned, "Google – Android" and "Apple – iOS" ecosystems have differences resulting from the business models of these companies. Apple's business model relies largely on the hardware sales. On the other hand, Google's business model is concentrated on offering "free products and services" to its users – these free services are used as data collection instruments, supporting the data gathering, and data optimization for advertising purposes. This is otherwise known as the "freemium model" of Google.[278]

"As former Wired editor Kevin Kelly put it:

[278] For more on the freemium model of Android, see 'In-App Purchases: ABC of Freemium App Monetization' (*Medium*, 12 April 2018) <https://medium.com/@aprofita_co/in-app-purchases-abc-of-freemium-app-monetization-e742043927d2> accessed 30 March 2019.

Ubiquity drives increasing returns in the network economy. The question becomes, what is the most cost-effective way to achieve ubiquity? And the answer is: give things away. Make them free."[279]

The advertising business is what keeps Google as well as other entities providing websites, products, and services alive and in turn enables data subjects to use these without paying any fee.[280] Big data-driven companies including Facebook and Google do not charge fees for the services they provide. They promote their services as "free". As Zuckerberg stated last year in the heated hearing[281]:

"There will always be a version of Facebook that is free."

This concept of "being free" is quite misleading, users give away their data, in return, they have access to the free services, which are not exactly free – as Elvy discusses comprehensively, users came to a point where they pay for privacy in the personal data-driven economy of today's world.[282] However, the problem is, giving away so much data without being aware of it, and that this exchange is in fact against fundamental human rights.

This Chapter aims to present an overview of Google's purposes of data collection. It starts with a brief explanation of the concepts of profiling and targeted advertising by giving examples from mobile ecosystem, and concludes by presenting Google's

[279] Kelly (n 275).
[280] Google, 'Advertising – How Google uses cookies in advertising' (n 269).
[281] Transcript of Mark Zuckerberg's Senate Hearing (*The Washington Post,* 10 April 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senatehearing/> accessed 30 March 2019.
[282] Stacy-Ann Elvy, 'Paying for Privacy and the Personal Data Economy' (2017) 117(6) Columbia Law Review 1369-1420 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3058835> accessed 24 March 2019.

non-commercial motives.

3.1. PROFILING

Profiling involves classifying individuals and putting them into categories in relation to "personal characteristics", which can be "unchangeable" (such as weight or eye colour) or "changeable" (such as daily routines, movie choices, favourite travel destinations).[283] Profiling involves data mining through which data subjects are categorised based on the individualities and characteristics that can be observed (the ones that are noticeable, apparent) - to be able to make accurate and useful deductions, of course, with an undeniable possibility of error, as well as other characteristics of data subjects which are not noticeable, or in other words, observable.[284]

The GDPR explicitly refers to profiling and Article 4 (4) defines it as

> *"Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person."*[285]

Also, pursuant to Article 22 of the GDPR, smartphone users (since they are data subjects) have the right to know how their "personal" information is being

[283] FRA, 'Preventing unlawful profiling today and in the future: a guide' (2018) 15 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf> accessed 25 March 2019.
[284] Jean-Marc Dinant, Nathalie Lefever, Christophe Lazaro, Yves Poullet and Antoinette Rouvroy, 'Application of Convention 108 to the profiling mechanism: some ideas for the future work of the consultative committee (T-PD): final version' (2008) 3 <http://www.crid.be/pdf/public/5945.pdf> accessed 30 April 2019.
[285] "…in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements," see Article 4 (4) of the GDPR.

processed when an automated decision is made about them. These automated decisions are known as profiling."[286] The GDPR also provides data subject a right not to be subject to "profiling" and "automated decision making" without appropriate safeguards.[287]

Corporations should not merely be able to explain the way the decisions are made, but also must provide a mechanism to have such activities. The GDPR addresses the term to refer to any fully or partly carried out personal data "automated processing" in order to assessing personal aspects of a data subject, including location data (Article 4(4)).[288] The GDPR does not merely concentrate on judgements based on profiling or automated processing; it also covers data collection performed in order to form profiles, together with the application of those profiles to individuals.[289]

Google, as one the top tracking businesses globally, engage in data processing activity that constitutes "profiling" under this definition[290]. Profiling can be effective in various situations such as services tailoring by private companies, academic research, Article 29 Working Party,[291] and outlook on online behavioural

[286] See Article 22 of the GDPR.
[287] Antoni Roig, 'Safeguards for The Right Not to Be Subject to A Decision Based Solely On Automated Processing (Article 22 GDPR)' (*Ejlt.org*, 2018) <http://ejlt.org/article/view/570/771> accessed 27 May 2019.
[288] Binns et al (n 8).
[289] See also Karl-Heinz Fezer, 'Data Property of the People—An Intrinsic Intellectual Property Law Sui Generis Regarding People's Behaviour-generated Informational Data' (2017) Zeitschrift für Geistiges Eigentum 356-57 ("*In the reality of the market, behaviour-generated informational data represents a tradable commodity and crucial asset of a booming industry in the digitized world. Being a commodity, informational data requires proprietary shaping in property law."*).
[290] Rita Heimes, 'Top 10 operational impacts of the GDPR: Part 5 – Profiling' (*IAPP*, 20 January 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/> accessed 26 March 2019.
[291] Working Party 29, 'Opinion 2/2010 on online behavioural advertising' (2010) 00909/10/EN WP171 24 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 20 February 2019.

advertising.

Even though profiling has many advantages for different stakeholders of the mobile ecosystems as much as other fields, it also touches on fundamental rights of data subjects and can possibly create menace for the enjoyment of their rights. Most of the time the tracking and profiling processes are opaque, especially resulting from the passive data collection. The data subjects might not know that they are being profiled or comprehend what is involved in such profiling to the full extent.[292] As classification is included in profiling, it may perpetuate already existing stereotypes and enable - if not trigger – "social segregation".

Another negative possible outcome of profiling concerns freedom of choice. For example, when a user opens up Chrome, YouTube, or another Google service or product, he/she will most likely see certain products such as dresses, tickets for holiday destinations, earphones, blogs, or newsfeeds because of profiling process Google carried out. Therefore, it could be concluded that profiling classifies data subjects into specific groups, or in other words, categories and quietly, without letting them know, locks them to Google's suggestions, and so, indirectly, through being profiled, data subjects' rights are also being undermined. Another example is Google Play Store, Google says "Google Play ads help you discover apps you might like"[293], helping in the meaning of choosing for the user. In practice, this is quite convenient for most users. On the other hand, it may be contended that the data subjects are given the option of choosing among the options Google chose for them,

[292] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2018) 17/EN WP251 rev.01 5 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826> accessed 21 February 2019.
[293] See more in 'Safety Centre – We do not sell your personal information to anyone' (*Google)* <https://safety.google/privacy/ads-and-data/> accessed 30 April 2019.

so they are being restricted.

Also, occasionally, profiling could result in "inaccurate predictions".[294] In other cases, it could result in "denial of services and goods and discrimination" which is not based on a legitimate justification.[295]

A store visit conversion is recorded when a user visits a business' physical store after clicking on one of the business' "Google AdWords location based ads" (within 30 days).[296] Google states on its website[297]that, if it is believed that visits to one's business' physical locations — such as hostels and brasseries— are significant for the business, the business can use conversion tracking to help itself see how its ad clicks and viewable impressions influence store visits.[298]

Google says it does not show users "personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health".[299] Moreover, Google further specifies that store visit conversions are only available to certain advertisers, excluding advertisers with sensitive location categories related to healthcare, religion, adult content, and children[300]. However, this turned out to be not true, since

[294] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292) 6.
[295] ibid.
[296] 'Store visit conversion tracking in Google Ads (AdWords)' (*Optimize Smart*) <https://www.optimizesmart.com/store-visit-conversion-tracking-google-adwords/> accessed 29 April 2019.
[297] 'Google Ads Help – About store visit conversions' (*Google)* <https://support.google.com/google-ads/answer/6100636?co=ADWORDS.IsAWNCustomer%3Dtrue&hl=en> accessed 29 April 2019.
[298] The website further informs the readers that, for the display network, an ad impression is considered viewable when at least 50% of the ad is onscreen for at least 1 second, based on Google's Active View technology.
[299] Aurelio Lopez-Tarruella, 'Google and The Law' (2012) 22 Information Technology and Law Series <https://link.springer.com/book/10.1007%2F978-90-6704-846-0#toc> accessed 18 January 2019.
[300] 'YouTube Kids Privacy Notice' (*YouTube*) <https://kids.youtube.com/t/privacynotice> accessed 30 April 2019.

recently Facebook was found to collaborate with Google for targeted advertising using the terms related to ethnicity, gender and healthcare on people's search history (via Chrome on both iOS and Android). This information is relevant under Article 9.[301]

Google's on its support website also talks about the benefits of this feature promoting its use, and unsurprisingly listing some of the benefits for businesses, such as seeing which campaigns, keywords and devices drive the most store visits to a business, as well as understanding their return on investment (ROI)[302], which allows them to make more informed decisions about their ad creatives, spend, bid strategies and other elements of campaigns.

As prescribed under Article 71 of the GDPR, "controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies, or discrimination" on the grounds of "special category data." The said measures must be utilized regularly. The use should not be limited to the design stage; it should be used continuously on a regular basis when the data subjects are being profiled.[303] Furthermore, the GDPR also urges data processors and controllers to take the necessary measures and show specific consideration as children require enhanced protection.

[301] Article 9 states as follows: *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*
[302] See Kolt (n 57) 38.
[303] Additional recommendations are listed in Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292) 31.

Children and profiling

There are additional requirements for the personal data processing carried out by data controllers that are set out by the GDPR. This includes also collecting the personal data of children. Recital 38[304] provides the reasons why children deserve additional protection.

The personal data collection as well as other ways of processing may be performed based on the exceptions provided in Article 22(2). In such circumstances, "appropriate" and "adequate" safeguards should be adopted and applied diligently. Furthermore, the GDPR requires and expects the controller to ensure that such safeguards are in place for the purposes of safeguarding and protecting the rights, freedoms, and legitimate interests of the children.[305]

Although Article 22 by itself does not make any distinction regarding the processing of children or adults' personal data carried out by data controllers and processors, the GDPR provides "that solely automated decision-making, including profiling, with legal or similarly significant effects should not apply to children"

[304] Furthermore, the GDPR refers to additional protection and underscore the fact that children deserve particular protection regarding their personal data, which is based on the possible lack of awareness the children may have about the risks and consequences as well as protections related to them and to their rights and freedoms that is reflected under Recital 38 of the GDPR. This particular protection required for processing children's personal data is also applicable in cases where such data is intended to be used for marketing – profiling purposes concerning children when services or products are presented directly to children. Recital 38 under the GDPR, which prescribes as follows: *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."*

[305] ibid.

under Recital 71 which states such measures should not concern children.

However, it must be noted that Working Party 29 opines that the above-mentioned statement does not necessarily mean that this entails an outright prohibition of processing children's data.[306] Nonetheless, it also advised for controllers not count on the exceptions listed in "Article 22(2)" as an excuse in order "to justify their processing."[307]

Article 22, itself, does not preclude controllers from taking "solely automated decisions," including profiling concerning children, on the condition that such decision does not create any legal or similarly significant effect on the child. Nevertheless, merely profiling that affects children's preferences, choices, manners, and behaviour in any way may possibly deemed to amount to have a "legal" or a likewise "significant effect" on them. The reason for this lies at the heart of the position that children have in society, representing a more "defenceless" and "vulnerable" group. This is why it is of utmost importance for entities and organisations, as a rule, to refrain from profiling this vulnerable group of society that are open to risks for advertising or marketing purposes.[308]

Also, Working Party 29 reinforces this stance by suggesting that those who deal with data should not process children's data for behavioural advertising purposes, targeting children in any possible way (directly nor indirectly) as this would exceed

[306] ibid 28.
[307] ibid. Also note that in certain circumstances where the data controller has compelling legitimate reasons to process children's data for the purposes of automated decision-making, the processing can be regarded as lawful. An example for such compelling reasons could be to safeguard rights and freedoms of the children. Such processing is relevant for apps used for education as well.
[308] 'Guide to the General Data Protection Regulation (GDPR): Children and the GDPR' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-if-we-want-to-profile-children-or-make-automated-decisions-about-them/> accessed 2 February 2019.

the limits of children's comprehension; thus, such processing would certainly go beyond the limits of legitimate processing of personal data[309] for the purposes of data protection as a fundamental right.

Also, it must be noted that children may have a tendency to be particularly susceptible in the smartphone ecosystem, and they can be more easily affected by behavioural advertising.[310]

Especially for children with learning or behavioural disabilities, profiling and targeted ads can become a real problem due to their addiction lenient nature or obsessive behaviours.[311] Therefore, Google should pay particular attention to such groups of children as well as adolescents, and keep in mind that children's use of smartphones is increasing every year and since mobile advertising is becoming more popularised and prevalent, Google should pay even closer attention to this issue.

In addition to children, processing which has a "slight effect"[312] on individuals

[309] Working Party 29, 'Opinion 02/2013 on apps on smart devices' (2013) 00461/13/EN WP202 26 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf > accessed 10 February 2019.

[310] An EU study on the impact of marketing through social media, online games and mobile applications on children's behaviour found that marketing practices have clear impacts on children's behaviour (ages between 6-12) See the reports in 'Evidence-based consumer policy' (*European Commission*) <https://ec.europa.eu/info/policies/consumers/consumer-protection/evidence-based-consumer-policy_en> accessed 30 April 2019.

[311] See also Nitasha Tiku, 'Privacy Groups Claim Online Ads Can Target Abuse Victims' (*Wired*, 27 January 2019) <https://www.wired.com/story/privacy-groups-claim-online-ads-can-target-abuse-victims/> accessed 3 March 2019; 'Smartphone Addiction: Should Children Kick the Habit?' (*Study International*, 2018) <https://www.studyinternational.com/news/smartphone-addiction-should-children-kick-the-habit/> accessed 5 January 2019.

[312] To see more details and examples on significant effect, see the separate guidelines of Working Part 29 on this issue in its 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292); also see Working Party 29, 'Guidelines on consent under Regulation 2016/679' (2017) 17/EN WP259 18 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 28 March 2019: *"Automated decision-making including profiling leading to differential pricing stemming*

normally could actually has a substantial impact on particular groups of society including people with disabilities, people from minority groups, vulnerable adults as well as children.[313]

3.2. ONLINE TARGETED ADVERTISEMENT

Data collection aiming to examine user behaviour, based on which customised advertising is positioned, is widely termed as "Online Targeted Advertising" has brought significant "benefits to advertisers since it was first proposed in the 1990s".[314] However, although it caught more attention with the development of technology, in fact, 'behavioural advertising' is quite old[315] dates back to 1960s[316].

Online advertising is offered by means of behavioural observation (behavioural advertisement) or displays of view or activity during website or app access.[317] When an advertised content is correlated with direct user interest based on words searched in a search engine like Google, this is considered as contextual

---

from individuals' characteristics or simply their personal data, could result in creating a "significant effect" in certain cases. For instance, unreasonably expensive goods or services can effectually refrain a data subject from having access or benefiting from them. Likewise, significant effects could as well be elicited or reinforced by data subjects' "actions different than the one to which the automated decision relates".

[313] Sonia Livingstone, *Children: a special case for privacy?* (Intermedia 2018) 46(2).

[314] The following terms are also used: "Online Behavioural Advertisement", "Online Targeted Advertisement", "Behavioural Profiling or Online Tracking". See Nigel Hollis, 'Ten years of learning on how online advertising builds brands' (2005) Journal of Advertising Research 45(2) 255–268 <https://www.researchgate.net/publication/4733801_Ten_Years_of_Learning_on_How_Online_Advertising_Builds_Brands> accessed 30 March 2019.

[315] Yang Liu and Andrew Simpson, 'Privacy-preserving targeted mobile advertising: requirements, design and a prototype implementation' (2016) Software: Practice and Experience 46 (12) <https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2403> accessed 20 April 2019.

[316] Agatha M. Cole, 'Internet Advertising After Sorrell v. IMS Health: A Discussion on Data Privacy & the First Amendment' (2012) Cardozo Arts & Entertainment Law Journal 30 (2012) 283–315.

[317] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292) 29.

advertisement.[318]

Also, Targeted Mobile Advertising owes most of its success to its effective use of data subjects' location information. Smartphones, as portable items with numerous sensors and network resources, are ideal tools to observe the user's location data as discussed in Chapter 2.[319]

This is important because the real-time location has the potential to enable advertisers to find consumers at particular times, for example delivering an advertisement for the nearest brasserie just after finishing the day at work.[320] Furthermore, keeping past location information can easily aid advertisers finding out about data subjects' daily lives, routines, and habits.[321] However, the recent announcement of Google saying that auto-delete feature is being introduced delimits the use of old location data to a certain extent.

The applicability of "behavioural advertisement" in data protection and privacy is contingent to instances where user profiles are constructed aiming to position

[318] Working Party 29, in its opinion on online behavioural advertisement, equally did not treat this sort of marketing/advertisement (n 291). In addition, according to the FTC Report on 'Online Behavioural Advertisement', this type of advertisement is not potentially harmful: see FTC, 'Self-Regulatory Principles For Online Behavioural Advertising' (2009) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf> accessed 30 April 2019.

[319] For example, "apps have access to users' precise locations using GPS or network location sources such as Wi-Fi and mobile towers." See Schmidt (n 3); also see Liu and Simpson (n 315).

[320] ibid.

[321] Yang Liu, 'Privacy-Preserving Targeted Advertising for Mobile Devices' (PhD, University of Oxford 2017) 14 <https://ora.ox.ac.uk/objects/uuid:c2c929cc-0931-457a-afff-d973624a356c/download_file?file_format=pdf&safe_filename=Dissertation.pdf&type_of_work=Thesis> accessed 20 April 2019.

tailored advertising.[322] This method is often described as profiling, which is characterised by Hildebrandt as follows:

> *"the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category."*[323]

In late 1990s, DoubleClick started to track and analyse users' browsing patterns using third-party cookies in order to offering targeted advertisements.[324] Through the use of the personal information gathered from data subjects' online behaviour on specific categories of content, advertisers can easily bring the most ideally "relevant"[325], in Google's words, or "useful" advertisements to data subjects.[326]

Google makes a statement on Safety Centre and says that they are paid by advertisers for placing ads and showing "advertisers how well their campaigns

---

[322] Ellison Gare, 'Profiling and Online Behavioural Advertisement under the GDPR: Has the new Regulation succeed in assuring the protection of fundamental rights without hindering innovation and economic interests in the digital economy?' (LL.M., University of Oslo 2016) 7 <https://www.duo.uio.no/bitstream/handle/10852/54586/ICTLLM-Master-Thesis.pdf?sequence=1&isAllowed=y> accessed 22 March 2019.

[323] Mireille Hildebrandt and Serge Gutwirth, *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Publishing Company 2008) 19.

[324] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum and Solon Barocas, 'Adnostic: Privacy preserving targeted advertising' (2010) 17th Annual Network and Distributed System Security Symposium <https://www.isoc.org/isoc/conferences/ndss/10/pdf/05.pdf> accessed 24 March 2019.

[325] Google uses the word "relevant" in many of its statement when requesting permission to collect data from the users or explaining its use of collected data for advertisement purposes. See more in Google, 'Safety Centre – We do not sell your personal information to anyone' (n 293).

[326] These advertisements "can match users' interests with a high level of accuracy; as such, Online Targeted Advertising significantly improves advertising effectiveness". See Liu (n 321).

worked".[327]

The objective of many of the most common trackers is behaviourally targeted advertising, through capturing demographic or behavioural information to determine their propensity to respond to specific marketing messages.[328] Profiling is delimited to a certain extent where it collides with data subjects' rights, more specifically, as explained above it is prohibited if it has "legal or significant" effects on the smartphone user. However, to weigh and identify the significance of the effect may be troublesome. This is because, as Working Party 29 underlines, in various typical cases, there can be a considerable difference in the significance of the effects on data subjects, resulting from the decisions to present targeted advertising based on "profiling."[329]

While the definition of "significant effects" is not entirely clear under the GDPR, the Working Party 29 tries to clarify it to some extent by providing advice regarding marketing purposes and underscoring certain important occasions such as intrusive profiling.[330]

There are concerns about the use of profiling in terms of sexual discrimination. Trackers can be a good example for such cases, since they can lead to such activities as Binns et al. discuss, without having the consent of the data subject. Hence, such

---

[327] *"We use data to make our services more useful and to show relevant advertising, which helps make our services free for everyone. Without identifying you personally to advertisers or other third parties, we might use data that includes your searches and location, websites and apps you've used, videos and ads you've seen, and basic information you've given us, such as your age range and gender,"* in Google, 'Safety Centre – We do not sell your personal information to anyone' (n 293).

[328] Binns et al (n 8) 1.

[329] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292) 22.

[330] ibid; *"even profiling for marketing purposes could potentially give rise to significant effects, including if it is: intrusive; targets vulnerable and minority groups, or those in financial hardships; involves differential pricing; or deprives certain groups of opportunities".*

processing through the infamous trackers could as a result be considered as breaching Article 22 - unless such profiling is required for contractual relationships, or it is allowed under another Member State's laws.[331] For instance, this recent study shows that DoubleClick (Google rebranded DoubleClick as "Google Ad Manager") was shown to target adverts for higher-paid jobs to male users at a higher rate than to female users[332]. This clearly demonstrates how the use of profiling can trigger, enable, and result in sexual discrimination.[333]

On IT Giants defence, Apple and Google both provide resettable, user-accessible identifiers for advertising purposes: "advertising Identifier (IDFA) on iOS[334] Advertising ID on Android"[335]. Google Play's (Android) Developer Policy Centre forbids "associating the Advertising ID with any personally identifiable information or persistent device identifiers"[336]. On the other hand, the iOS App Store

[331] See Binns et al (n 8). Many of the trackers studied in Binns et al.'s research is told to have the capacity to be used in such ways, and evidence of such practices is beginning to emerge.
[332] Amit Datta, Michael Carl Tschantz and Anupam Datta, 'Automated experiments on ad privacy settings' (2015) 1 Proceedings on Privacy Enhancing Technologies 92–112.
[333] While web-based price discrimination has also been documented by numerous studies. See also Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove and Christo Wilson, 'Measuring price discrimination and steering on e-commerce web sites' (2014) Proceedings of the 2014 Conference on Internet Measurement Conference 305–318; Jakub Mikians, László Gyarmati, Vijay Erramilli and Nikolaos Laoutaris, 'Detecting price and search discrimination on the internet' (2012) Proceedings of the 11th ACM Workshop on Hot Topics in Networks 79–84.
[334] See 'advertisingIdentifier' and 'ASIdentifierManager' on 'Apple Developer Documentation' (*Apple)* <https://developer.apple.com/documentation> accessed 30 April 2019.
[335] 'Google Play – Monetization and Ads' (*Google Play)* <https://play.google.com/about/monetization-ads/ads/ad-id/> accessed 30 April 2019.
[336] ibid.

persistently rejects apps using "the IDFA for purposes beyond advertising"[337].

The technical workings and permitted use of identifiers on both iOS and Android have evolved and will – probably – develop even more. Platforms provide app developers with identifiers with different properties, to be used for different purposes. However, generally, these identifiers are designed to assist the developers and app providers rather than being user facing. In the context of users exercising their legal rights, Norvel *et al*. contend that there is a need to heighten awareness of issues concerning data subjects' rights, and the technical ways, which can be used by data subjects, should be weighed upon.[338]

It is also noteworthy to mention that there are also some advantages of such processing for online behavioural advertising, for example, "The FTC Report on Online Behavioural Advertisement" opines that this method of advertising is not necessarily harmful, in fact, can be very beneficial for different stakeholders of internet ecosystem.[339] The Working Party 29 views the effects of this advertising

[337] "Apps which access these identifiers for different purposes than advertising "may find themselves rejected from the platform marketplace's review process". See Sarah Perez, 'Apple's Latest Crackdown: Apps Pulling the Advertising Identifier, But Not Showing Ads, Are Being Rejected from App Store' (*TechCrunch*, 3 February 2014) <https://techcrunch.com/2014/02/03/apples-latest-crackdown-apps-pulling-the-advertising-identifier-but-not-showing-ads-are-being-rejected-from-app-store/> accessed 14 April 2019. For example, in a scenario where an app requests this identifier but adverts are not enabled within that app.

[338] Chris Norval, Jennifer Cobbe, Heleen Janssen and Jatinder Singh, 'Reclaiming Data: Overcoming App Identification Barriers for Exercising Data Protection Rights' (2018) 4th Workshop on Legal and Technical Issues in Cloud and Pervasive Computing (IoT) <https://arxiv.org/pdf/1809.05369.pdf> accessed 24 February 2019.

[339] See FTC (n 318); see also 'Online Behavioural Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles' (FTC) <https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf> accessed 9 May 2019.

type similarly in a more limited scope.[340] Also, Clarke outlines that profiling is utilized by businesses and organisations, predominantly to spot users who are possibly to be susceptible to offers of products and services, but also to identify "staff-members and job-applicants relevant to vacant positions".[341]

"The Report of the Norwegian Data Protection Authority" indicates that profiles are currently constructed based on a collection of information from user search history, social media activity, pursuit of online news resources, online products and registered user/customer information.[342] As such, profiling widely makes use of Big Data processing attempting to discover relational information and patterns. Various online parties, most of which unknown by active online users, become intertwined as a result of the construction of profiles and subsequent positioning of tailored advertising. Advertisers, ad network providers, and publishers become key stakeholders in the placement of behavioural advertising.[343]

3.2.1. Personalization

Online advertising, the pillar of the online "free" content, is a revolution for the marketing business. The current advertising model builds upon a complicated structure with many intermediary entities and technologies whose key objective is

[340] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292); see also Hildebrandt and Gutwirth (n 323) 19.
[341] Roger Clarke, *A 'Future Trace' on Dataveillance: The Anti-Utopian and Cyberpunk Literary Genres* (Xamax Consultancy Pty Ltd 1993).
[342] 'The Great Data Race: How commercial utilisation of personal data challenges privacy' (*Datatilsynet*, November 2015) <https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf> accessed 24 February 2019.
[343] '5Rights Foundation's Response to the Information Commissioner's Call for Evidence' (*5Rights Foundation*) <https://5rightsfoundation.com/static/5Rights_Response_IC_Call_for_Evidence_v2.pdf> accessed 25 February 2019.

to deliver personalized ads.[344]

The online shopping platforms and the emergence of mobile app shopping enable the shops to show consumers different prizes in other words to deliver personalized pricing. Personalized pricing in such context stems from the people's different characteristics, which is reflected on the personal data collection for the goal of categorising the consumers. This overall triggers price discrimination.[345] The GDPR is applicable only if personal data is processed; Borgesius and Poort adamantly argue that discrimination occurs when prices are personalized. GDPR aspires "to compel entities to be more transparent around data collection and usage"[346], which denotes that the shoppers must be informed in cases of personalization of prices before asking for their consent.[347]

The GDPR is aimed to empower data subjects to have more control over their personal data and enjoy their fundamental rights.[348] However, to be able to benefit from personalization, one must give up his/her stance of not sharing data. This is because personalization requires data. In the effort to personalize campaigns, offers

[344] José Estrada-Jiménez, Javier Parra-Arnau, Ana Rodríguez-Hoyos and Jordi Forné, 'Online advertising: Analysis of privacy threats and protection approaches' (2017) 100 Computer Communications 32-51 <https://www.sciencedirect.com/science/article/pii/S0140366416307083> accessed 18 March 2019.

[345] *"An online shop can easily recognize customers, for instance through cookies, and categorize them as price-sensitive or price-insensitive. Consequently, it can charge price-insensitive people higher prices."* See Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) J Consum Policy <https://ssrn.com/abstract=3009188> accessed 4 March 2019.

[346] Shmuel I. Becher and Uri Benoliel, 'Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR' (2019) Consumer Law & Economics <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3334095> accessed 27 February 2019.

[347] Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) J Consum Policy <https://ssrn.com/abstract=3009188> accessed 4 March 2019.

[348] Paul De Hert and others, 'The Right to Data Portability in The GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review <https://www.sciencedirect.com/science/article/pii/S0267364917303333> accessed 12 May 2019.

or (more generally), shopping experiences, retailers need to collect, store, combine and analyse data about shoppers.

Google provides personalized services, including ads and content. Google does this through using the data it collects to customize their services for users, including but not limited to making recommendations, providing content that is personalized based on the characteristics of the specific individual, and customized search results. Moreover, Google Play collects information like apps the user has already installed and videos he/she has watched on YouTube to use it for making suggestions for the new apps that the user is likely to use.

In Ad Settings, Google states that "it facilitates for data subjects to control what data they use to personalize ads to them" and even in CNIL case Google adamantly contended that the data subjects' consent are to be taken for ads personalisation[349]; however, the Restrictive Committee found the information on processing operations for the ads personalization to be sporadically diluted in numerous documents underscoring the fact that such way of delivering information does not allow the data subject to be conscious of their scope".[350]

Furthermore, in "Ads Personalization" section, "it is not possible to be aware of the variety of services, websites, and apps engaged in the data processing operations (such as YouTube)".[351] Thus, the scope of data collected and combined together is not being clearly conveyed to the data subjects. Consequently, as it was approved by CNIL the "so-taken" consent fails to be "specific" and "unambiguous".[352] The

[349] Google, 'Safety Centre – We do not sell your personal information to anyone' (n 293).
[350] CNIL (n 132).
[351] ibid.
[352] 'CNIL Fines GOOGLE €50M for GDPR Violations' (*The GDPR Guys*, 2019) <https://gdprguys.co.uk/cnil-fines-google-50m-gdpr-violations/> accessed 11 May 2019.

details regarding consent will be further discussed in Chapter 7.

The data subject has to click on the button "More options" to access the configuration for ads personalization, where the display of the ads personalization is pre-ticked. According to GDPR, consent is "unambiguous" only with a clear affirmative action from the user. Therefore, in this case the pre-ticked box would definitely not satisfy the consent requirements expected to be fulfilled under the GDPR.[353]

Google gives the option to turn the ads personalization off, or deactivate personalized ads altogether. However, still, the user is obliged to see the ads, but they will most likely be "less relevant."[354]

A data subject is left no option other than performing many actions and combines numerous document resources in order to fully grasp the purposes and the scope of the personal data collection carried out by Google for personalized ads. Firstly, they must read the Privacy Policy, before clicking on the "More options" button and then on the "Learn more" link to show the page "Personalized advertising."[355] Subsequently, the data subjects will therefore "have access to a first description of

[353] ibid; see also in its original source, CNIL, 'Délibération n°SAN-2019-001 du 21 janvier 2019: Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC'
(2019) <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1> accessed 20 February 2019. Finally, before creating an account, the user is asked to tick the boxes "I agree to Google's Terms of Service" and "I agree to the processing of my information as described above and further explained in the Privacy Policy" in order to create the Google Account. Therefore, "the user gives his/her full consent, for all the processing operations purposes performed by Google based on this consent (ads personalization, speech recognition, etc.)". However, the GDPR provides that the consent is "specific only if it is given distinctly for each purpose".
[354] Google, 'Safety Centre – We do not sell your personal information to anyone' (n 293).
[355] CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 Of 21 January 2019 Pronouncing A Financial Sanction Against GOOGLE LLC.' (*CNIL*, 2019) <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> accessed 15 May 2019.

the processing relating to personalised advertising, which is found to be "incomplete" by CNIL."[356] In order to complete and understand the information relating to the data processed for this purpose, the user will still have to consult, in its entirety, the "Provide personalised services" contained in the "Privacy Policy"[357] document that is accessible from the "Privacy Policy and Terms of Service".[358]

3.2.2. Micro-targeting

Micro targeting has a crucial role in the exercise of fundamental rights as well as the ability to question, exchange ideas in a democratic society, as EDPS stated in its report. [359]

Amongst other methods, political campaigns use micro targeting, a particular technique employed to address the individual voter.[360] In the political context, micro targeting plays a crucial role affecting users' voting behaviour, which is proved true by Alcott et al.'s research[361]. Today, political campaigns and manipulation through the use of data and technology became a very contestable topic, recently the Spanish Data Protection Authority" (DPA), "the Agencia Española de Protección de Datos" (AEPD) issued a notification (circular)[362] on the

[356] ibid.
[357] 'Advertising Policies Help – Political content' (*Google)* <https://support.google.com/adspolicy/answer/6014595?hl=en&ref_topic=1626336> accessed 30 March 2019.
[358] CNIL (n 132).
[359] EDPS, 'Ethics Advisory Group: Report 2018' (2018) 28 <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> accessed 21 April 2019.
[360] Orestis Papakyriakopoulos, Simon Hegelich, Morteza Shahrezaye and Juan Carlos Medina Serrano, 'Social media and microtargeting: Political data processing and the consequences for Germany' (2018) SAGE Journals: Big Data & Society 5(2) <https://journals.sagepub.com/doi/full/10.1177/2053951718811844> accessed 20 March 2019.
[361] Hunt Allcott and Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' (2017) Journal of Economic Perspectives 31(2) 219.
[362] 'Spain DPA Limits the Use of Data in Political Campaigning' (*GDPR Today*, 2019)

use of political data during elections AEPD's notification sets some of the most restrictive conditions for political campaigning in Europe.[363]

Micro targeting can be in numerous forms; for example, it may reside in an e-mail to a group of friends having specific qualities or it may theoretically be involved in pricing decisions for products/services.[364] Some contend that the issue of fake news is also what stems from micro targeting and what undermines users' right to information as well as the ability to decide according to their free will without being misled.[365]

Also, smartphone ecosystem is particularly perilous for such targeting enabling the flow of contact and information by the virtue of being always carrying around the phone – higher risk of being subjected to misleading information or manipulation. For example, in mobile context, online services that have achieved "network effects" overtly[366] trapping people who feel the need to be on the phone regularly being victim of their "fear of missing out" when they do not regularly go on the app[367]. Another negative result concerning micro targeting is that manipulation can take the form of micro targeted, managed display of content that is shown as

<https://www.gdprtoday.org/spain-dpa-limits-the-use-of-data-in-political-campaigning/> accessed 12 May 2019. See also 'Boletin Oficial Del Estado' (*BOE*, 11 March 2019) <https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf> accessed 30 March 2019.

[363] ibid.

[364] EDPS (n 274).

[365] For example, see Lindsey Hilsum, 'Kenyans Bombarded with Fake News in Presidential Election' (*Channel 4 News*, 2018) <https://www.channel4.com/news/kenyans-bombarded-with-fake-news-in-presidential-election> accessed 3 May 2019. Also see Privacy International, 'Further Questions On Cambridge Analytica's Involvement in The 2017 Kenyan Elections and Privacy International's Investigations' (2018) <https://privacyinternational.org/feature/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy> accessed 7 May 2019.

[366] EDPS (n 274).

[367] See for instance Michael Hogan, 'Facebook and the 'Fear of Missing Out' (FoMO)' (*Psychology Today*, 14 October 2015) <https://www.psychologytoday.com/us/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo> accessed 20 April 2019.

"relevant" for the data subject yet which is decided to be able to increase profits for the platform.

Overall, EDPS' opinion on this topic is an excellent reflection of the GDPR's as well as EU Law's stance concerning protecting personal data. EDPS states that the objective is to necessitate the respect for the rights of the data subject simply by calling for he/she to be treated as "an individual" not merely as "a consumer" or a "user'". EDPS further highlights ethical concerns and controversial matters around the impact of "predictive profiling" and "personalisation."[368]

3.3. VALUE OF PERSONAL DATA

To explain how important and valuable data is, the following is a highly prominent comparison:

"the world's most valuable resource is no longer oil, but data."[369]

Accordingly, entities like Facebook and Google, as the leading hubs of global data, have become some of the most influential and affluent corporations in the world.[370] Specifically, Google's business liable is heavily built upon data collection

[368] ibid.
[369] It was Clive Humby who first coined the parallelism of data to oil back in 2006 to denote that data are just like crude: "It's valuable, but if unrefined it cannot really be used." See Michael Palmer, 'Data is the New Oil'" (*ANA Marketing Maestros*, 3 November 2006) <http://ana.blogs.com/maestros/2006/11/data_is_the_new.html> accessed 25 April 2019.
[370] Kate O'Flaherty, 'This Is Why People No Longer Trust Google and Facebook with Their Data' (*Forbes*, 10 October 2018) <https://www.forbes.com/sites/kateoflahertyuk/2018/10/10/this-is-why-people-no-longer-trust-google-and-facebook-with-their-data/#2b7712f44b09> accessed 10 March 2019.

and analysis of that data.[371] These corporations have amassed vast quantities of data, which "give them enormous power"[372].[373] Google's adventure throughout the years is summarised as such in Zuboff's landmark article.[374]

Zuboff describes the change in Google's strategy as such:

> *"As pressures for profit mounted, Google's leaders were concerned about the effect that fees-for-service might have on user growth. They opted instead for an advertising model."*

This novel vantage point was contingent upon gathering user data to drive big data analyses whereby patterns and algorithms could be created. These relational connections would allow Google to target and place advertising exactly according to user interest and behaviour with a unique model that was more definitive than ever before. As success allowed their revenues to explode, the model they created and adopted grew to increasingly support the Notion of extensive data collection.[375] Therefore, concepts like data science and big data analytics thrived, with Google's astounding success as their locomotive.[376]

---

[371] See Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) UCLA L. Rev. 61 606 (discussing Facebook's and Google's business models); Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) Wm. Mitchell L. Rev. 40 849 (discussing Google's business).

[372] 'Regulating the Internet Giants 4. Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data' (*The Economist*, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 23 March 2019.

[373] Stacy-Ann Elvy, 'Paying For Privacy and the Personal Data Economy' (2017) 117 CLR.

[374] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75–89.

[375] See Roben Farzad, 'Google at $400 billion: a new no. 2 in market cap' (*Bloomberg*, 12 February 2014) <https://www.bloomberg.com/news/articles/2014-02-12/google-at-400-billion-a-new-no-dot-2-in-market-cap> accessed 17 February 2019.

[376] Zuboff (n 374) 85.

Google's way of business became a public auction business, with advertisers as its main customers.[377] AdWords, which is Google's method of abovementioned algorithms to position targeted online advertising, now gathers and examines substantial bulks of user data to establish where each tailored advertisement can land. 'Googlenomics', Levy summarised the relationship between internet use, data gathered and the ad business.[378] This notion is echoed in the work of Mayer-Schönberger and Cukier, as they comment:

> *"Many companies design their systems so that they can harvest data exhaust. Google is the undisputed leader…every action a user performs is considered a signal to be analysed and fed back into the system."*[379]

Understanding this motive is key to clarify the reason behind Google's bid against competing offers to become the free Wi-Fi provider of all Starbucks cafes and its three billion customers annually.[380] The higher the amount of web users, the more extensive the pool of data gathered, and thereby the more accurate the prediction made over analysing these data sets. As algorithms have increased accuracy, the better they target the very users whose data they collect and process. Therefore, it can be said that in the initial data collection process, the quantity of information gathered is more important than its quality.

It is also significant to add that, so far, Google has not been subject to public

---

[377] For useful discussions of this turning point, see Ken Auletta, *Googled: The end of the world, as we know it* (Penguin Books 2009); Siva Vaidhyanathan, *The Googilization of Everything* (University of California Press 2011); Jaron Lanier, *Who Owns the Future?* (Simon & Schuster 2013).
[378] Steven Levy, 'Secret of googlenomics: data-fueled recipe brews profitability' (*Wired*, 22 May 2009) <https://www.wired.com/2009/05/nep-googlenomics> accessed 20 March 2019.
[379] Lanier (n 377) 113.
[380] Bill Schmarzo, 'The value of data: Google gets It!' (*EMC InFocus*, 10 June 2014) <https://infocus.emc.com/william_schmarzo/the-value-ofdata-google-gets-it> accessed 12 March 2019.

oversight over these data collection, and processing practices.[381] Google's Schmidt recently shared in a public statement his views on the possibility of a wave of public oversight, showing discontent as he intimidatingly describes the prospect as "heavy-handed regulation" and expects "serious economic dangers".[382] This letter not only portrays the lack of public oversight the company has enjoyed in its previous practices, but also stresses its general 'rightful' approach towards data collection and the empire of success it has built, upon the output of the processing of that data.

There is viable potential in the future of tremendous amount of data collection and analysis, and their direct effect on individuals' behavioural tendencies, through which extensive deductions and propositions are made about their lives.[383] As data science and data mining have become the processes through which the data gathered are made sense of, the sources from which data is acquired have also become more extensive, varied, and invasive as ever. MIT's Pentland agrees by thinking that "sensors, mobile phones, and other data capture devices" have become the "eyes and ears of a world-spanning living organism from a God's eye view".[384] Entirely amplified by the web and mobile platforms, the larger game is thereby in play. As Zuboff calls it, the world-spanning ecosystem of data surrounding individuals is a 'living organism', or an inter-operational, behaviour-modifying, market-making,

[381] Vaidhyanathan (n 377) 44-50. See also Emma Finamore and Kunal Dutta, 'Tesla Boss Elon Musk Warns Artificial Intelligence Development is Summoning the Demon' (*The Independent*, 26 October 2014) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/ tesla-boss-elon-musk-warns-artificial-intelligence-development-is-summoningthe-demon-9819760.html> accessed 14 March 2019.
[382] Eric Schmidt, 'A chance for growth' (*Frankfurter Allgemeine Zeitung*, 9 April 2014) <http://www.faz.net/aktuell/feuilleton/debatten/eric-schmidtabout-the-good-things-google-does-a-chance-for-growth-12887909.html> accessed 22 March 2019.
[383] Ioanna Constantiou and Jannis Kallinikos, 'New Games, New Rules: Big data and the changing context of strategy' (2015) 20(1) Journal of Information Technology 44-57.
[384] Alex Pentland, 'The Global Information Technology Report 2008-2009: Reality mining of mobile communications: Toward a new deal on data' (2009) World Economic Forum & INSEAD 75–80 <https://hd.media.mit.edu/wef_globalit.pdf> accessed 23 March 2019.

and proprietary God view. This notion of surveillance capitalism introduces accumulation as the new norm. Individuals, their surroundings, and relational interaction are all subject to a type of change, together with the idea of the new 'reality'. Commodified and monetised, the new reality is defined as 'behaviour'. Data collected with regard to the behaviour of the physical, of the mind and of objects have all allowed a possibility to arise. Analysing this data can now mean that the behaviour of individuals can be modified, adapted, customised, in order to maximise financial gain and power – as harnessed by the behavioural data analytics based business model fostered and encouraged by the likes of Google. [385]

3.4. NON-COMMERCIAL USE

Google also collects data for non-commercial purposes, in the sense of non-advertising use. Google says that it collects data to ameliorate its services for users. Lastly, in terms of "non-commercial" use of personal data, although Google also uses the collected data "to build better services."[386] This purpose should be considered as "trivial" since it is not the main purpose of collection.

3.5. CONCLUSION

Overall, although Google has several purposes for collecting users' personal data, the crossroad of these purposes lies at one point: personal data, irrespective of the specific purpose of collection, feeds Google. Google would not have existed if there were no collection of personal data.

[385] Zuboff (n 374) 85.
[386] 'Google Privacy Policy – We use data to build better services' (*Google)* <https://policies.google.com/privacy#whycollect> accessed 30 April 2019.

CHAPTER FOUR

4. PURPOSE LIMITATION

After looking into the purposes of personal data collection, this Chapter aims to evaluate Google's purposes for such collection in scope of one of the bedrock principles stipulated in Article 5 of the GDPR: "Purpose Limitation". As it can be deduced from its name, "purpose limitation" concerns delimiting the purposes of processing data. Pursuant to the GDPR, "all personal data should be collected for a determined, specific, and legitimate purpose".[387]

In order to carry out any "additional processing", the entities collecting and processing personal data should ensure that the "further processing is not be incompatible with the purposes specified at the outset"[388] - the purpose(s) specified in the beginning of "data collection". This basically means, "that it is not acceptable"[389] for Google to state that it needs users' data for one purpose, and then use it for something else without giving a clear prior notice or reasonable and legitimate justification.

Purpose limitation is a well-established principle that "dates back to the 1973 CoE Resolution, the 1980 OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data"[390], and "the 1981 CoE Convention for the

[387] Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49).
[388] See Serge Gutwirth, Ronald Leenes and Paul De Hert, *Reloading Data Protection Multidisciplinary Insights And Contemporary Challenges* (1st edn, Springer 2014).
[389] Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49).
[390] OECD, 'Issues Related To Security Of Information Systems And Protection Of Personal Data And Privacy' (OECD 1996) <http://www.oecd.org/internet/ieconomy/2094252.pdf> accessed 19 February 2019.

Protection of Individuals with regard to Automatic Processing of Personal Data"[391]. Prior to the enactment of the GDPR, it was also a principle of the DPD.[392] However, the GDPR enhanced the principle of "purpose limitation" by making it a "requirement" or in other words "a must" as prescribed by Article 5 (2) "Accountability". This principle is especially effective in preventing the unethical leveraging of excessive data collection through smartphone apps[393] where "special categories of personal data" are concerned. These "special categories of personal data" (as set out in Article 9) enjoy particular protections.

Unless the data have been made "manifestly public" by the person that they concern, the appropriate "legal basis" for processing personal data is "explicit consent." Therefore, this principle protects an individual's option to decide, to opt-in to whatever specific service or feature used in a service/product they decide, and further forbids an entity from automatically opt-ing a data subject in to all of its services/products, where this entails data processing purposes that far exceeds what the data subject has already opted-in to.[394]

When the purpose limitation is enforced, it prevents today's tech giants and super powered – or "data powered" players such as Google from automatically hoarding

[391] ibid.
[392] Johnny Ryan, 'Why GDPR is Kryptonite to Google & Facebook on Anti-Trust' (*Brave Insights, GDPR, Policy, Research, Security & Privacy*, 10 October 2018) <https://brave.com/vestager/> accessed 10 March 2019.
[393] Examples could be: Rachel Metz, 'Smartphone app monitors mental health status' (*Privacy International*, 15 October 2018) <https://privacyinternational.org/examples-abuse/2513/smartphone-app-monitors-mental-health-status> accessed 23 February 2019; 'Best Mental Health Apps For Sleep in 2019' (*Mobile App Daily*, 3 May 2018) <https://www.mobileappdaily.com/best-mental-health-apps-for-sleeping> accessed 23 February 2019. It must also be noted that over time, the interest in the topic of data collection in fields such as both physical and mental health (including psychology and neurology) has significantly increased, and is considered by individuals in other disciplines as a useful resource as opposed to legal experts.
[394] Ryan (n 392).

and controlling personal data that they collect for one purpose in one business in another business[395], to the disadvantage of their competitors or new entrants[396].

Also, more importantly, concerning data subjects' rights and Article 5 principles, these tech giants – in this case, Google – are making a collection and accumulation of data that exponentially increase year over year on an incomprehensible scale. With the exceptional power the use of this data for different purposes brought, Google can be said to have become the "Big Brother" of today's world, known for its discovery of the exploitation of the new commodity, or so to speak, the new "oil": "data".[397]

The principle of purpose limitation is highly relevant for evaluating personal data collection carried out by Google when taken into account the considerable amount of data it gathers on its users with the help of mobile operating systems and through its own services installed on smartphones. As discussed in earlier Chapters, Google collects data through various ways and uses them for more than one purpose – generally, the purpose of data collection is to provide services free of charge, where Google currently uses that very data with the purpose of its own profit-making through its advertisement business.

This Chapter starts with a brief introduction explaining the principle of purpose

---

[395] ibid.
[396] See 'Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising' (*European Commission Press Release Database*, 20 March 2019) <http://europa.eu/rapid/press-release_IP-19-1770_en.htm> accessed 27 March 2019; 'Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine' (*European Commission Press Release Database*, 18 July 2018) <http://europa.eu/rapid/press-release_IP-18-4581_en.htm> accessed 27 March 2019; 'Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' (*European Commission Press Release Database*, 27 June 2017) <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> accessed 27 March 2019.
[397] Zuboff (n 374) 85.

limitation and its importance, after which it focuses on Google's data collection on smartphones by giving relevant examples. Lastly, it concludes that the information collected by Google on mobile operating systems far exceeds the key purposes of data collection services. The principle of transparency, data minimisation, and accountability are also briefly mentioned in this Chapter for the purposes of this thesis due to their strong interlink with the purpose limitation.

4.1. DEFINITION

According to "Article 5(1)(b) of the GDPR, purpose limitation requires that personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".[398] This means in general that processing of personal data[399] in the EU requires a plainly defined purpose at the time of data collection, and that such data cannot be re-used for a different purpose that is incompatible with the first purpose.

The full definition of purpose limitation under Article 5 (1) (b) of the GDPR states as follows:

> *"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical*

[398] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89 Sec. 1 GDPR, not be considered to be incompatible with the initial purposes, see Article 5 Section 1 (b) GDPR.
[399] Marcelo Corrales, Mark Fenwick and Nikolaus Forgó, *New Technology, Big Data and the Law* (Springer Publishing Company 2017).

> *purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes."*[400]

Also, it is noteworthy to recall that "Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, in line with the purpose limitation."[401]

There are two widely accepted "exceptions" to purpose limitation principle: it is acceptable if data processing is done:

> *"(1) with the consent of the data subject, or (2) by the authority of law; however, these exceptions can generally be abused and misused."*[402]

The consent threshold is of utmost importance for the purposes of this thesis, since data subjects' consent is used as a legal basis by Google to justify certain grounds

---

[400] *"Other sources of law also provide for purpose limitation, for example: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose in Organisation for Economic Cooperation and Development.* See OECD, 'The OECD Privacy Framework' (2013) 14 <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 13 February 2019; also see, *"Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes,"* in CoE, 'Convention 108+: Convention for the protection of individuals with regard to the processing of personal data' (2018) Art. 5 (4)(b) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 13 February 2019; Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49) 38.

[401] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, *The Principle of Purpose Limitation and Big Data* (Springer Publishing Company 2017).

[402] ibid.

for its data collection[403], or defends its data collection practices[404].

Accordingly, in the landmark decision of CNIL[405] delivered in January 2019, the following was stated:

> *"the protection of the individual's fundamental rights and freedoms overrides Google's legitimate interests to collect such a large database, and no contract justifies this large combination of data. Google empowers itself to collect vast amounts of personal data about internet users, but Google has not demonstrated that this collection was proportionate to the purposes for which they are processed."*

Determining the reasons behind and the drive for which the processing of personal data will occur is vital as it contributes to the implementation of other principles such as transparency and data minimisation through forming the backdrop for clarifying the scope of such processing, and therefore indirectly contributing to the essences of data protection by treating the personal data as a fundamental right. Put differently, "the purpose of processing personal data is the foundation of the purpose limitation principle[406] as it permits to determine whether the principles of

[403] Examples as such can be given: 'We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy,' and 'with your consent we'll share personal information outside of Google when we have your consent.' For example, if you use Google Home to make a reservation through a booking service, 'we'll get your permission before sharing your name or phone number with the restaurant'. 'We'll ask for your explicit consent to share any sensitive personal information'. See 'Privacy & Terms' (*Google)* <https://policies.google.com/privacy?hl=en-US#infocollect> accessed 27 March 2019.
[404] The penalty was imposed by CNIL. Also, see CNIL, 'Working Party 29: Letter to Google' (2012) <https://www.cnil.fr/sites/default/files/typo/document/20121016-letter_google-article_29-FINAL.pdf> accessed 28 January 2019.
[405] ibid.
[406] Marit Hansen, Jaap-Henk Hoepman, Ronald Leenes and Diane Whitehouse, *Privacy and*

data minimisation, accuracy, and storage limitation are being respected."[407] Thus, it could be concluded that the existence of purpose limitation and its proper application would prepare a strong base for and contribute to the main objectives of other basic principles such as data minimisation.[408]

This key principle exists to "limit processing of data through an IT system"[409] to its initially identified purpose; to ensure purpose limitation if different kinds of data are collected, therefore, processed for different purposes; to implement "internal rules for the assessment of compatibility needs on a case-by-case basis[410] to allow a change of purpose; to communicate clearly and plainly to data subjects any change of the mainly specified purpose of collecting their data."[411]

In practice, the principle of purpose limitation urges entities (in this case, Google)

> *"to be clear about what their purposes for processing are from the beginning, to record the processors' purposes as part of their documentation obligations and specifically*

Identity Management for Emerging Services and Technologies (Springer Publishing Company 2014).

[407] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017) 89.

[408] 'Guide to the General Data Protection Regulation (GDPR): Principle (c): Data minimisation' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/?q=%22data+minimisation%22> accessed 2 February 2019.

[409] Working Party 29, 'Opinion 03/2013 on purpose limitation' (2013) 00569/13/EN WP203 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 10 February 2019.

[410] ibid.

[411] EDPS, 'Guidelines on the protection of personal data in IT governance and IT management of EU institutions' <https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf> accessed 16 February 2019.

state them in their privacy information" for data subjects." [412]

According to this principle, Google "can only use personal data for a new purpose if either this is compatible with its original purpose and Google gets consent, or it has a clear basis in law."

This discussion is strongly linked to the transparency and consent notions that will be further discussed in detail in the following Chapters.

4.2. WHY IS PURPOSE LIMITATION IMPORTANT?

The "purpose limitation principle" is the "cornerstone of data protection"[413] in the general implementation of "data protection rules" and compliance with these rules. More specifically, both transparency and accountability are "central elements of the purpose limitation principle", for the reason that having a clearly communicated specific purpose for processing enables data controllers to be transparent both to regulators and data subjects about how they use personal data, thus ensuring the accountability of companies processing personal data.[414]

In addition, this principle has strong links with data minimisation, which will be further discussed in Chapter 5. Also, in terms of data protection and privacy rights, being compliant with this principle as well as showing compliance for the purposes of the "accountability", introduced under "Article 5 (2) of the GDPR", is of utmost importance.

---

[412] Working Party 29, 'Opinion 03/2013 on purpose limitation' (n 409) 18; see also Lee Bygrave, 'Data Privacy Law: An International Perspective' (2014) Oxford University Press 5(1) 153.
[413] ibid.
[414] ibid.

Purpose limitation is "vital for the protection of fundamental rights to privacy and data protection" as well as devices' security in technical sense, which, again, indirectly contributes to the enhancement of these fundamental rights. This is because, when the necessary measures are taken with diligence, the security of the mobile phones would be safeguarded at least to a certain extent, which, in return would allow the data subjects enjoy the smartphone ecosystems, feeling safer leaving the last years' notorious, not-trustable cunning, sneaky image behind and move on in mobile technologies. There is also a peril apropos of the disregard for the purpose limitation in the smartphone ecosystem. One of the compelling reasons for this is that personal data collected by apps can be extensively transferred to several third parties for purposes that are not material.[415] There is an obvious tendency and trend developing towards data maximisation and the elasticity of specific purposes for which personal data are collected further contribute to data protection risks found within the current smartphone app ecosystem[416].[417]

Especially, in the smartphone ecosystem, purpose limitation can minimise the indicative privacy risks to a substantial extent, including excessive collection and sharing of data. An example for this could be the data collected from numerous sensors of smartphones that are activated without actually need.[418] As part of the effort to minimise this risk, a recent set of provisions have been made in order to "particularise and complement the general rules on the protection of personal data", explaining that previous regulations have not been keeping up with the pace of "the

[415] Working Party 29, 'Opinion 02/2013 on apps on smart devices' (n 309) 6.
[416] ibid.
[417] 'Data Protection Guidelines on Apps' (*Data Protection*) 3 <http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Guidelines%20on%20apps.pdf> accessed 19 February 2019.
[418] David Nield, 'All the Ways Your Smartphone and Its Apps Can Track You' (*Gizmodo*, 4 January 2018) <https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704> accessed 19 February 2019.

evolution of technological and rapidly emerging market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality", particularly focusing on the effects "in relation to electronic communications".[419]

4.3. YOUTUBE EXAMPLE

The app in question initially has a purpose to allow users to share videos with each other. However, the app developer decides to change its business model and merges its users' account information (contact information such as e-mail address) with the phone numbers of users of another app. The respective data controllers would then have to separately approach all data subjects and ask for their prior express consent for the novel purpose(s) of personal data processing[420].

For example, as it is the number one preferred app, Google's champion in mobile devices, taking YouTube app as an example, to be able to get the finest YouTube experience, Google asks its users to upgrade to the most up-to-date version of the app. With app version 12.13, the data subjects have to accept new app permissions before updating to Android OS versions 5.0 and 5.1.[421] Google informs the user that he/she will see a notification asking the user to accept these new permissions, which will allow YouTube to have these permissions. The app will accordingly present

[419] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - 6467/19' (n 13) 7.

[420] 'Opinion 02/2013 On Apps on Smart Devices' (*Pdpjournals.com*, 2013) <https://www.pdpjournals.com/docs/88097.pdf> accessed 11 May 2019.

[421] For some versions of Android (versions 5.0 and 5.1) the YouTube app includes new permissions to enable new features and improvements. Google Play Store requires that these permissions are accepted before updating the app. If the new permissions are not accepted, the upgrade will not proceed and the app will not be updated beyond its current version. See in 'YouTube Help: Update the YouTube app for Android 5.0 and 5.1' (*Google)* <https://support.google.com/youtube/answer/7370539?hl=en&co=GENIE.Platform=Android> accessed 24 February 2019.

the user with new features and improves his/her viewing experience.[422] When apps require new permissions, Android versions 5.0 and 5.1 will prevent auto-update, so that the user has a chance to review the new permissions before accepting the update. As such, auto-update will resume after the permissions are accepted. This practice is compliant for the purposes of Article 5, which prescribes respect to data subjects' rights.

Android versions 5.0 and 5.1 include new permissions, which require the user's acceptance, whereby the user is not given the option of using the updated version of the app without consenting to all of the permissions asked for by Google. Newer versions of Android request permissions[423] as the user makes use of the app[424], in place of accepting when updating. However, if the user does not want to accept the permissions, he/she can continue using the current version of the YouTube app.

4.3.1. Why does YouTube need these permissions?

Google informs that the new permissions enable new features, which improve users' visual and practical experiences, and sets forth-specific "examples" of these benefits. Google states, "see examples below", which implies that the below given details are solely some "examples", which can translate to the fact that there may be other permissions given, of which the "improvement from permissions" are not listed.

Another possible interpretation could be that, below given permissions are the only ones which the user is directly asked for and gives permission to – and perhaps that

[422] ibid.
[423] 'Google Play Help: Review app permissions through Android 5.9' (*Google)* <https://support.google.com/googleplay/answer/6014972?co=GENIE.Platform%3DAndroid&hl=en> accessed 7 March 2019.
[424] 'Permissions' (*Android Source)* <https://source.android.com/devices/tech/config/runtime_perms.html> accessed 7 March 2019.

there are no other permissions Google needs for which the explicit permission of the user is not necessarily a ‘must’.

However, for the second interpretation then, there might be other “improvement from permissions”, while the below listed are only examples to these improvements, possibly meaning that there are others.

Figure 4.1: Google’s “Improvement from Permissions”

Permission	Improvement from Permissions
Record audio	Enables video recording and live streaming within the app.
Precise location	Allows you to more easily attach location information to your videos and live streams. Also allows for features such as improved recommendations and ads. Your precise location is never shared with advertisers.
Read contacts	Helps find people for you to share videos with.
Receive SMS	Simplifies additional verification of your phone number that you need to access some advanced features, including live streaming, long uploads, and sharing.
Send SMS	Enables sending an invitation to share via SMS.
Read	Allows YouTube to optimize the experience for some mobile data plans, which include special rates for video.

phone number	
System alert window	Allows video live streaming from other apps, such as mobile games.

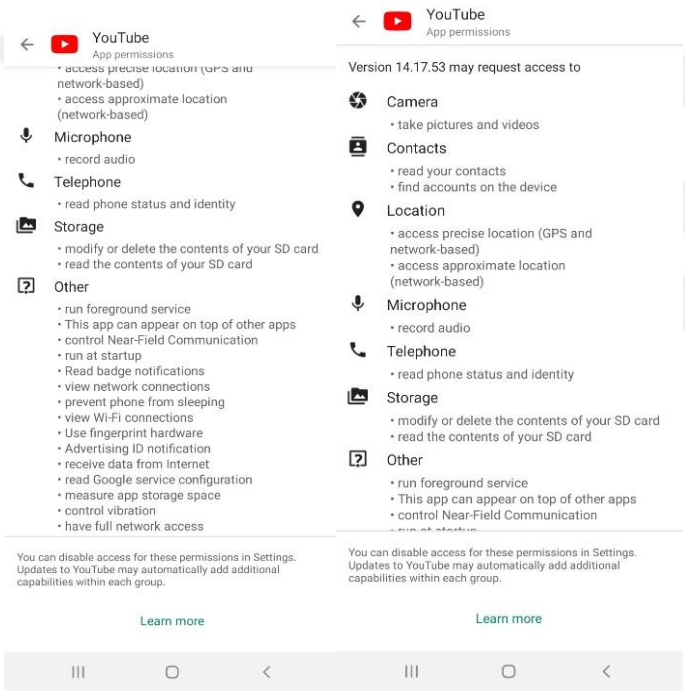
Source: Google, 'Improvement from Permissions' (n 370).

YouTube is an app that provides online services for video streaming and sharing to its users. However, as it can be seen, the YouTube app, as well as the website, is used to collect data as well. For instance, the YouTube app can be used without approving location information to be 'on' for the app, as it acquires the user's IP-geolocation information, checking the smartphone's regional settings. YouTube also uses other users' data to makes the overall YouTube experience "better" for a user, offering the concept of "using data to make Google services more useful for you" as addressed to its users, where its practices of data collection and analysis are key. The experience is improved as YouTube selects content that the user wants to watch based on what he/she, as well as what others with similar viewing histories, watched before.

Therefore, it could be inferred that: if a user wants to allow Google to access his/her data, only for the purpose of seeing more relevant ads, but not for his/her data to be used for other purposes, the user does not have the explicitly stated option of selecting what the user consents to his/her data being collected for. Google adds that it receives "cues about what is trending" based on what users are viewing, and accordingly shows the user specific videos that he/she would be interested in. Considering this app is automatically turned on when a Google account is created,

it is safe to say that users, indeed, do not get much of a say in what purposes they do or do not approve for their data to be collected and used. These are not explicitly stated with explanation for each different kind of data collected. Overall, it could be argued that YouTube not only collects more data than necessary, it also does not proactively allow the user with an extent of options to decide on what, and what not, to approve.

Figure 4.2: Google Play's YouTube App Permissions



Source: Samsung Galaxy A10 2019 Screenshots

Similar to the case of YouTube, some mobile applications provide location services allowing the user to find nearby pubs that offer discounts. However, the data collected is also used to build a profile on the data subject for marketing purposes - to identify their drink and food preferences, routines, or lifestyle in general. The data subjects expect their data to be used to find pubs, but not to receive adverts for

pizza delivery only because the app has found out that they arrive home late. This further use of data subjects' location data may not be compatible with the purposes for which it was collected in the first place. This is why the new purpose thus urges Google to ask for consent of the data subject in question.[425]

> *"Whether this additional processing is compatible with the initial purposes for which the data was collected depend on a different factor, including what information the controller originally provided to the data subject." These factors[426] are reflected in the Article 6(4) of the GDPR are as follows:*
>
> *"the relationship between the purposes for which the data have been collected and the purposes of further processing; the context in which the data were collected and the reasonable expectations of the data subjects as to their further use; the nature of the data; the impact of the further processing on the data subjects; and the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects."*

4.4. CHALLENGES

Mobile apps entail particular "risks not only to privacy, but also to security"[427] stemming from "their nature, as well as the overall context of mobile app

[425] See Leenes et al (n 258); also see Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292).
[426] Working Party 29, 'Opinion 03/2013 on purpose limitation' (n 409).
[427] See David Wright, Michael Friedewald, Yves Punie, Serge Gutwirth and Elena Vildjiounaite, *Safeguards in a world of ambient intelligence* (Springer 2010).

development."[428] Accordingly, this is not only creating security and privacy risks, but also put the core principles stipulated in Article 5 at stake. "When an app collects personal data, it needs to have a specific legitimate purpose for such collection and for that reason must notify and inform the data subject regarding the collection."[429] Although the prevalence of the smartphones and the increasing shift from PC to mobile devices is emerging every single day while users are in ever-await for a new product to be introduced, or a major breach to occur on twitter, this non-exhausted and in fact hyper nature of the field creates an ever- ecosystem where different stakeholders are going one step further in different senses – one in terms of technology as well as awareness of the legal implications of personal data collection, privacy, security etc.

Further processing for other purposes is only allowed on the basis of a specific set of criteria in "Article 6 (4) of the GDPR". "It is still common that application developers collect data on the basis of broadly construed general purpose." This practice is for sure not sufficient to the full extent in order to comply with the GDPR's requirements. Accordingly, for example, processing personal data "to provide the service and develop new features and future services" is too general to be able to be compliant with the legal requirement of purpose specification.[430] This is also applicable to the Google's terms and Services since when looked at the app.

However, hiding behind the excuses of providing a better service and developing new features for future services should not be considered as compelling reasons, because, in most cases, this can be a gateway for evading the probing questions of explaining the purpose of data collection in detail, especially for separate data that

[428] ENISA (n 18) 17.
[429] ibid.
[430] ibid.

Google collects.

Purpose limitation has strong bonds with the principle of data minimisation, which will be discussed in the following Chapter. Kane and Thurm's research shows that "lots of apps abundantly collect data from smartphones"[431] without need and without any significant liaison to app's main functionality.[432] To be able to prevent the abundant data collection and unnecessary data processing, "app developers must prudently consider which data"[433] they actually need in order to perform the main desired functionality. However, this might also constitute a challenge. Third parties obtaining access to user data through the apps must respect the principles of purpose limitation and data minimisation[434]. On another note, unique, often unchangeable,[435] device identifiers should not be used for the purpose of interest-based advertising and/or analytics.

Data subjects should also be provided the technical ways to check statements about stated purposes, by letting the data subjects' access to information regarding the extent of outgoing traffic for each app, in relation to user-initiated traffic. The plainly explained information provided enabling user controls are significant features to safeguard and enhance the application of the principles of data minimisation and purpose limitation, and consequently, accountability.

---

[431] Scott Thurm and Yukari Iwatani Kane, 'Your Apps Are Watching You' (*The Wall Street Journal*, 17 December 2010) <https://www.wsj.com/articles/SB10001424052748704694004576020083703574602> accessed 12 March 2019.

[432] ibid.

[433] Raffaele Zallone, 'Here, There and Everywhere: Mobility Data in The EU (Help Needed: Where Is Privacy?)' (*Digitalcommons.law.scu.edu*, 2014) <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&amp=&article=1576&context=chtlj> accessed 8 May 2019.

[434] Working Party 29, 'Opinion 02/2013 On Apps on Smart Devices' (n 309).

[435] It is important to note that ADID/IDFA on both Android and iOS are resettable. The user can limit tracking, however how aware most users are of this option, is open to debate.

Indeed, there is an attractive convenience to the power that subject data analysis brings, specifically in the advertisement business, which is universally evident. In Facebook's case, the Court has taken into account that, an advertising funded social network generally needs to process a great amount of personal data. However, Bundeskartellamt held that "the efficiencies in a business model based on personalised advertising do not outweigh the interests of the data subjects when it comes to processing personal data from sources outside of the social network".[436] This applies in particular where users have insufficient control over the processing of their data and its allocation to their Facebook accounts.

Similarly, the same could be argued for Google. Although the business models of both companies are different in some ways, they have their similarities: Their impact on shaping market behaviour is highly similar, in that their services are in globally prevalent use, they hold a vast number of active users, and they intensely engage in online ads.

Academics adamantly contend also provide compelling reasons with real-life problems concerning different countries, Naranjo suggests that there is a need for a globally recognised data protection law.[437] Kunt also underscores the urgent need for a globally accepted and understood approach – finding the middle way between different legal systems and values, cultures of various countries globally. He further points out the fine balance between the consumer and e-commerce focused approach as opposed to the over protection over data protection and privacy as fundamental rights, "reflecting the respective public policies" and "nature" of the

[436] 'Facebook, Exploitative business terms pursuant to Section 19 (1) GWB for inadequate data processing' (*Bundeskartellamt*, 2019) B6-22/16 <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4> accessed 9 May 2019.
[437] 'Protecting Personal Data World Wide: Convention 108' (*EDRi*) <https://edri.org/protecting-personal-data-world-wide-convention-108/> accessed 8 May 2019.

countries. Therefore, for companies such as Google, which are omnipresent, have to adapt and respect different legal systems since there is no international standard concerning data protection. Bringing an international standard to data protection laws would not only enhance and strengthen the position/weigh of the right to data protection, but also would promote equal treatment globally (of data subjects), which Google could contribute to the best since not only because it is everywhere, but also because it is the perfect opportunity to use its position and power for something good – leading this break off. Therefore, compliance, striving for understanding the essences of the GDPR, rather than memorising and staying on guard against the EU data protection laws, it could make a new definition frame breaking – game changer role privacy.

Another point to consider in above case was that, pursuant to the guidelines of the data protection board, Facebook, as a dominant company, has bargaining power over its users and is in a position to impose far-reaching data processing conditions, which users cannot prevent as they have no additional control mechanisms. This is why, due to its dominant power, data processing to the extent at hand cannot be justified without the users' voluntary consent. Voluntary consent to their information being processed cannot be assumed if their consent is a prerequisite for using the Facebook.com service in the first place.[438] The same is applicable for Google, as it will be discussed in Chapter 7.

Having mentioned these current examples as part of today's data-amassed reality, it is noteworthy to state that, even prior to GDPR, the principle of purpose limitation required that personal data may only be collected and processed for specific and legitimate purposes.

[438] ibid.

As such, this principle was, in fact, present beforehand. The same applies to personal data being collected by entities that then widely distributed this data to a number of third parties for undefined or elastic purposes[439] such as market research. The same tormenting disregard is shown for the principle of data minimisation, which will be discussed in the following Chapter.

As mentioned above, the indicative privacy risks of excessive collection and sharing data in smartphones are menaces to the data subject's fundamental rights to privacy and data protection. For GDPR compliance purposes and according to ENISA's report, app providers/developers who want their app to be run on both iOS and Android platforms should use the data for a specific purpose that the data subjects have been made aware of and no other, without further consent. [440]

In addition, if the personal data is used for a different purpose(s) other than the original purpose, they must be "anonymised" or the data subjects must be clearly notified[441] and accordingly a new consent is necessary once more for the new purpose(s).[442]

Going into the idea of 'one or more purposes', what comes to mind is that 'the whole is more than the sum of its parts.'[443] Esayas uses the term 'individualistic' in terms of being engaged in a system constructed from numerous components, one emphasizes the constituent (individual) parts of the system, contrasted with the system as a collective whole. In terms of EU data protection rules, this issue of 'individualistic nature' arises when an organisation collects or in any way processes

[439] Kindt (n 47).
[440] ENISA (n 18) 22.
[441] ibid.
[442] ibid.
[443] ibid. "This is often attributed to Aristotle, although others are also credited for it"; see Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 117.

personal data for numerous purposes.[444]

The use of the term 'purposes' (plural) pursuant to Article 5(1)(b) of the GDPR[445] entails that personal data can be collected for more than one purpose. In such cases, the Article 29 Working Party requires that "each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose complies with the law".[446]

The key argument in Esayas' research is that this "individualistic" approach fails to be adequate in an era where companies process personal data for multiple purposes, where more or less every use of the service or product generates personal data, and where data are combined across several processing activities. This is partly because the individualistic approach is based on the underlying assumption that there are well delimited, separate processing activities carried out for separate purposes, with every piece of data fitting into those delineated and delimited specific boxes of processing activities.[447] However, when the ever-growing commercial value of personal data is taken into consideration, this assumption is a half-truth at best.[448]

Going back to the practical implications of the purpose limitation, the 29 Working Party's Opinion on purpose limitation should be recalled, where it is clearly noted that:

> *"when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of*

[444] Samson Y. Esayas, 'The idea of 'emergent properties' in data privacy: towards a holistic approach' (2017) 25(2) International Journal of Law and Information Technology 139–178.
[445] CoE, 'Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC' (2016) OJ L119/1.
[446] Working Party 29, 'Opinion 03/2013 on purpose limitation' (n 409) 12, 16.
[447] Esayas (n 444) 139.
[448] ibid 139-140.

> *individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking[449] and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."*[450]

"In light of this, Google would have to seek consent for various data processing purposes appropriate to its respective business interests if it were to comply with the purpose limitation principle."

For example, consider Google's various advertising businesses:

1. "All personalised advertising[451] on Google properties including "Search", "YouTube", "Maps", and "the websites where Google provides advertising" should

---

[449] *"This stickiness is due to the tracking IDs and other information specific to you and your device, which is routinely included in ad auction "bid requests". Tracking IDs and other personally specific information are not strictly necessary for ad targeting, but they make it easy for companies to re-identify and profile you."* See Johnny Ryan, 'Update on GDPR Complaint (RTB Ad Auctions)' (*Brave*, 2019) <https://brave.com/update-rtb-ad-auction-gdpr> accessed 14 February 2019.

[450] Working Party 29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP217 47 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 10 February 2019.

[451] 'Advertising Policies Help: Personalized advertising' (*Google)* <https://support.google.com/adwordspolicy/answer/143465?hl=en> accessed 23 March 2019; also note that even users who are not signed out receive personalised search results, as described in Brian Horling and Matthew Kulick, 'Personalized Search for everyone' (*Google Blog*, 4 December 2009) <https://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html> accessed 23 March 2019.

require that users opt-in. The services that should "be affected include targeting features of AdWords such as "remarketing",[452] "affinity audiences",[453] "custom affinity audiences",[454] "in-market audiences",[455]"similar audiences",[456] "demographic targeting",[457] "cross-device tracking"[458], "customer match", which target users in general and users with similarities, based on the data provided by advertisers[459]; some of these products may share common purposes, but people should have to be asked to opt-in to many separate processing purposes before Google can necessarily rely on all of these products.

2. "Location targeting"[460]and "location extensions" are "technologies in Google Maps that enable advertising to target users based on geographical proximity." This

[452] 'AdWords Help: About remarketing lists for search ads' (*Google)* <https://support.google.com/adwords/answer/2701222?hl=en> accessed 18 April 2019.
[453] According to Google, this is "based on their specific interests as they browse pages, apps, channels, videos, and content across YouTube and the Google Display Network as well as on YouTube search results" for which, see: 'AdWords Help: About targeting your ads by audience interests' (*Google*) <https://support.google.com/adwords/answer/2497941?hl=en> accessed 18 April 2019.
[454] ibid.
[455] 'In-Market Audiences' (*Think with Google*, January 2014) <https://www.thinkwithgoogle.com/products/in-market-audiences/> accessed 18 April 2019.
[456] *"AdWords looks at browsing activity on Display Network sites over the last 30 days, and uses this, along with its contextual engine, to understand the shared interests and characteristics of the people in your remarketing list,"* in 'AdWords Help: About similar audiences on the Display Network' (*Google)* <https://support.google.com/adwords/answer/2676774?hl=en)> accessed 18 April 2019.
[457] *"When people are signed in from their Google Account, we may use demographics derived from their settings or activity on Google properties, depending on their account status,"* in 'AdWords Help: About demographic targeting' (*Google)* <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en> accessed 18 April 2019.
[458] 'Campaign Manager Help: About Floodlight' (*Google)* <https://support.google.com/dcm/answer/2823388?hl=en&ref_topic=4241549&visit_id=636927650664772867-2089473498&rd=2> accessed 18 April 2019.
[459] 'AdWords Help: About Customer Match' (*Google)* <https://support.google.com/adwords/answer/6379332?hl=en> accessed 18 April 2019.
[460] 'AdWords Help: Target customers near an address with location extensions' (*Google)* <https://support.google.com/adwords/answer/2914785?hl=en&ref_topic=3119074> accessed 18 April 2019.

example might not constitute a compatible purpose with the original purpose for which location data were shared by users." If so, people should have to be asked to opt-in to this business.

3. Google Marketing Platform[461] is Google's 'programmatic' advertising business, which targets specific ads to specific individuals on websites. It should require multiple opt-ins, because it involves a large number of separate processing purposes. For example, this (click "Learn More") is an "inexhaustive list" of purposes that are currently pursued by the industry (note that many are probably unlawful, and few are openly acknowledged).

Purpose limitation requires that people should be asked to opt-in to each of these purposes, and may have to do so in multiple contexts before Google can process personal data for this business. If, however, users have manually chosen to "sign in" to Google Search, Google may argue that the purpose of these technologies is "compatible" with purposes users agreed to, and hope to use an opt-out rather than an opt-in. Having said that, Google did not give users a choice in this matter. It recently introduced a policy wherein users of Google Chrome are automatically signed into all Google businesses as mentioned above. Following a loud user outcry, Google announced a partial reversal of the 'auto opt-in-to-everything policy' on 26 September, announcing that the next Chrome update will give users an opt-out.[462] However, for the reasons outlined above, this opt-out is hardly an adequate or lawful solution. Purpose limitation in this context should mean that Google cannot leverage its dominant position in one business such as YouTube to

[461] Other companies and app developers use Google's GMP products, partially or fully, either in embedding or integrating them into the products or services they offer.
[462] Zach Koch, 'Product updates based on your feedback' (*The Keyword by Google*, 26 September 2018) <https://www.blog.google/products/chrome/product-updates-based-your-feedback> accessed 19 April 2019.

leverage a data subject's data in another business such as Shopping.

4.4.1. Suggested areas of work

Purpose limitation has the potential to be a useful and proportionate tool to enhance data protection and prevent undue cross-market dominance. There are two areas that merit attention if this potential is to be realised.

First, the individual purpose must be firmly defined, so that anti-competitive conflation of manifold purposes can be clearly identified and addressed. What a "purpose" is has not yet been strictly defined. The definition is absent from the GDPR, and from the previous Data Protection Directive. In its 2013 opinion on "purpose limitation", the Article 29 Working Party of Member State data protection authorities made progress towards a definition: a purpose must be "sufficiently defined to enable the implementation of any necessary data protection safeguards," and must be "sufficiently unambiguous and clearly expressed".[463]

The test for judging what a single purpose is appears to be (quoting the 2013 opinion): "If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable."[464] One reading of this is that a purpose must be describable to the point the processing of the data should not surprise the person who gave consent for that data. The concern, however, is that this may not be specific enough to clearly define where a single purpose begins and ends, or to protect against the conflation of separate purposes as one 'catch-all' purpose. Also worrying is that the 2013 opinion on purpose limitation observed that, it is generally possible to break a 'purpose' down into a number of sub-purposes. Without further guidance, this could provide a pretext for the hiding of

[463] Working Party 29, 'Opinion 03/2013 on purpose limitation' (n 409) 12.
[464] ibid 13.

various purposes under an umbrella when they should actually be presented clearly and in a granular way. This would risk unexpected use of personal data by the controller or by third parties, and subsequently in loss of data subject control.[465]

Second, the competition and data protection authorities should together consider whether there is adequate enforcement of the purpose limitation principle. Google and Facebook are prime candidates for enforcement and should be unable to use the personal data they process for the purpose of providing their service for other purposes without user permission. Nevertheless, in reality, they do currently use a 'service-wide' opt-in for almost everything. Although competition is outside the scope of this thesis, it is still worthy to mention due to its heated momentum in today's mass media and debates.

4.5. CONCLUSION

Yesterday it was PCs, today it is smartphones, and tomorrow it can be something else. However, the approaches taken in the application of purpose limitation should be applicable to developing technologies unless the priorities of the society or authorities' change. When the smartphone ecosystem, particularly Android, is evaluated in light of the key principle of purpose limitation, there are issues that clearly violate data protection rules. For most apps, the "end user," to use an app, is required to give in to provide all the necessary permissions; if not, there is no guarantee that the app will function well. However, focusing on the practices of Android platforms, the pre-installed or OEM (original equipment manufacturer) apps in Android are automatically granted all the required permissions.[466]

The rapidly changing and developing mobile technologies, the mass generation,

[465] ibid 12, 53.
[466] Julien Gamba et al (n 245) 9.

collection, and analysis of personal data are proofs to show that these principles are important and relevant more than ever. The goal of processing and the projected usage of personal data should be plainly and evidently indicated and further explained to the data subjects. If the data is processed for a purpose other than the initial one, the smartphone user must be "sufficiently informed and a legal ground for this processing should be determined".

As such, data exploitation is a big problem of today's world especially in smartphone ecosystems, not only because users increasingly integrate phones into every aspect of daily life, but also even in cases of lower smartphone use, these devices are 'smart' enough to act on their own, informing their creator and owners while seemingly "dormant"[467], as discussed previously in this thesis.

However, regardless of the outcome, it is unmistakeable that devices and software are designed facilitating the data exploitation. The data-driven world frees them to gather any and all data, pursuing patterns and similarities, generating intelligence, making decisions that shape countless individuals' futures, who arguably are not ready for what is already being built. As the technologies everyone unquestioningly uses are insecure and leaking data, legislation is not yet able to address these risks. In turn, almost no one's data is entirely secure.[468]

Where the processing of personal data confers extra profits and is convenient to be used for more than one purpose, this usage of the same data collected should not inevitably translate to being legitimate based on Google's business model and its

[467] Jack Morse, 'Your Android phone pings Google a lot more than you might think' (*Mashable*, 22 August 2018) <https://mashable.com/article/google-android-data-collection-study/> accessed 29 March 2019; 'Safety Center – Data Privacy' (*Google)* <https://safety.google/privacy/data/> accessed 29 March 2019.
[468] Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49) 5.

corporate structure, as Alphabet being a parent company offering a multitude of other products and services.[469] Therefore, this section concludes that the principle of purpose limitation should be better leveraged to combat bundling, offensive leveraging, and other anti-competitive behaviour by dominant digital businesses.[470]

Finally yet importantly, it is crucial to underscore the fact that the reliance on consent should not "negate" the obligation on data controllers to comply with Article 5. Even when relying on consent, data controllers should warily consider, through different ways such as a data protection impact assessment any prejudice to the rights of data subjects resulting from the data collection or any other way of processing and take steps to alleviate any and all risk of a violation of these rights.[471]

[469] EDPS (n 274).
[470] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292) 11.
[471] See ENISA (n 18) 56.

CHAPTER FIVE

5. DATA MINIMISATION

Data minimisation[472] ensures that processors and controllers only process the minimum amount of personal data they need to fulfil a particular purpose. Although data minimisation is not a new concept in EU law[473] and in international law[474], it has recently become one of the most soaring topics of discussion following the enactment of the GDPR. This is linked to the GDPR's introduction of accountability, and the severe fines relevantly imposed by the GDPR starting to show its teeth. Additionally, data minimisation has a pivotal role in the protection of personal data for the purposes of its legal processing, while complementing purpose limitation, transparency, and accountability.

Businesses that benefit from profiling, low-cost storage rates, and most importantly, the opportunity to process tremendous amounts of data can easily encourage tech giants to continue with their excessive personal data collection. Most entities do this, literally 'hoarding' as much information as possible, thinking of the future, in case the data gathered proves to be useful in time. For example, Menchen-Trevino underscores the challenges faced in understanding and addressing this issue, in that large-scale patterns become possible to detect, whereby analyses like the following can be deemed possible. Although, not for commercial purposes, Song et al found out that, looking at previous location history and movement tendencies upon studying smartphone location data, an individual's future location is, in fact, 93%

[472] ibid 17; also see Article 5(1)(c) and Recital (39) of the GDPR for Data Minimisation.
[473] Also see 1998 Act UK – adequacy concept.
[474] OECD states that "Personal data should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date." See also Convention 108 [Article 5 (4) (c)].

predictable, even despite great variation in individual patterns.[475] This approach, for sure, contradicts with data minimisation purposes.[476]

This Chapter aims to evaluate Google's personal data collection on smartphones through examples, and to underscore the intersection between data minimisation and purpose limitation, creating a strong relationship with reference to transparency and consent, and with a focus on the scope of the GDPR while referring to other relevant laws (including the upcoming ePrivacy regulation) where necessary. General remarks referring to current technical challenges related to data minimisation in mobile applications will be discussed, aiming to draw attention to the existing gap between ever-developing mobile technologies and the already adopted data protection legal framework. Last but not least, in addition to these technical details strongly attached to data minimisation, randomly selected opinions from relevant case law will be briefly presented. As a result, a concrete picture will be drawn regarding data minimisation and purpose limitation notions for the purposes of accountability, in terms of the practical application and impact of data minimisation in the mobile ecosystem.

5.1. DEFINITION

This Chapter evaluates Google's personal data collection in light of data minimisation set out in Article 5(1)(c) of the GDPR, stipulating:

[475] Chaoming Song, Zehui Qu, Nicholas Blumm and Albert-László Barabási, 'Limits of Predictability in Human Mobility' (2010) Journal of Science 327(5968) 1018-1021 <https://science.sciencemag.org/content/327/5968/1018> accessed 30 March 2019.
[476] Ericka Menchen-Trevino, 'Collecting vertical trace data: Big possibilities and big challenges for multi-method research' (2013) Policy & Internet 5(3) <https://onlinelibrary.wiley.com/doi/abs/10.1002/1944-2866.POI336> accessed 30 March 2019.

> *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".*

In general, data minimisation ensures that personal data is adequate, relevant, and not excessive for the purpose. Furthermore, this principle limits personal data selected to process, to a processing, which is directly appropriate for the initially specified purpose. Lastly, it considers and makes use, if feasible, of privacy-enhancing technologies paving the way for and even directly enabling the avoidance of excessive usage of data subjects' personal data, or allowing to utilize anonymised data.[477] However, it must be noted that it is not an obligation to minimise data processing to an absolute minimum, but rather a requirement to minimise data collection onto a sufficient scale with regard to the purposes of processing.[478] Accordingly, as Voigt states, this requires an evaluation of the proportionality of envisaged processing activities.[479]

This principle is highly relevant for the purposes of this thesis, since it responds to privacy risks, which data subjects may face in the mobile ecosystem. This is because, especially due to the use of third-party libraries[480] on mobile operating systems, there is a high risk of excessive processing[481]. As mentioned above, Android is a Google product, but it is also much more than that. Android is Google's Trojan horse[482], a metaphor which implies the fact that, the more data it collects,

[477] EDPS, 'Guidelines on the protection of personal data in IT governance and IT management of EU institutions' (n 411) 1-36; ENISA (n 18) 17.
[478] Voigt and dem Bussche (n 407) 90.
[479] ibid.
[480] See Ryan, 'Update On GDPR Complaint (RTB Ad Auctions)' (n 449).
[481] As stated in the indicative privacy risks in ENISA (n 18) 17.
[482] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 1-704.

the more dominant and strong its position becomes.[483] In fact, Android acts as Google's instrument for data collection, facilitating Google's data collection practices, for instance, through pre-installed apps[484].

For the purposes of the GDPR, when Google's business model and the amount of data it collects on mobile operating systems (especially on Android OS) is taken into account, the tech giant's data collection, whether assisted by its 'Trojan horse'[485] or another one of its services, definitely falls under the scope of data minimisation. This is because Google acts both as a controller, and as a processor, ("the fact that it collects data suffices for Google to be considered a processor"). Article 5 requires Google to be transparent and show that the data collected is adequate, relevant, and limited to what is necessary, relevant to the purposes of processing.[486]

This principle, in fact, delimits the scope and amount of data collected through Android, and compels Google to question the relevance of the data, while triggering to identify the extent and purposes of the collection, which reinforce the notions of

[483] Alexandre de Corniere and Greg Taylor, 'On the Economics of the Google Android Case' (*Oxford Law Blog*, 31 August 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/economics-google-android-case> accessed 2 April 2019.
[484] Also see for further competition law and economics perspective for pre-installed apps: Julien Gamba et al (n 245).
[485] John Naughton, ''The goal is to automate us': welcome to the age of surveillance capitalism' (*The Guardian*, 20 January 2019) <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> accessed 20 February 2019; also, for a discussion on Google's emergence and data collection aggravation see Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (n 374) 30.
[486] ENISA (n 18) 17.

privacy and data protection.[487]

Data processing must be limited to what is necessary to realise a legitimate purpose. This is highly relevant especially for the "Web & App Activity" feature, not merely because it "tracks" data subjects and processes personal data (such as "location data"), but also because it constitutes one of two services that Google automatically enables without explicit user consent in the process of setting up a new Google Account. Google's lack of requirement of user consent to enable its 'Web & App Activity' tracking automatically eliminates "consent" as a potential ground for its processing activities. This will be discussed thoroughly in Chapter 7 under "Google's Privacy Policy - Data Subjects' Rights".

However, it must be noted that even if Google could have logically based its personal data collection and processing on 'consent', this does not negate the obligation of complying with the bedrock elements in Article 5.[488]

Noting the following is important: While stating that personal data must be limited to what is necessary in relation to the related purposes, the principle of data minimisation appears to be stricter than in the DPD, as the latter states in its Article 6(1)(c), that personal data must not be excessive in relation to the purposes.[489] Google's new feature of "auto-deleting location history" is a perfect example where

[487] ibid; also see Working Party 29, 'Opinion 02/2013 on apps on smart devices' (n 309). As Article 29 Working Party describes: "*Purpose limitation goes hand-in-hand with the principle of data minimisation. In order to prevent unnecessary and potentially unlawful data processing, app developers must carefully consider which data are strictly necessary to perform the desired functionality."*

[488] As Privacy International argues: *"Reliance on consent should not negate the obligation on data controllers to comply with the data protection principles including transparency, fairness, purpose limitation, and data minimisation. Even when relying on consent, data controllers should carefully consider (for example through a data protection impact assessment) any prejudice to the rights of individuals as a result of the processing, and take steps to mitigate these"* (n 49).

[489] For the purposes of Recital 39 and Article 5(1)(c) of the GDPR, the slightly stricter principle of data minimisation requires, particularly, ensuring that the period for which the data are stored is limited to a strict minimum.

this can be observed. This also reminds that data minimisation does not necessarily mean collecting less data or a small amount of data, but it is rather about how the processor treats the data, and ensures that only a necessary amount of data is collected for the initial purpose the processor has in mind, of which the data subject is informed. Purposeful data collection must be proportionate, so in other words, the system – being able to collect data - should not be abused.

Consequently, the processing of personal data should only take place when the purpose of processing cannot be reasonably realised, or in other words, fulfilled through other means. To be able to ensure that the collected data is not kept longer than it is necessary, time limits must be set by Google, either for erasure or for a periodic review.[490] Here, with the latest features Google brought – as discussed in Chapters 1 and 2 – Google becomes closer to be in good terms with data minimisation, purpose limitation principle, and therefore, the GDPR.[491]

New findings such as this open up further possibilities for comparison and the need to comprehend the context of these patterns: Are locations more or less predictable among individuals with different socio-economic circumstances?[492] What are the

[490] Andreas Wiebe and Nils Dietrich, 'Open Data Protection: Study on legal barriers to open data sharing – Data Protection and PSI' (2018) OpenAIRE by the European Commission 173 <https://www.ouvrirlascience.fr/wp-content/uploads/2018/09/Data-protection-Study-on-legal-barriers-to-open-data-sharing_wiebe_.pdf> accessed 28 April 2019.

[491] Also, it should be noted that data processing may not disproportionately interfere with the interests, rights and freedoms at stake. Only data processed should be that which is "adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed" pursuant to Article 5(1)(c) of the GDPR. The categories of targeted data must be necessary to achieve the declared aim, overall, of the processing operation, and a controller should strictly limit the collection of data to information that is directly relevant for the specific purpose pursued by the processing. This also the case under Article 5(4(c)) of the Modernised Convention 108.

[492] An example of the effect of growth of the mobile ecosystem and its implications on a unique socio-economic context is detailed in the following source: Daniel Miller, 'The Unpredictable Mobile Phone' (*UCL Anthropology*) <https://www.ucl.ac.uk/anthropology/people/academic-and-teaching-staff/daniel-miller/unpredictable-mobile-phonei> accessed 29 April 2019.

key differences between the most and least predictable? So on and so forth. Even with a small amount of data, it is possible to make numerous discoveries about a smartphone user[493], further demonstrating how attentive processors should be when collecting data. If limitless, unqualified, and causeless collection of data becomes the norm, as a result of which, the essence of the rights to privacy and data protection can be severely torn down.

5.2. WHY DOES THE DATA MINIMISATION PRINCIPLE MATTER?

This principle obliges those processing data to consider the scope of the data that can be identified as the minimum amount of data necessary to be able to achieve the specified purpose.[494]

Building on countless examples of IoT and data connecting every aspect of physical life, data minimisation becomes more relevant and in fact vital than ever before. Changes in tech industry is drastically improving analytical techniques in order to look for, use, and aggregate huge data sets to be able to cultivate heightened intelligence, from which the most unique insights can be obtained. With the assumption that collecting more personal data will enable better accuracy in predicting people's behaviour, there is a continued interest and motivation to hoard massive amounts of data to expand the sample size. Thus, an urgent need to challenge this narrative appears in order to guarantee sole use of data, which is

[493] See Henk Fernee, Nathalie Sonck and Annette Scherpenzeel, 'Data collection with smartphones: experiences in a time use survey' (2013) The Netherlands Institute for Social Research 2,8 <https://ec.europa.eu/eurostat/cros/system/files/NTTS2013fullPaper_204.pdf> accessed 28 April 2019.

[494] CNIL, 'Compliance Package: Connected Vehicles and Personal Data' (2017) 1-35 <https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_en.pdf> accessed 30 April 2019. Processors should hold merely that specific amount, and no more, as it is not acceptable to collect extra data by justifying that it may be useful in the future. For instance, processing precise and detailed location data for connected cars for a purpose concerning technical maintenance or model optimisation can be considered as excessive.

needed and appropriate for a particular purpose, must be collected, and utilized.

5.3. THE SMARTPHONE ECOSYSTEM

This section focuses on building upon the data minimisation principle in the context of the mobile platform. Google, for example, in its Privacy Policy does not explain nor mention that usage of location data (processing) in 'Web & App Activity' is essential and/or indispensable for its proper working. There is also no mention whatsoever in other statements, and in fact, not even in its blog posts, which are publicly accessible on the website. Indeed, the fact that users can switch off ("pause") this feature proves that Google's data collection and processing are not indispensable. Put differently, since the user is allowed and can technically pause the 'Web & App Activity' feature, this in itself indicates that Google's data collection is not necessary. Therefore, Article 6(1) (b) ("Lawfulness and Processing") cannot constitute a valid legal ground in this example.[495]

As it can be seen, data minimisation is interlinked with the purposes of lawfulness and processing under the GDPR. This principle is also intertwined with the purpose limitation principle, above discussed, since data processing should be done in the limits of the purpose limitation principle. Working Party 29 underscores the worrying disregard that exists regarding data minimisation in the mobile ecosystem, in the context of personal data collected by apps.[496]

---

[495] Article 6(1) provides as follows: *"Processing shall be lawful only if and to the extent that at least one of the following applies: ……. (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."*

[496] Working Party 29, 'Opinion 02/2013 on apps on smart devices' (n 309) 6. This is because, as mentioned in Chapter 4 on the principle of purpose limitation, the data collected by mobile apps may be widely distributed to third parties for undefined or elastic purposes, such as market research.

In Working Party 29's opinion given in 2013, a reference was made to 'recent' research conducted by WSJ[497], pointing out the excessive data collection by apps; ironically, 6 years later in 2019, this remains to be a topic of research and debate.

The principle of data minimisation is prescribed in Article 5 (1) (c) of the GDPR, respectively, in collecting and processing of personal data. Pursuant to Article 32 of the GDPR, app developers and OS providers should arrange and implement security measures for the protection of the data they process. At the same time, EU data protection laws also permit some exceptions. If data are disclosed to the controller, and data processing is necessary for the basic functionality of the apps, Article 6 (1) (f) of the GDPR permits processing based on legitimate interests, so long as the data subjects' rights are ensured.

Schmidt states "Android sends periodic updates to Google servers, including device type, cell service carrier name, crash reports and information about apps installed on the phone. It also notifies Google whenever any app is accessed on the phone, in that, Google knows when an Android user accesses their Uber app, for example".[498]

As explained in Chapter 1 in detail, the above given information constitute personal data and in fact may lead to identification of the data subject when numerous data are combined; therefore, as much innocent as it may seem, for the purposes of data minimisation and purpose limitation principles, Google should inform data subjects "WHY" it needs all the data – actually, each single data – for what purposes? What would happen if one of the above given information (or any other information Google collects on smartphones) is not available/cannot be collected? If the effect

[497] Thurm and Kane (n 431): *"Recent research showed that many apps abundantly collect data from smartphones, without any meaningful relationship to the apparent functionality of the app".*
[498] Schmidt (n 3) 13.

is not that substantial, then why Google collects such data? And the most relevant question is: are all data collected on smartphones such as the ones given above absolutely necessary? The precise and reasonable grounds for such collection should be made "sufficiently clear".

Unfortunately, although similar questions will be discussed and Google's practice of data collection as well as its respect for data subjects' rights will be evaluated in Chapter 7 to a certain extent rather focusing on the Privacy Policy considerations, it is still striking and in fact ironic to note that the "fully" correct answers to the above given questions can only be given in light of the information Google provides. In other words, the assessment as to whether every single data collected satisfies the data minimisation threshold and falls under the purposes of the principle, depends on the information provided by Google – unless an expert who is closely linked with Google makes such analysis.

It is astonishing to see how GDPR's principles and rules are unbelievably interconnected with each other. Here transparency steals the show: as Gonzales puts it: "At its core, transparency is indeed not about disclosing any hidden practice, or about bringing data subjects closer to anything at all, but about generating and adapting a certain data story to an imagined data reader, that is, about re-creating and triggering new accounts about data, built on some data visions." Transparency is, in this sense, about translating, and creatively transcribing and delivering to data subjects an account of what is being done to their personal data, tailored to a certain idea of what individuals might want to hear, and what they can perceive. It is about being told how you are being profiled, but in a language that inevitably betrays you were already 'being profiled' in order for controllers to decide how they would tell

you about it.[499]

In addition to these startling findings, Schmidt adds that Google can "de-anonymise such data" as previously mentioned[500]. Assuming that the study is accurate, this is also a factor that Google adamantly contends in addition to its claim that it does not track activity while the data subject is signed out of Google accounts with a user's Google account information. For example, in such cases, criticising Google would not make any sense since there is a need for proof and further explanation.

5.4. CONCLUSION

For the purposes of data minimisation and accountability (to be detailed in the next Chapter) prescribed under Article 5 of the GDPR, Google should ask itself whether the collected data is necessary for achieving the purposes of processing. The main objective of data minimisation is to achieve the reduction of data collection to the minimum possible level, fulfilling the main purposes of processing.[501] This principle is highly relevant for the purposes of this thesis, since it responds to privacy risks, which data subjects may face in the mobile ecosystem. On mobile operating systems, especially due to the use of third party libraries, there exists a high risk of excessive processing[502]. This risk is heightened with Android as a mobile OS, acting as Google's Trojan horse of both seamless and seemingly endless collection and processing of data.

Google does appear to be making an effort to be compliant to some extent, with recent developments like the auto-delete feature for 'Web & Apps Activity' and

[499] Emre Bayamlıoğlu et al, *Being Profiled Cogitas Ergo Sum* (1st edn, Amsterdam University Press BV 2018) 53.
[500] Schmidt (n 3) 20.
[501] Voigt and dem Bussche (n 407) 90.
[502] Also see ENISA (n 18) 22.

‘Location History’. However, it must be noted that Google has not been demonstrating a significant compromise. Moving from the above example, for instance, the degree of past history location’s benefits for Google is questionable, when considering the ever-updating nature of collecting data. Even with the deletion of past-accumulated data, as long as creating an endless stream of new user data is possible, the cycle is bound to continue.

This is especially the case when considering the exponentially growing value of new data generated by users today in a much more connected, data-driven world, fuelled with information of all types from a myriad of spectrums of daily life. Thus, it can be said that focusing on this future source is possibly incomparably more relevant and valuable to Google, than past data that is lost. Therefore, the need to reconcile privacy and security remains to be resolved. The gap between the technical tools and methods used for the implementation of the GDPR must be addressed by the likes of Google. As such, all entities collecting and processing user data must not only become compliant with the principles set out under Article 5, but also must openly display that compliance for the world to see, an aspiration for which ensuring data minimisation is absolutely vital.

CHAPTER SIX

6. ACCOUNTABILITY

"Accountability encapsulates everything the GDPR is about."[503] Following the adoption of the GDPR, the principles of accountability[504], data protection by design, and data protection by default became increasingly important for every data processor and controller including IT giants like Google. Accountability has become the nightmare of data processors due to the severe penalties that they may face in case of non-compliance with the principles set out under Article 5 of the GDPR.[505]

This Chapter explains the concept of accountability under the GDPR, and further discusses its importance by providing relevant examples and explanations from different jurisdictions. It then continues by presenting technical measures prescribed under the GDPR that are relevant to Google's data collection on mobile operating systems, in the context of accountability.

6.1. DEFINITION

[503] 'Data Protection Practitioners' Conference 2019 - Elizabeth Denham's speech at the Data Protection Practitioners' Conference on 8 April 2019' (*ICO*, 8 April 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/04/data-protection-practitioners-conference-2019/> accessed 28 April 2019.

[504] Similarly, OECD states that, a data controller should be accountable for complying with measures which give effect to the principles stated above.

[505] Working Party 29, 'Opinion 3/2010 on the principle of accountability' (2010) 00062/10/EN WP173 8 <https://www.dataprotection.ro/servlet/ViewDocument?id=720> accessed 10 April 2019; for more information, see Chapter 4 of Voigt and dem Bussche (n 407). The 'accountability' requirement is directly enforceable and can be fined with up to EUR 20,000,000.00 or up to 4% of the organisation's total worldwide annual turnover, as stated under Article 83 Section 5 of the GDPR. The looming fines shall increase the pressure on controllers to take the necessary steps and implement appropriate measures for data protection purposes. The principle is further specified by the different material and organisational obligations under the GDPR.

One of the biggest changes introduced by the GDPR is accountability. Different from the former DPD, the GDPR brought a novelty: a fresh data protection rule saying entities are responsible for, will be hold accountable for, and must be able to demonstrate, compliance with the principles set out under Article 5.[506]

Article 5(2) provides for accountability by stipulating as follows:

> *"the controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation' and security ('integrity and confidentiality')."*

There are two main elements that are key to the fulfilment of this stipulation. First, the accountability rule clarifies that the organisation itself is responsible for compliance. Second, it puts data processors in an important position in taking the necessary measures to be able to demonstrate their compliance. Although Google has been taking steps to comply with the GDPR, recently, despite CNIL's explicit recognition of Google's efforts in terms of accountability and compliance, Google was still fined €50 million, after CNIL determined that the company failed to comply with EU data protection laws, more specifically, the GDPR. This principle of 'accountability', as a novelty brought by the GDPR, has caught up with Google very rapidly, which triggered mass influence in the media.

[506] As explained in paragraph 5, the legislator has declared that the data protection legislation for EU institutions shall be adapted to apply the same principles, ideally at the same time. See EDPS, 'Guidelines on the protection of personal data in IT governance and IT management of EU institutions' (n 411).

Google, collecting and dealing with personal data, in its capacity as data controller or processor, is hold accountable for complying with standards, and taking measures, which give effect to the provisions, set out in the GDPR. The companies with responsibility for data processing must thereby should show how they comply with data protection rules,[507] aiming to internalise the culture of compliance within the DNA of the business, and not take a formulaic or generic approach to their GDPR obligations.[508]

As such, accountability puts a burden on corporations to comprehend the risks that they make for others as a result of their data processing, and to mitigate those risks. As the responsibilities of data protection authorities shift, the description of their profession is formalised in moving away from box ticking. Thus, data protection begins to be seen as a cornerstone that is part of the cultural and business fabric of organisations.[509]

6.2. WHY IS ACCOUNTABILITY IMPORTANT?

The accountability is key to an effective and feasible data protection framework, ensuring the proper application of the prescribed rules under the GDPR. It brings

[507] See 'Accountability and governance' (*ICO*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 27 March 2019. The main accountability for any processing operation lies with the data controller, who is the entity that determines purpose and means of data processing. The controller incurs the responsibility for this and is liable for the processing operation. The controller must also fulfil a number of compliance aspects, and must facilitate the fulfilment of data subject rights, such as the rights of the person whose personal data is controlled. Furthermore, the controller must choose the appropriate legal basis for any processing operation prior to commencing the processing, as in, before a study is conducted. Possible legal bases are consent, performance of a contract, legal obligation for the controller, vital interest of the data subject, public interest, or legitimate interest (which does not apply for public bodies carrying out a public task).

[508] 'ICO: business falling short on GDPR accountability' (*Out-Law*, 2019) <https://www.out-law.com/en/articles/2019/april/ico-businesses-fail-gdpr-accountability-/> accessed 28 March 2019.

[509] ICO, 'Data Protection Practitioners' Conference 2019 - Elizabeth Denham's speech at the Data Protection Practitioners' Conference on 8 April 2019' (n 503).

together all other principles and rules that are traced back to the essences lying at the heart of fundamental rights to data protection as well as privacy. Accountability further puts the burden on those processing data subjects' data, whether a corporation or a public body, to be held accountable for dealing with the responsibilities given under the GDPR.

In real world, technically, accountability urges entities to be more open, honest, transparent about the processing of data subjects' personal data and acts as an obstacle for those who are responsible under Article 5 not to take data subjects' lack of technical knowledge for granted for their ulterior motives. This ground-breaking rule in fact brings justice and equality to today's data driven world aiming to put those whose data are being used (in Zuboff's terms exploited "as commodity") and those who possess the tech-knowledge rooted capital of "knowing and controlling" the processing to the same level. Accountability does this by compelling those "controllers of data" and "owners of technical knowledge" – the elite exploiter class – to comply with the GDPR and respect data subjects' rights by being more open and proactive about the way in which they handle data. Also, accountability may be thought to enhance the respect for the regulators as entities such as Google are put into a position where they are expected to explain, demonstrate and prove that they respect individuals' rights to regulators in addition to data subjects.

The importance of the accountability principle is flawless when considering contexts in which there are no accountability mechanisms in place, for example, in cases where there is no structure to report breaches of the law.[510]

As an example to show the importance of accountability, South Africa can be taken

[510] Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49).

into consideration.[511] Privacy International expects things to change drastically in South Africa.[512] Although this might be an extreme example that is far from Europe's reality, it is a great example to internalise and understand why data protection principles are more widely discussed than ever and actually, why accountability becomes crucial when it comes to real cases in practical terms.

Related expectations from Google have existed for a while, and there are many cases being handled in the US as well, which address the topics of pre-installed apps, consent, and transparency as discussed in this thesis. CNIL made recommendations to Google in 2012 and 2013 as a result of similar debate, and Google has, in fact, even lost several cases due to their data collection and processing practices. However, if this issue now echoes as powerfully as it does across different disciplines and platforms, it is due to the introduction of the accountability principle.

Accountability mechanisms today play an important role in investigating breaches and holding entities subject to the law to account. After the enactment of the GDPR,

[511] ibid.

[512] Government Gazette Staatskoerant – Republic of South Africa, 'Protection of Personal Information Act, 2013 (Act No. 4 of 2013) Regulations Relating to the Protection of Personal Information' (2018) <https://www.michalsons.com/wp-content/uploads/2017/11/PoPI-Regulations-Final-14-Dec-2018-3-languages-42110_14-12.pdf> accessed 30 March 2019. For example, in South Africa, the Protection of Personal Information (PoPI) Act was adopted in 2013, providing for the establishment of Information Regulators, though this body was not put in place until April 2017. At present, data breaches in South Africa often go unreported. In 2015, it was noted that only five data breaches were registered in South Africa. See more in Privacy International, 'State of Privacy Mexico' (2019) <https://privacyinternational.org/state-privacy/1006/state-privacy-mexico> accessed 30 April 2019. Also, for an example of companies facing official review is from Uber. In 2017, following a major leak of data from taxi-hire app Uber in 2016, the Mexican National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) requested the information about the number of "Mexican users, drivers and employees" who had been affected from Uber. INAI added that it asked Uber for information on the measures it is taking to mitigate damage and safeguard clients' information. See Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49) 46-47.

the number of the cases concerning illegal data processing has dramatically increased.[513] As such, companies, including Google, make an additional effort to avoid receiving damages. However, companies should not merely make effort not to face fines but they should internalise the principles set out under Article 5. They should not only take steps for the purposes of compliance in Europe but in every country in which they operate, it should be in their DNA's to respect data protection rules – this is the only way to create an international standard.

In building the case of accountability, not only in the context of complying with the GDPR in Europe, but also national legislation[514] globally[515], accountability is the most powerful rule compelling entities to be obliged to comply – this would shift data protection laws globally if properly understood and implemented in different countries. Fortunately, the GDPR caught wind globally leading mass media, academics, and authorities to discuss accountability.

Those that process data have obligations in relation to that data, and enforcement and redress must be available when these principles, rights, and obligations are not adhered to. The GDPR is the perfect legal framework showing its teeth in cases of violation, with a magnitude that is urging other countries, including the US, to consider adopting similar rules. It is also creating an immense platform for discussion in academia. As a result, Google has dealt with several such instances, where types of redress like punitive damages were sought. This is because Google's

[513] ENISA, 'Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default' (2019) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> accessed 30 April 2019.
[514] For a discussion on the importance of accountability on a national level and its essence, see: ibid 16.
[515] Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (n 49) 46-47.

approach to data privacy and protection is often considered malicious, oppressive, and wilful[516]. Therefore, punitive damages can be said to be warranted to deter defendants, such as Google, from engaging in future misconduct.

To avoid such cases in showing accountability, communication is of utmost importance. For the purposes of Article 5 and Article 6, when personal data is being collected by Google, the extent and the purpose of this collection should be communicated to data subjects as prescribed by Article 5 of the GDPR. This communication should be performed "clearly and conspicuously"[517], or in other words, easily noticeable and understandable by regular data subjects.

Thanks to the GDPR, in June 2018, Google announced that it would stop mining emails in Gmail to personalise ads. The company insisted the case was unrelated to GDPR, and that this change was carried out in order to harmonise the consumer and business versions of Gmail.[518] Later, Google revamped its privacy dashboard, first launched in 2009, to be more user-friendly[519]. Facebook also took similar steps and announced recently that it takes users' privacy and data protection very seriously and makes it a priority. Therefore, it can be seen that, although the law currently

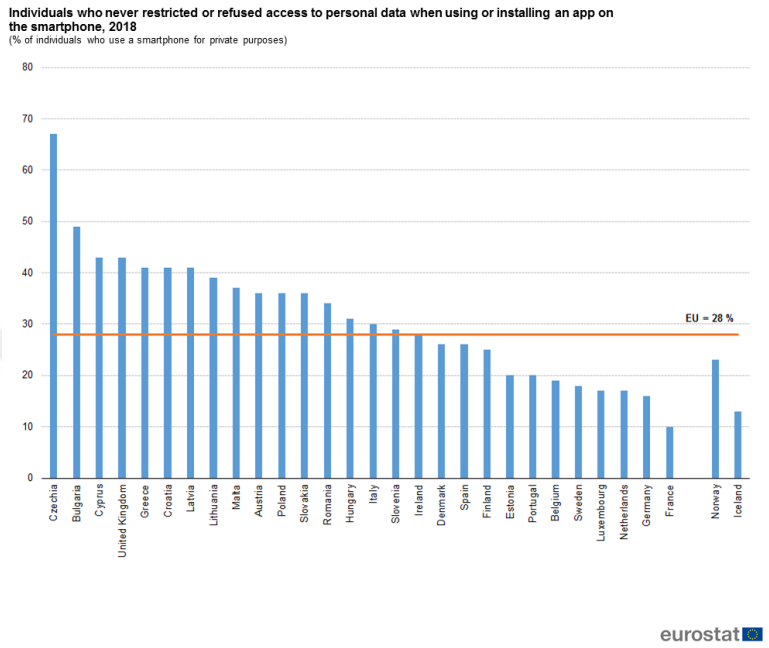
[516] Napoleon Patacsil, individually, and on behalf of other persons similarly situated, *Plaintiff, v. Google Inc.*, Defendant. FTC California Case [2018] Case 3:18-cv-5062.
[517] See US case in FTC, 'In the Matter of General Workings Inc., a corporation, also d/b/a Vulcun, and Ali Moiz and Murtaza Hussain individually and as officers of General Workings Inc.' <https://www.ftc.gov/system/files/documents/cases/1604vulcundo.pdf> accessed 20 April 2019; FTC, 'FTC Approves Final Order in Vulcun Deceptive App Installation Case' (2016) <https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-order-vulcun-deceptive-app-installation-case> accessed 20 April 2019.
[518] 'The Keyword - As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align' (*Google)* <https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/> accessed 20 April 2019.
[519] Laura Goode, 'Google's new privacy dashboard makes it easier to see what Google knows about you' (*The Verge*, 8 September 2017) <https://www.theverge.com/2017/9/8/16276000/google-dashboard-my-account-privacy-security-redesign> accessed 21 April 2019.

only applies in Europe, companies are making changes globally.

When examining how 'open' and 'proactive' service providers are, it is also interesting to look into the level of consumer awareness regarding the collection and processing of their data, where some interesting facts come into play. In 2018, 75% of people aged between 16-74 in the European Union (EU) used a smartphone for private purposes. Yet, 28% responded that, when using or installing an app on the smartphone, they never restricted or refused its access to personal data. 7% of smartphone users in the EU did not know it is possible to restrict or refuse access to their personal data when using or installing an app on the smartphone.[520] Less than one half (43%) of smartphone users reported that they had a security system that had been automatically installed, or provided within the operating system of their smartphones.

[520] 'Do you protect the personal data on your smartphone?' (*Eurostat*, 28 January 2019) <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20190128-1> accessed 15 February 2019; also see 'Trust, security and privacy – smartphones' (*Eurostat*, 2019) <appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-1021385_QID_-47A4BBBC_UID_-3F171EB0&layout=INDIC_IS,L,X,0;GEO,L,Y,0;IND_TYPE,L,Z,0;TIME,C,Z,1;UNIT,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-1021385IND_TYPE,IND_TOTAL;DS-1021385UNIT,PC_IND_MPP;DS-1021385TIME,2018;DS-1021385INDICATORS,OBS_FLAG;&rankName1=TIME_1_0_-1_2&rankName2=UNIT_1_2_-1_2&rankName3=INDICATORS_1_2_-1_2&rankName4=IND-TYPE_1_2_-1_2&rankName5=INDIC-IS_1_2_0_0&rankName6=GEO_1_2_0_1&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23> accessed 10 May 2019.

Figure 6.1: Individuals Who Never Restricted or Refused Access to Personal Data When Using or Installing an App on the Smartphone, 2018 (% of Individuals Who Use a Smartphone for Private Purposes)



Source: Eurostat (n 458).

Technology is a fact, creating awareness is a must, in light of which, Google should take more concrete action. It is normal that Google is in plain sight with regard to the discussion surrounding data privacy and protection, and cannot be justly compared to Apple, as their business models are quite different. Therefore, Google can benefit significantly from acting as one of the pioneering institutions to become known for the value they place on individuals' rights, and their public recognition of the respect they have for the provisions set forth under the GDPR. Thus, accountability could be a good place to start.

In a practical sense, this requires that Data Protection Impact Assessments be

conducted when necessary, as per the principle of accountability, and that proper records must be kept by data controllers (including app providers), detailing personal data processing activities performed by the organisation. As part of these measures, data protection by design, or by default, has become explicit obligations under Article 25(1) of the GDPR. This constitutes a crucial requirement for app developers, since the design of an app has a significant impact on the data it handles. This can be dissected by relevant authorities to determine whether appropriate privacy by design (or by default) practices are in place, upholding data subjects' rights.[521]

Being accountable furthermore allow the organisation to create confidence in individuals' minds and may help mitigate enforcement action where applicable, and Google certainly needs that trust keeping in mind the flashy headlines published over the last two years deeming Google notorious and monstrous company.

It is essential to recall that Google acts as a processor of personal data, and makes available data processing terms, "reflecting the controller-processor relationship, where required".[522] Android Enterprise is among the products where Google acts as a processor.[523] In addition to the benefits of adhering to the principle of accountability, implementing these measures can also enhance the security protection of the smartphone experience that Google so attractively offers.

6.3. TECHNICAL AND ORGANISATIONAL MEASURES

While the GDPR does not specify an exhaustive list of actions are needed to be

[521] ENISA (n 18) 20.
[522] 'Businesses and Data – We are committed to complying with applicable data protection laws' (*Google)* <https://privacy.google.com/businesses/compliance/#!?modal_active=none> accessed 28 April 2019.
[523] ibid.

taken to be accountable, it does set out several different measures that organisations can take to become compliant. It is key to note that some measures are obligatory, while some are voluntary. It will differ depending on what personal data the organisation holds, and what exactly is done with this data. These measures can form the basis of the organisation's programme controls. It is Article 24 of the GDPR, which describes that technical and organisational measures must be implemented to "assess the risks of personal data processing operations in light of the rights and freedoms of natural persons, as well as to demonstrate compliance with the GDPR".[524] These measures should be risk-based and proportionate, which should be reviewed and updated as needed.

Accountability obligations are ongoing. Investing time and energy in the compliance with accountability requirement can also strengthen the controller's understanding of and practical commitment to data protection, as the controller is responsible for implementing appropriate technical and organisational measures before beginning processing operations to be able to thwart violations of the GDPR.[525]

Executing the responsibilities for the purposes of accountability in Article 5, is not,

[524] ibid 20, 21. To ensure accountability, with respect to a general progression that organisations can follow, ENISA describes the following steps: *"Once risks have been identified and analysed, they need to be addressed by considering technical or organisational options that may remove, minimize, or mitigate them."* See ENISA, 'Guidelines for SMEs on the Security of Personal Data Processing' (2016) <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed 23 April 2019. Technical options are various and may consist, for example, in minimizing data collection and processing (necessity and proportionality), implementing transparency and accountability measures (i.e., via privacy dashboards and privacy policies), providing control mechanisms to users over their personal data (consent). Other technical options may consist in adopting a privacy-by-design approach and using privacy enhancing technologies (such as data anonymization). Finally, organisational measures, such as access control, or staff training should also be considered." See also ENISA (n 18) 24.
[525] Voigt and dem Bussche (n 407); also see Working Party 29, 'Opinion 3/2010 on the principle of accountability' (n 505).

as the EDPS puts it, merely a 'box-ticking exercise'.[526] The real demanding task relates to the practical implementation of measures. Hence, the sole path accountability can walk is when the compliance is pursued. As Hide reminds us, "Left on a shelf, the Swiss army knife or the cell phone 'does' nothing."[527] It is only when the measures prescribed under accountability rule are reflected on the routine daily practice that multifaceted negotiations between controller and users will emerge and the material – tangible shape of accountability can be seen and understood.

In terms of demonstrating accountability, the Madrid Resolution attempts to set up international standards on accountability, and notes that demonstrations should be to supervisory authorities and data subjects.[528]

Yet, the GDPR is more comprehensive. Article 5 (2) encapsulates more and reaches out to more when the essences and the main objectives of the GDPR are understood and read together with the rule of accountability. Striving to understand the implications and the scope of accountability merely by looking at Article 5 would be incorrect, a waste of time, in fact, it can be dangerous for the purposes of concrete implementation since without the rest of the Regulation, stakeholders will find themselves perplexed trying to interpret the provision, being locked to their own

[526] 'Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards' (2009) Privacy Conference 2009 <http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf> accessed 26 March 2019.
[527] Lachlan Urquhart, Tom Lodge and Andy Crabtree, 'Demonstrably doing accountability in the Internet of Things' (2018) 26(4) International Journal of Law and Information Technology 1-27 <https://www.research.ed.ac.uk/portal/files/78865742/eay015.pdf> accessed 24 April 2019.
[528] Privacy Conference (n 526).

limited understanding.[529]

Article 24 covers concepts that necessitate to be read with Art 5 (2) to be able to situate and understand the scope of data controller responsibilities. However, this thesis focuses on the main issues defining and putting into relevant context the principle of accountability.[530] Therefore, this Chapter does not go into more details.

As a processor of data, Google's general response to questions regarding its data collection and processing practices is as follows, regarding the measures taken to address its progress towards GDPR compliance:

> *"We are committed to complying with applicable data protection laws: We are always working to stay compliant, which helps make compliance easier for your business. We are audited regularly by third parties, maintain certifications, provide industry-standard contractual*

[529] See Art 24(1) GDPR. For instance, Article 24 precisely focuses on the nature of their wider responsibilities: *"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."*
[530] Urquhart et al (n 527).

protections, and share tools and information you can use to strengthen your business' compliance."[531]

6.4. CHALLENGES

The GDPR brought many significant changes in 2018, and businesses have a long way to go becoming, as well as remaining, compliant. These changes present some challenges for organisations in the face of GDPR requirements. One such change is the need for privacy by design or by default[532]. Privacy by design and by default are addressed in Article 25 of the GDPR, which this section will elaborate on.

As data privacy and protection are now an integral part of technological development, as well as how the product or service is delivered, GDPR introduces these new requirements, while not being specific about how these changes must be implemented. Thus, for many organisations, such as Google, adopting a privacy by design (or by default) approach will require a significant cultural change, as well as ground-breaking measures to be taken, both in terms of establishing new products and services, as well as amending and adapting those that are already available for public use and consumption. This will undoubtedly present a significant challenge for organisations to overcome to be able to comply with the GDPR.

To this end, it must be added that concerning the 'by default' requirement, reference

---

[531] Google, 'Businesses and Data – We are committed to complying with applicable data protection laws' (n 522). Google adds as follows: *"Publishers and advertisers who use our advertising and measurement products globally must comply with our EU User Consent Policy, and are required to collect consent from EEA users for personalized ads and use of cookies/local storage on their sites and apps. So if you're a publisher or advertiser using Google advertising and measurement services, you'll need to take steps to make sure users' preferences are respected to meet the requirements of Policy."* See 'EU user consent policy' (Google) <https://www.google.com/about/company/user-consent-policy.html> accessed 24 April 2019.

[532] Andrew Clearwater and Brian Philbrook, 'Privacy by Design and GDPR: Putting Policy into Practice' (*CPO Magazine*, 29 June 2018) <https://www.cpomagazine.com/data-privacy/privacy-by-design-and-gdpr-putting-policy-into-practice/> accessed 17 April 2019.

is made to the principles of purpose limitation, data minimisation and storage limitation. They are reflected by four criteria in "Article 25(2) of the GDPR" that characterise a data protection-friendly default structure, and should, thus, be used by controllers when defining the defaults:

Criterion 1: Minimum amount of personal data - The amount of personal data has to be the minimum for the purpose. This is linked with the data minimisation principle that is discussed in Chapter 5. This does not mean that the number of bits is reduced as much as possible. Instead, the alternatives of datasets whose collection could be less infringing, concerning the private sphere of an individual, have to be compared with each other. It could be fewer attributes of less sensitive data. Obviously the amount of personal data can be decreased, too, if the data are not, or less, personally identifiable. This could be aggregated information that yields anonymous data, or it could also be pseudonymised data where the additional information is kept without access of others.

CNIL said Google had also not made it "sufficiently clear to users where it is relying on their consent to process personal data for the purpose of personalising ads". It said consent obtained from users is not "sufficiently informed, specific enough, or unambiguous, as required by the GDPR".

After taken into account the information Google provides to users in relation to their privacy, and the configuration tools it makes available to users to allow them to control how their data is used, CNIL found the deficiencies found deprive users of fundamental guarantees concerning treatments that can reveal whole areas of their privacy in spite of Google's efforts in implementing measures. It pointed to the volume of data collected, the wide variety of services from where data is sourced, and the possibility to combine the data from these services as the reason for this.

Criterion 2: Minimum extent of the processing of personal data - The personal data processing should also be minimised according to each specific purpose, such as the limitation of whether data are stored at all, whether and how the data are analysed once or multiple times, whether the data are transferred to other recipients, whether the data are linked with other information like profiling purposes as per Article 21 GDPR. In this regard, the provision of effective tools (by the controller, in this case, Google) that can enhance the exercise of data subjects' rights is also very strongly linked to minimising the extent of the processing, while contributing to the overall empowerment of data subjects.

Criterion 3: Minimum period of the storage of the personal data - Clearly, the period of storage of personal data by the controller plays an important role. With respect to the purpose, the minimum time for storing the personal data has to be chosen. This could mean no storage at all, or an anonymization or erasure as soon as possible. Anonymization would not suffice since as discussed before in mobile ecosystems, it is very easy to combine data and identify an individual. However, erasure is a good way to comply with the criterion; Google recently announced a new feature, in fact, showing compliance with this criterion since it stated that it will no longer keep the location and activity data more than 18 months.[533]

Criterion 4: Minimum accessibility of the personal data - Accessibility in Article 25(2) GDPR tackles possible access by any entity, examples of which can be people such as other users, organisations such as the data controller or government authorities, tools such as search engines or cloud servers. The accessibility depends on where the data are stored or processed, how the access is limited by assigned access rights, whether the data is stored or processed in clear

[533] 'The Keyword - Introducing auto-delete controls for your Location History and activity data' (*Google*, 1 May 2019) <https://www.blog.google/technology/safety-security/automatically-delete-data/> accessed 5 May 2019.

text or in an encrypted matter and who could decrypt the data, who the recipients of the data are, and whether multiple copies, including not securely erased files, may exist that can be accessed by others.

The location of storage and processing is important to determine the accessibility, like the difference between local processing on a device on the user's side and the central processing on the cloud or on servers on the data controller's side. Limiting the accessibility also means to limit the storage in jurisdictions where the law allows governmental access without sufficient guarantees for the protection of personal data. Also, when emitting personal data, the range should be narrowed as far as possible concerning the purpose to prevent unauthorised accessibility. With regard to accessibility, it is interesting to note that Article 25 (2) GDPR specifies that, by default that personal data must not be made accessible without the individual's intervention to an indefinite number of natural persons. Consequently, the data controller should implement technical and organisational measures that prevent personal data from being made public by default.[534] This provision can be especially relevant in the case of social networks[535], for data sharing in an IoT scenario[536], or for data exposure via search engines[537].[538]

[534] EDPS (n 274) 12.
[535] Marit Hansen, 'Data Protection by Default in Identity-Related Applications' (2013) 3rd Policies and Research in Identity Management 4-17 <https://hal.inria.fr/hal-01470500/document> accessed 21 April 2019.
[536] Working Party 29, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' (2014) 819/14/EN WP215 23 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf> accessed 24 April 2019.
[537] International Working Group on Data Protection in Telecommunications ("IWGDPT"), 'Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy' (2013) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2013/2013-WP-Personal_Data_Web.pdf> accessed 26 April 2019.
[538] ENISA (n 18) 17-18.

From another angle, it is worth mentioning that as ENISA emphasized it in its detailed report[539], that security violations are another challenge for organisations to overcome in the process of ensuring accountability. According to the report, it is not atypical in security engineering papers for authors to equate privacy with security of personal data, and additionally, with confidentiality requirements. The report notes that even if data subjects could be safeguarded to a certain extent against numerous types of privacy violations when the majority of the security problems regarding personal data depicted in the report are fixed, many of the data protection challenges that are often related to the principles of data protection like accountability, purpose limitation, and data minimisation will not be covered at all.[540]

6.4.1. Specific rules for children[541]

Another challenge that is worthy to include in this Chapter concerns the issue of accountability regarding the protection of children's data and their rights and freedoms. If children want to use online services, they are often expected to get approval from their parent (or legal guardian). The child stops needing the parental consent once he/she is over 16 (in some EU Member States the age limit might be

[539] ibid 29.
[540] Working Party 29, 'Opinion 02/2013 on apps on smart devices' (n 309) 1. As mentioned in the previous Chapters another variable could be the nature of processed data itself. For example, as Working Party notes that referring to pseudonymising techniques to mask identities to enable collecting data relating to the same individual, without having to know his/her identity, could be beneficial in terms of reducing the risks to data subjects. These techniques thus represent important safeguards, which can be taken into account when assessing compliance. Nonetheless, the use of pseudonymous or pseudonymized data is, in itself, does not suffice in order to justify a lighter regime on accountability obligations. Therefore, not being able to benefit from such processes can be said to present another challenge on organisations working to establish accountability measures.
[541] See more in Sapna Maheshwari, 'YouTube Is Improperly Collecting Children's Data, Consumer Groups Say' (*The New York Times*, 9 April 2018) <https://www.nytimes.com/2018/04/09/business/media/youtube-kids-ftc-complaint.html> accessed 30 March 2019.

as low as 13 as allowed under Article 8 (1) of the GDPR).[542] However, specific control measures must be put in place to ensure the privacy of and protect the data of possibly the most important aspect of individuals' rights, namely children's rights.

The smart pets are becoming more popular, the use of apps by children increases in parallel with the emergence of the smartphones every day one step further. For example, the smart pet was released in 2013, and is available both on Android and iOS platforms, the app had 10 000+ installs from the Google Play store as of July 2018.[543] The results obtained in Chu et al.'s research suggests that smart pets and Internet-connected children's toys call for cyclical security and privacy measures and diligent auditing, it also calls attention to the lack of research in this area to help IoT toy manufacturers improve security and privacy development practices.[544] Therefore, as technology emerges more into children's lives, practical measures and technical solutions will always be necessary outdating themselves, requiring new measures to fulfil accountability requirements.

Also, Binns et al's[545] recent study finds that most apps contain third-party tracking, and the distribution of trackers is long-tailed with several highly dominant trackers accounting for a large portion of the coverage and the research further adds that news apps and apps targeted at children appear to be among the worst, in terms of the number of third-party trackers linked to them. Consequently, it could be argued

[542] Controls to check parental consent have to be effective, for example by using a verification message sent to a parent's email address. As an example, YouTube's terms of service hold that visitors to its main site are affirming that they are at least 13 and agree to Google's privacy policy.
[543] Gordon Chu, Noah Apthorpe and Nick Feamster, 'Security and Privacy Analyses of Internet of Things Children's Toys' (2018) IEEE Internet of Things Journal <https://arxiv.org/pdf/1805.02751.pdf> accessed 30 March 2019.
[544] ibid 1-6.
[545] Binns et al (n 8). The study notes that, as a result of this tracking feature, governments and courts are reaching a point where they can request detailed data on an individual's whereabouts.

that there are significant legal compliance challenges encountering the user tracking industry[546].

6.5. TRANSPARENCY

Although transparency will be thoroughly discussed later on in this thesis in terms of Google's privacy policies, this principle is worth being mentioned in the context of accountability. Transparency is related to the principles concerning openness and it is a prerequisite for accountability.[547]

Although many multinational technology companies have their own privacy policies, developer distribution agreements and end-user license agreements ("EULA"), a lack of transparency still exists about the nature, amount and purpose of personal (including location) data processing of smartphones. For example, there are strict procedures that app developers must follow before they qualify to sell their apps in the Apple App Store. Users of iPhones do not have any option but to agree with the terms and conditions of Apple, and in most cases, the users do not know about the nature and volume of their personal data that is processed when installing and using apps on their iPhones. In case of iOS, it is only possible to turn location services on or off. If location services are turned off, then according to Apple, no location data is collected by Apple (that is, no GPS, WiFi or GSM information), nor is any data made available to apps. Here it is important to note that there is a possibility to track users' location without the use of GNSS, WiFi or GSM. On the other hand, where the user has turned location services to on, then Apple receives

[546] Ryan (n 449): *"This stickiness is due to the tracking IDs and other information specific to you and your device, which is routinely, included in ad auction bid requests. Tracking IDs and other personally specific information are not strictly necessary for ad targeting, but they make it easy for companies to re-identify and profile you. This processing is not compliant with the purpose limitation and data minimisation principles prescribed under Article 5 of the GDPR, one of the bedrock principles which will be discussed in Chapter 5."*
[547] ENISA (n 18) 48.

anonymous location and WiFi data, and also chooses whether to determine location by GPS, WiFi, GSM or some other means. There is no way to 'opt out' of this data processing when location services are turned on.

In this regard, the total system for monitoring and processing location data involves ambiguity and lack of transparency and accountability, keeping it based on user trust to the OS and app developers with regard to the nature, extent, and means of the whole process. Even app approval processes of multinational technology companies, such as Apple and Google and their EULAs, is based on one-sided terms and conditions, irrespective of international or regional data protection principles. This raises the question on how giant technology companies can disregard international and regional norms of privacy and data protection in their collection of user data. According to ENISA's report, "these OSs, using infrastructure such as GPS or Wi-Fi to provide location services while not being transparent about exactly what data are being tracked, should be held legally accountable if they violate European data protection law. Such aspects require that the international community collaborate to ensure a safer, more transparent mobile ecosystem."

6.6. PRIVACY RISK MANAGEMENT

Privacy risk management is one of the major elements of GDPR and ePrivacy legislation in general. In particular, Recital 75 GDPR addresses the risks to the rights and freedoms of natural persons that could occur as a result of personal data processing, potentially leading to physical, material or non-material damage, such as discrimination, identity theft, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Correspondingly, Recital 75 explicitly mentions as a risk, processing of sensitive personal data, of children's data, of large amounts of data, or a large number of data subjects. This is highly

relevant when taking the endless extent of personal data collected on smartphones into account.

6.7. CONCLUSION

There is more personal data that data subjects need to protect or can protect, both in the collection of this data, as well as its processing. This, now and in the future, makes the responsibility much greater for data-driven organisations like Google.

Data protection compliance is never a one-size-fits-all, or a single one-time policy document. The nature of what amounts to personal data, and the activities for which such data can be processed, are ever changing. Due to which, organisations need to be constantly on alert with regard to compliance issues and changes, while being aware of the challenges they can face, so that new policy and measures can be established to ensure open, clean and rapid progress in the face of GDPR requirements.[548] Although data protection laws may seem like a rigidity, a burden, or a hoop to jump through, they actually present a data model that can be most beneficial to organisations in the long run. Taking responsibility for how personal data is handled, and demonstrating the steps taken to protect individuals' rights, not only result in better legal compliance, but also offer a "plus" point in terms of competition. Owning and showing accountability create a real opportunity demonstrate, and even prove, how an organisation respects the privacy of others. Building an image of sensibility, of trust, and of compliance, can only be advantageous to its legacy. Furthermore, in case of any risk of compliance, then honestly and transparently being able to show that risks were actively evaluated, and measures and safeguards were put in place accordingly, this could provide

[548] Paul Lambert, *The Data Protection Officer: Profession, Rules, and Role* (Auerbach Publications 2016) 57, 58.

mitigation against any possible enforcement action. In reverse, if an organisation cannot show good data protection practices, it may find itself exposed to fines and reputational harm.[549] When the downside is considered, the price to pay for the road to compliance is quite negligible. The need for transparency and accountability is now more vital than ever, not only for the organisation, but also for the user. Looking at it from the user perspective, clicking to accept murky terms of service screen when it appeared to be a "no-brainer". The upside was incredible convenient, and the downside, it seemed, was just some annoying shoe advertisement following the user around the web. Nevertheless, past years have shown how that same personal data has been weaponised to target individuals with their own data for financial purposes, tailor content in exploit of their behaviour, and even in some political situations, radicalise specific segments of a population or suppress political beliefs to sow division. Personal data can be, and is, used to influence behaviour, and determine what products individuals see, what services they have access to, and what prices they pay, both financially and with respect to having their rights infringed.[550] To cut a long story short, the GDPR is an opportunity to flip the inner workings of the smartphone data collection ecosystem. Since the emergence of the web, companies have been financially incentivised to hoard data and turn it to money later. Today, data subjects expect the freedom to decide whether to opt in, rather than the burden of opting out. This emphasis on organisations being 'accountable' to answer to that freedom, and individuals giving 'consent' to exercise their fundamental right, will not only foster user trust in the celebration of data protection and privacy, but also bring financial prosperity to those who respect these terms.

[549] See Article 83 GDPR.
[550] See Wolfie Christl, 'Corporate Surveillance in Everyday Life' (2017) Institute for Critical Digital Culture <https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 24 April 2019.

CHAPTER SEVEN

7. GOOGLE'S PRIVACY POLICY VS DATA SUBJECTS' RIGHTS

This Chapter will aim to question the legal basis Google has for personal data collection on smartphones. To do so, it first presents data subjects' rights and gives a brief overview of "Google's latest Privacy Policy"[551] in light of the latest developments and data protection principles prescribed by the GDPR. This Chapter continues by analysing Google's Privacy Policy and where necessary refers to the information Google provides under its Privacy and Terms or other headings on his support website. While carrying out the analysis, examples and explanations used in the subsections will refer to the above-discussed Article 5 principles – namely, purpose limitation, data minimisation, and accountability. The main objective of this Chapter is to find answers to the remaining two questions while solidifying and reiterating the above laid discussions and conclude that transparency, consent in addition to purpose limitation, data minimisation, and accountability are inseparable notions and that although Google is being overly judged based on the information whose accuracy is not known to be verified. This Chapter will also aim to demonstrate the inseparable nature of the evaluated principles, in light of data protection principles with a focus on transparency and consent. Location data is used as an example when assessing whether Google's "legal grounds for personal data collection suit the purposes"[552] of the data subjects' rights. Location data collection is chosen on purpose, as currently one of the highly debated[553] topics, it

[551] 'We Read Your Wearable Tech's Privacy Policy So You Don't Have To' (*Wareable*, 2019) <https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765> accessed 19 May 2019.

[552] 'Scalable Policy-Aware Linked Data Architecture for Privacy, Transparency and Compliance' (*Specialprivacy.eu*) <https://www.specialprivacy.eu/images/documents/SPECIAL_D1.2_M6_V1.0.pdf> accessed 6 May 2019.

[553] This is an extensively debated and referred to topic, and considerably more data is available for

is anticipated to be an integral part of Google's products and services with high potential for data aggregation[554], and the recently referred type of personal data with quantitative and empirical studies.[555] During user experience with Android OS and iOS-based phones, consent for the collection of this data is requested in a persistent manner, which facilitates making a comparative study where both operating systems can be observed.

Article 5 is a component of the GDPR and therefore although the title seems to be merely an evaluation of the purpose limitation, data minimisation and accountability principles – in fact these bedrock concepts are baked into the data subjects' rights and therefore irrelevant of what Article be observed in any context – these three in blend with the transparency have to be discussed at least to a minimum extent.

This Chapter gives brief information on the data protection and privacy rights in EU Law, which is followed by a succinct list presenting data subjects' rights in scope of the GDPR with reference to "ePrivacy Laws" where necessary. The main objective is to evaluate "Google's new Privacy Policy" through the vantage point of "data subjects' rights". However, due to soaring debate and subsequent adoption of the accountability requirements, 2019 became a pivotal year in coming a step closer to reaching a more mature approach. As opposed to 2018, this year has been increasingly practical in terms of resolving the issues around these notions in a more concise and realistic manner. This change of approach accelerated the focus on and the crucial need to strive for the potential results of new measures' appropriate

its detailed analysis, which is why it was chosen for the purposes of this Thesis.

[554] Schmidt (n 3) 30-31.

[555] ibid; also see Binns et al (n 8). For more information, see 'Anonymisation: managing data protection risk code of practice' (*ICO*, 18 October 2018) <https://ico.org.uk/media/1061/anonymisation-code.pdf> accessed 22 February 2019; Norval et al (n 338); Gamba et al (n 245).

applications. While such optimistic progress boosted the interest in fundamental rights, at the same time, IT giants have begun to work towards filling the gap between mobile technologies and legal delimitations, mostly because of the severe consequences they may face if they do not comply.

This Chapter particularly focuses on "consent", since it is highly interlinked with "transparency" and "the legal grounds". References to ""Google's Terms of Service"[556], "Android's Privacy Policy" and "Apple's Privacy Policy" will be presented, where necessary, for comparison to help juxtapose Google's position and its stance regarding "data protection and privacy laws" in the mobile ecosystem.

This Chapter also uses Google's tracking of its users' location via different technologies referring to the above-explained empirical research explained in Chapters 1 and 2. Location data is chosen as an example to discuss "Google's new Privacy Policy", and aims to find out whether Google, in fact, respects data subjects' rights as it claims it does for the purposes of the GDPR and "ePrivacy"[557] Laws.

This Chapter further discusses children's rights who are among the most vulnerable data subjects requiring strict protection. After evaluating Google's Privacy Policy, particularly in scope of recent laws, "the GDPR", "ePrivacy and the Audiovisual

[556] 'We Read Your Wearable Tech's Privacy Policy So You Don't Have to' (*Wareable*, 2019) <https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765> accessed 19 May 2019.
[557] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - 6467/19' (n 13).

Directive ("AVMSD"),[558],[559] this Chapter concludes as the following: Although Google has taken considerable steps towards showing its compliance, there is still much to do in terms of respecting data subject's rights and demonstrating this practice. Thus, Google's latest Privacy Policy – although less than the previous ones - still undermines data subjects' rights to a certain extent, and is not fully compliant with the GDPR "for the purposes of the principles prescribed in Article 5"[560], and discussed in previous Chapters.

7.1. LEGAL FRAMEWORK AND DATA SUBJECTS' RIGHTS

For almost 20 years, "the Charter of Fundamental Rights of the European Union"[561] has distinguished "the rights to privacy and data protection" as two fundamental rights. Right to privacy was established by "Article 7, and right to data protection" was established by "Article 8".[562] This distinct approach and the recognition of their distinction represented a clear modernisation and improvement compared to the CoE. This is because pursuant to the "European Convention of Human Rights" ("ECHR") both notions of privacy and data protection are covered under Article

[558] The EU Audio-visual Media Services Directive (AVMSD), 'On the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services (Audio-visual Media Services Directive)' (2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013&from=EN> accessed 20 April 2019.
[559] Sally Broughton Micova, 'The playing field between YouTube and television will be a bit fairer, but still far from level' (2018) LSE Media Policy Project Blog <https://blogs.lse.ac.uk/mediapolicyproject/2018/10/09/the-playing-field-between-youtube-and-television-will-be-a-bit-fairer-but-still-far-from-level/> accessed 25 April 2019.
[560] 'Complete Accounts Limited Data Protection Policy' (25 May 2018) <http://www.completeaccounts.co.uk/wp-content/uploads/2018/05/Data-protection-and-security-policy-vMay-2018.pdf> accessed 20 March 2019.
[561] Leenes et al (n 258).
[562] See *ECtHR MS v. Sweden* [1997] (Application No. 20837/92) para. 41 ("the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8").

8[563].[564] "Rights to privacy and data protection are fundamental rights in the EU"[565]. Therefore, in the smartphone ecosystem, "there is a high barricade to set aside individual's rights and interests in data protection and privacy matters"[566].[567]

However, on the other hand, there are critics about the data-driven economy's use of digital advertising and its potential to suffer more than necessary, affecting the whole system, which has already become a reality of today's world. Current legal frameworks regulating data use in scope of commercial activities primarily aim to protect personal data. Kolt observes[568] that today's legal frameworks focus too much on privacy issues, and "they treat data protection as a "standalone issue", distinct from the benefits which consumers receive"[569]. Kolt's arguments are realistic in terms of people's everyday activities, their quality of life through the use of smartphones, and the management of their lives by use of smartphones.

Article 5 of the GDPR entitled[570] "Principles relating to the processing of personal data" contains "the principles applicable to any processing of personal data,

---

[563] See Art. 8 ECHR ('Right to respect for private and family life').
[564] Art. 8(1) of the Charter of Fundamental Rights of the European Union; Art. 16(1) of the treaty on the Functioning of the European Union (TFEU); Art. 1(2) and recital 1 GDPR. See also Wolfgang Benedek, 'Understanding Human Rights' (2012) European Training and Research Centre for Human Rights and Democracy <http://www.manual.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/manual/versionen/english_3rd_edition/Manual_2012_FINAL.pdf> accessed 23 March 2019.
[565] 'High Level Ethical and Legal Framework, formulating ethical and legal requirements for eVACUATE' (2013) European Commission under the 7th Framework Programme <http://www.evacuate.eu/media/10345/evacuate_deliverable_d111_v10.pdf> accessed 20 March 2019.
[566] ibid.
[567] Forbrukerrådet ("Norway Policy Report"), 'Every step you take - How deceptive design lets Google track users 24/7' (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf> accessed 20 February 2019.
[568] Kolt (n 57).
[569] ibid.
[570] EDPB (n 14).

including the requirement that any processing of personal data shall be lawful and fair".[571]

Article 6 describes the circumstances in which "processing of personal data shall be lawful, one of which relates to the consent of the data subject". Article 7 further specifies the conditions for valid consent within the meaning of the GDPR.[572]

With the enactment of the GDPR, data subjects are entitled to comprehensive information in addition to "other rights against data processing entities"[573]. On the other side, data processing "entities now have to proactively fulfil several obligations towards data subjects, such as granting information on processing, erasing personal data, or rectifying incomplete personal data."[574]

Furthermore, the GDPR offers a more explicit right to erasure, also called the right to be forgotten (Article 17), the right to restriction of processing personal data (Article 18), a new right to data portability (Article 20) and a right not to be subject to automated decision-making and profiling without appropriate safeguards (Article 22).

Most private information is hoovered up through communications services that are the "digital fountains"[575] from which accurate information about data subjects' lives is track down. Location data let slip every single movement of smartphone users, shows where the users live, which pubs or restaurants they prefer to go, as well as

[571] See also Recital (39) GDPR ("Any processing of personal data should be lawful and fair").
[572] As endorsed by the EDPB on 25 May 2018, see Working Party 29, 'Guidelines on consent under Regulation 2016/679' (n 312).
[573] Voigt and dem Bussche (n 407).
[574] ibid 5.
[575] Giovanni Buttarelli, 'Buttarelli: The urgent case for a new ePrivacy law' (2018) <https://silviamartinellilaw.com/2018/11/01/buttarelli-the-urgent-case-for-a-new-eprivacy-law/> accessed 24 March 2019.

which political events they attend, which medicine they need etc. This kind of information revealing habits and interests is what "users are entitled to expect to have the most control over"[576] and also the fact that it "relates to health" makes it "sensitive".

The focal legislative instrument for giving companies the control of users' own personal data has been to require companies to seek consent.[577] Consent is susceptible to be misused or abused, so Article 4 (11) of the GDPR has clarified the term to mean:

> *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

According to the most recent "ePrivacy Regulation Proposal", the definition of and the conditions for consent provided for in Articles 4 (11) and Article 7 of the GDPR apply.[578] In cases where the processing of personal data is not specifically dealt with through the ePrivacy Directive (or where the ePrivacy Directive does not contain a "special rule"), the GDPR applies.[579]

---

[576] Giovanni Buttarelli, 'The urgent case for a new ePrivacy law' (*EDPS*, 2018) <https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en> accessed 24 March 2019.
[577] ibid. Also see 'The Urgent Case for a New ePrivacy Law' (*GDPR.ie*, 19 October 2018) <https://gdpr.ie/the-urgent-case-for-a-new-eprivacy-law/> accessed 30 March 2019.
[578] Working Party 29, 'Guidelines on consent under Regulation 2016/679' (312) 4.
[579] ibid. See also Hunton Privacy Blog (n 168). For example, the GDPR provisions regarding the exercise of data subjects' rights with respect to their personal data will apply, as there are no specific ePrivacy provisions on these rights. Similarly, any subsequent processing of personal data

7.2. WHAT ARE DATA SUBJECTS' RIGHTS?

In addition to abovementioned rights, the GDPR focuses heavily on data subjects, and protects personal data, not only in the shape of security, but also in privacy.[580]

The GDPR gives data subjects seven rights that ensure transparency – one of the bedrock principles stipulated under Article 5 (a)[581]– between data subjects and organisations processing their personal data, such as Google. According to Chapter 3 of the GDPR, Google should respect the following rights:

(1) Right of Access[582]: All data subjects have the right to be informed whether any of their personal data is being processed by Google, and where this is the case, have the right to access this data and to be provided with specific information about the processing of their personal data.

On 21 January 2019, ironically one day before "Google's new Privacy Policy" became effective; the CNIL found that Google failed to provide users with accessible, clear and understandable information, thus preventing them from

(such as personal data obtained via cookies) must also have a legal basis under Article 6 of the GDPR in order to be lawful and comply with all other provisions of the GDPR.

[580] European Commission, 'What are my rights?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en> accessed 25 March 2019. Also see Chapter III of the GDPR. With the enactment of the GDPR, data subjects have a right to information about the processing of their personal data; to obtain access to the personal data held about them; to ask for incorrect, inaccurate or incomplete personal data to be corrected; to request that personal data be erased when it is no longer needed or if processing it is unlawful; to object to the processing of their personal data for marketing purposes or on grounds relating to their particular situation; to request the restriction of the processing of their personal data in specific cases; to receive their personal data in a machine-readable format and send it to another controller ('data portability'); to request that decisions based on automated processing concerning them or significantly affecting them and based on their personal data are made by natural persons, not only by computers. The data subjects also have the right in this case to express their point of view and to contest the decision.

[581] Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, and transparency').

[582] See Chapter III of the GDPR (Section 2 Article 15).

determining, in advance, the extent and consequences of the processing of their personal data.[583] Although the reasoning behind this decision was evaluated around transparency, CNIL's findings encapsulate a lack of respect for data subjects' rights, and therefore a failure to comply with the GDPR for the purposes of Article 15 ("right of access by the data subject") and Recital 63 ("right of access")[584]. Article 15 of the GDPR gives individuals a right to their personal data. At a minimum, data subjects are entitled to know whether a controller is processing personal data relating to them, without having to jump through hoops to provide any justification other than wanting to know. They are also entitled to a copy of the personal data, free of charge. In many ways, it is the foundational right allowing individuals to enforce the obligations imposed by the GDPR.

This is reflected in the wider scope of the right of subject access: individuals are now entitled to information, as to the source of the data, any likely recipients of the data, and the envisaged period of storage. When proceeding with a thorough analysis of Google's information practices, the restricted committee applied the EDPB transparency criteria, providing useful guidance for data controllers[585]. The GDPR has highlighted these additional aspects of the subject access right, many of which were provided previously, but were not often relied upon. Anecdotal evidence suggests more requesters are including them in their requests.[586] The CNIL found that Google failed to provide users with accessible, clear, and

[583] Alexandre Balducci et al, 'FRANCE: A new phase in European privacy law enforcement – CNIL fined Google LLC 50 million euros!' (*DLA Piper Blogs*) <https://blogs.dlapiper.com/privacymatters/france-a-new-phase-in-european-privacy-law-enforcement-cnil-fined-google-llc-50-million-euros/> accessed 25 March 2019.
[584] See Rec. 63 GDPR ('Right of access'): *"A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."*
[585] DLA Piper Blogs (n 583).
[586] 'On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (n 1) 12.

understandable information, thus preventing them from determining, in advance, the extent and consequences of the processing of their personal data. When proceeding with an in-depth analysis of Google's information practices, the restricted committee applied the EDPB transparency criteria, providing useful guidance for data controllers.

As implemented, Google's general information architecture results in information being disseminated across several documents that are provided to users at different times. In addition to this fragmented information, users are forced to navigate and cross-check a large amount of information, across complex web notices and policies, several links to click, in order to be able to understand what data is collected, for which purposes it will be processed and for how long it will be retained by Google.[587] This complex architecture results in a general lack of accessibility, making it hard for users to find and understand the information.

The CNIL illustrates such statement by the conditions of processing for targeted advertising and geolocation where, in both cases, the user needs to carry out several actions (several clicks) and combine various information to know how his/her personal data is processed and how to exercise his/her rights.

Another example relating to sensitive data as well as mobile ecosystems and right of access concerns https://academic.oup.com/jamia/article/26/5/412/5376662

(2) Right to Rectification[588]: Data subjects have the right to obtain the rectification

[587] DLA Piper Blogs (n 583).
[588] See Chapter III Section 3 Article 16 GDPR ('Right to rectification'): *"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."*

or erasure of their personal data.[589] It is notable that very recently Google announced that it introduces new auto-delete controls for its users' 'Location History' and activity data.

(3) Right to Erasure ('right to be forgotten')[590]: Data subjects have the right to erasure of the data collected from them, or in other words, 'be forgotten' in the context of the entity holding their data.

This right is presented as a result of the following response by Google, which is common to nearly all mobile users especially using Google services.**[591]** (See Figure 1.4 above).

Furthermore, app providers need to provide proper information about the availability of data subject rights. Information about data subject rights shall be included in the privacy policy. In practice, app developers should ensure that the app architecture facilitates the exercise of data subject rights, including the right to access and correct personal data or to obtain erasure of personal data. The exercise of the right to erasure is of particular interest in the case of users deleting the apps

[589] For further information regarding the retention process and retention period, see 'Google Ads User Data Retention Policy' (*Google)* <https://privacy.google.com/businesses/retention/> accessed 30 March 2019; 'How Google retains Data We Collect' (*Google)* <https://policies.google.com/technologies/retention> accessed 30 March 2019.

[590] See Working Party 29, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' (2015) 176/16/EN WP179 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf> accessed 30 March 2019. Also see Chapter III Section 3 Article 17 GDPR ('Right to erasure ('right to be forgotten')). See also *Google v Spain* for comments; also see Christopher Kuner, 'The European Union and the Search for an International Data Protection Framework' (2014) Groningen Journal of International Law 2(1) <http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf> accessed 20 February 2019.

[591] Google, 'Manage your Location History' (n 135). *"What happens after deleting Location History? If you delete your entire Location History, some Google apps may not work the same as they did before. Even after you delete your Location History information, some location data may continue to be saved in other settings, like Web & App Activity, as part of your use of other services, like Search and Maps."*

from the smartphones.[592]

(4) Right to restriction of processing[593]: The notification obligation regarding rectification or erasure of personal data, or restriction of processing, is covered under Article 19. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out, in accordance with Article 16, Article 17(1), and Article 18, to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

(5) Right to data portability: All data subjects have the right to receive their personal data and have it transmitted to another data controller. This right applies only in the following cases and does not apply to paper files: i) Processing is subject to a contract[594] or based on the consent of the data subject, and ii) processing is carried out by automated means.

This is a significant new right, which has not, thus far, received much press, but has stealthily been changing individuals' ability to access their personal information. Data portability gives individuals a right to obtain from organisations an electronic copy of their personal information, in "a structured, commonly used and machine-readable format', when the organisations have obtained that personal information on the basis of consent or because of a contractual relationship with the individual.

---

[592] ENISA (n 18) 20.
[593] See Chapter III Section 3 Article 18 GDPR ('Right to restriction of processing').
[594] See also Josef Drexl, 'Data Access, and Control in the Era of Connected Devices' (2018) BEUC 131 <https://www.beuc.eu/publications/beuc-x-2018 121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 30 March 2019. Also, *"Article 6 (1)(b) GDPR, the Trojan horse of data protection, dispenses of the need to seek consent of the data subject where the processing of personal data is necessary for the performance of a contract. This may well invite businesses to try to circumvent the requirement of consent by contractual arrangements."*

This is an enhanced right of access to electronic information, and is the reason that Facebook and Google have now instigated an easy way for individuals to download all their personal data.

The right to data portability also empowers individuals to require organisations to 'port over' the personal information the individual has given them, making it much easier for people to switch providers of data-driven services, such as mobile phones, banks, insurance, cloud services and social networking platforms.

The House of Lords Committee on AI has welcomed this new right as a way of promoting competition and preventing creation of data monopolies. It is notable that public authorities may be affected by this right as it pertains to personal data held by HR, accounts and payroll, as well as potentially encompassing leisure service provision and even social services.[595]

(6) Right to object[596]: All data subjects have the right to object to the processing of their personal data. As a result of this objection, Google should no longer process the personal data, unless one of the following applies: i) Google demonstrates compelling, legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject, or ii) processing the personal data is necessary for the establishment, exercise or defence of legal claims.

(7) Right in relation to automated decision-making[597]: "As with all data subject rights under the GDPR, individuals are free to exercise their right to restrict processing "without prejudice to any other right".

---

[595] 'On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (n 1) 12.
[596] See Art. 21 GDPR.
[597] See Art. 22 GDPR.

Automated Decision-making and Profiling

A further right relates to automated computer decision-making, which relates to automated decisions being taken without human oversight or intervention. The traditional example often used is adverse credit decisions being taken automatically without human intervention. However, it can equally encompass such adverse decisions and activities as neutral algorithmic processing, arranging of information and result outputs. Examples include search rankings and priorities, search suggestions, search prompts, auto-suggest, auto-complete, and so on. Other examples could arise in relation to profiling and advertising-related activities.

Acknowledging the increasing use of AI and machine learning, as well as the capabilities of big data analytics, the GDPR addresses the risks related to automated decision-making, including profiling. Individuals have the right to be proactively informed about, and to object to, "the existence of automated decision-making, including profiling". The latter is newly defined by the GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". Automated decisions involving profiling could include differential pricing of online products or decisions concerning eligibility for credit.

Article 15 enables individuals to request meaningful information about the logic behind, as well as the significance and envisaged consequences, of the processing of their data. Article 22, on the other hand, regulates decision-making based purely on automated means, and provides that individuals have the right not to be subject to such decisions where they produce legal or similarly significant effects. There is an ongoing regulatory debate about the extent of this individual right. The EDPB's

current guidance provides that the term "right" in the provision does not mean, "Article 22 applies only when actively invoked by the individual". Instead, the EDPB considers that "Article 22 establishes a general prohibition against decision-making based solely on automated processing, which produces legal or similarly significant effects, unless the individual consents or the decision is required by a contractual relationship".[598]

This interpretation is controversial, and much of the consultation on the draft form of the guidance, asserted that Article 22 merely gives individuals the right to object to such processing, whereupon it can continue only with consent, or if it is required by the contractual relationship.[599] The EDPB's current guidance, adopted on 6th February 2018, nevertheless treats Article 22 as imposing a prohibition. This has significant ramifications for, among others, insurance and credit industries, which rely heavily on automated decision-making.[600]For example,

> *"by collecting large amounts of data on road users' behaviour, future automated vehicles will offer the possibility of addressing the 'how, where and who' of all aberrations and accidents on the road. Using these data is pivotal for preventing traffic accidents, but it also generates questions about ethics of privacy. Thus, the question is not whether sensors will acquire road users' behavioural data, as this is already happening and will most certainly be expanded towards more sophisticated data. Rather, the*

[598] 'Data subject rights and personal information: data subject rights under the GDPR' <https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/> accessed 30 March 2019.
[599] ibid.
[600] 'On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (n 1) 12.

> *question is whether people are willing to share their data, so that upon analysis, data can become "information" which, in turn, can be used to improve road safety."*[601]

Accordingly, in the future, an increasing tension between "a utilitarian use of data" and "a position of privacy" is expected to be "dominant".[602]

7.3. GOOGLE'S NEW PRIVACY POLICY

This Section gives an overview and general updates regarding Google's Privacy Policy and continues by discussing transparency, consent, and legitimate interests' grounds under the GDPR.

7.3.1. Overview

In December 2018, Google announced[603] that "it was going to update its Privacy Policy in early 2019 to further GDPR compliance".[604] Google notified the European Economic Area ("EEA")[605] and Switzerland users of updates to the company's Terms of Service and Privacy Policy". Before the new version of the Privacy Policy[606] officially came into effect, Google had already given some important information regarding the changes.

---

[601] Joost de Winter et al, 'Will Vehicle Data Be Shared To Address The How, Where, And Who Of Traffic Accidents?' (2019) European Journal of Futures Research 7 <https://eujournalfuturesresearch.springeropen.com/articles/10.1186/s40309-019-0154-3> accessed 18 May 2019.
[602] ibid.
[603] 'Some changes to our service model in Europe' (*Google*, 12 December 2018) <https://www.blog.google/around-the-globe/google-europe/some-changes-our-service-model-europe/> accessed 30 March 2019.
[604] Miller (n 492).
[605] 'European Economic Area (EEA) / Relations with the EU' <https://www.efta.int/eea> accessed 30 March 2019.
[606] Google, 'When you use our services, you're trusting us with your information' (n 253).

One of the most important of changes that Google announced was that Google Ireland Limited would become the "data controller" legally responsible for EEA and Swiss users' information. This means that Google Ireland Limited becomes responsible for responding to requests for its user data, including from EU law enforcement, consistent with Irish law. It is also responsible for compliance with applicable privacy laws, including the GDPR. Google explained the rationale behind this decision by stating the data controller change was done to facilitate engagement with EU data protection authorities via the GDPR's "One Stop Shop"[607]. This is a tool introduced with GDPR to establish a mechanism that could ensure the consistency of regulatory decisions for companies and EU citizens.[608]

Also, Google Ireland Limited became the "service provider" responsible for consumer services, including Search, Gmail, and Maps. Google's European headquarters have long been based in Dublin. Until recently, Google LLC, based in the US was the "service provider". These changes are reflected in Google's general Terms of Service[609]. Google also announced that similar changes would be made in the separate terms for Play, YouTube, and YouTube Paid Service.[610] However, in Google's written statement, the most important note is the following:

> *"These changes do not in any way alter how our products work or how we collect or process user data within our services. Nothing changes about your current settings and you will continue to have granular control over the data you*

[607] See EDPB, 'First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities' (2019) 2-4 <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> accessed 30 March 2019.
[608] Google, 'Some changes to our service model in Europe' (n 603).
[609] 'Google Terms of Service' (*Google)* <https://policies.google.com/terms> accessed 30 April 2019.
[610] Google, 'Some changes to our service model in Europe' (n 603).

share with us when you use our services. And of course, we remain fully committed to compliance with the GDPR across all of the services we provide in the European Union.[611]*"*

In this statement, Google implies that it does not need any changes to be made, neither in the data collection nor in the data processing within its services. This, unfortunately, includes mobile applications such as Google Maps, Gmail, and YouTube etc., namely those that are discussed as not being compliant with GDPR principles. The irony in Google's statement comes afterwards, when it shows off about Google's commitment to be compliant with GDPR.

To date, data subjects, regulators and "sometimes even app developers and advertisers are unaware of the extent to which data flow is rushing from smartphones to digital advertising groups, data brokers and intermediaries that buy, sell and blend information"[612]. Companies that do choose to raise awareness and implement the protocol must do so in a manner that complies with the laws of the jurisdictions in which they operate. In this regard, CNIL says it best:

"The GDPR does not aim at regulating technologies per se, but regulates how actors use these technologies in a context involving personal data."[613]

Before assessing whether the consent was "sufficiently specific and clear (or

[611] Google, 'Businesses and Data – We are committed to complying with applicable data protection laws' (n 522).
[612] Kindt (n 47).
[613] Michael Hahn, 'Why the OpenRTB Does NOT Violate the GDPR' (*Digital News Daily*, 13 February 2019) <https://www.mediapost.com/publications/article/331879/why-the-openrtb-does-not-violate-the-gdpr.html> accessed 30 March 2019.

unambiguous)", CNIL examines whether it was informed. For consent to be informed, the G29 Guidelines state that, "a controller must ensure that consent is provided on the basis of information that allows the data subject to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested."[614] In this case, due to the dilution of information within several documents, users cannot have an informed perception of what they were consenting to. Thus, the consent cannot be not "sufficiently informed". CNIL concludes that the consent was not informed[615], because the explanatory text displayed to the user upon launching the app was too complex and imprecise.[616] Moreover, users were not informed of the identity of the companies with which their data was shared, as this information was only available after several clicks and scroll-downs.[617]

With respect to the unambiguity of the consent, CNIL recalls Recital 32 of the GDPR, which requires a clear affirmative act given through an active motion or declaration. While recognising that users can theoretically modify some options associated with their account by clicking on the "More options" link, CNIL underlines that the account personalisation settings are pre-checked by default. Moreover, if users do not click on the "More options" link and simply continue the creation of the account, their consent is deemed as automatically given to Google. CNIL therefore concludes that this consent is not unambiguous, as there is no

[614] Working Party 29, 'Guidelines on consent under Regulation 2016/679' (n 312) 14.
[615] CNIL followed its case law under the former Data Protection Act. In its formal notice issued in November 2018 against Vectaury (a small ad-tech company focusing on providing geolocation-based data to retailers).
[616] Decision No. MED 2018-042 of Oct. 30, 2018, issuing notice to Vectaury.
[617] Marco C. Laurita and Anita Maklakova, 'Google's Fine and The French Data Protection Authority's Far-Reaching GDPR Compliance Measures' (*Kramer Levin*, 27 February 2019) <https://www.kramerlevin.com/en/perspectives-search/googles-fine-and-the-french-data-protection-authoritys-far-reaching-gdpr-compliance-measures.html> accessed 13 March 2019.

affirmative action from the user to consent to ad personalisation. Therefore, in its decision, the CNIL follows abovementioned guidelines stating that, "the GDPR does not allow controllers to offer pre-ticked boxes or opt-out construction that require an intervention from the data subject to prevent agreement."[618]

Finally, CNIL observes, "the consent is not sufficiently specific". Indeed, in order to create an account, users have to agree to Google's Terms of Service and to the processing of their personal data as detailed in the latter, and, in doing so; they have to accept all data processing as a whole. However, the G29 guidelines also provide that the consent must be specific to the purpose, as "a safeguard against gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data."[619] The consent should be given distinctly for each purpose.

Consent also needs to be considered *before* any processing, reading or storing of personal data from or onto the smartphones. All essential elements of valid consent should be present at that time. In a way, valid consent means open consent. Put differently, this can mean to obtain valid consent before installing the app from the app store.[620] When the pre-installed apps on Android smartphones are considered, as well as those on iPhones, it could be said that these do not apply in a proper way. Google can do this through a setup page inside the mobile apps. As on iPhones, the official search app of Google can be directly downloaded without taking any previous consent of the iPhone user. An essential element of consent is the

[618] CNIL (n 132).
[619] 'Counting down to 25 May 2018: mapping the GDPR age of consent across the EU: May 2018' (2018) <https://biblio.ugent.be/publication/8561253/file/8561256.pdf> accessed 30 March 2019.
[620] EDPS, 'Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions' (2016) 8 <https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf> accessed 30 March 2019.

information provided and the necessary details given prior to that consent.[621]

The methods used for providing information and obtaining end user consent should be as user-friendly as possible. Given the ubiquitous use of tracking techniques, end users are increasingly requested to provide consent to store tracking cookies on their devices. As a result, end users are overloaded with requests to provide consent. Therefore, the use of technical means to provide consent through transparent and user-friendly settings may address this problem. As such, Regulation should provide for the possibility to express consent by using the appropriate settings of a browser[622] or another application. The choices made by end users when establishing the general privacy settings of a browser or another application should be binding on, and enforceable against, any third parties.

As mentioned in Chapter 2, the principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. As opposed to the requirements under these principles, currently the default settings for cookies are set in most current browsers to 'accept all cookies'. Hence, providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software with the aim of offering the option to prevent third parties from storing information on the device. This is often presented as 'reject third-party cookies'. End users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies'), and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in an easily visible and intelligible manner.[623]

---

[621] Working Party 29, 'Guidelines on consent under Regulation 2016/679' (n 312).
[622] Web browsers are a type of software application that permits the retrieval and presentation of information on the internet.
[623] ePrivacy (n 13).

Google continuously tracks the location of its users both on Android and iOS platforms through a number of different technologies. As explained in Chapter 1, this tracking is realised and empowered through the features of 'Location History' and 'Web & App Activity.' These settings are integrated into all Google accounts as a 'personalisation' feature and are also used to facilitate targeted advertising. The Norwegian Consumer Council's report argues that consumers are deceived into being tracked when they use Google services. This happens through a variety of techniques, including withholding or hiding information, deceptive design practices and bundling of services.[624] This report further contends that these practices are unethical, and that they are in breach of European data protection legislation, because they fail to fulfil the conditions for lawful data processing.

Does Google Run Afoul of the GDPR?

As briefly presented in the previous Chapters, there are some vague explanations, or in some cases, no explanations when setting up and using an Android smartphone. As established, there are some gaps between what Google actually does and what it presents to its users, while making the information accessible. Its Privacy Policy, Terms of Service, or even informational screens popping up the device when using Google's apps and services may not be satisfactory for the purposes of protection of data subjects' rights and the GDPR. So on top of how Google presents these settings to the data subject, especially about data collection methods and purposes for which the collected data will be used, there are several questionable legal issues, as well as ethical ones, about the ways in which Google implements 'Location History' and 'Web & App Activity' into Android and end users' Google accounts. This section furthers the discussion by pointing out some legally problematic issues, which could be a burden on data subjects' shoulders.

[624] Norway Policy Report (n 567) 4.

After a clear discussion and analysis on the legal implications of these issues, this section concludes that Google is at odds with, or has run afoul of, the GDPR to a certain extent.

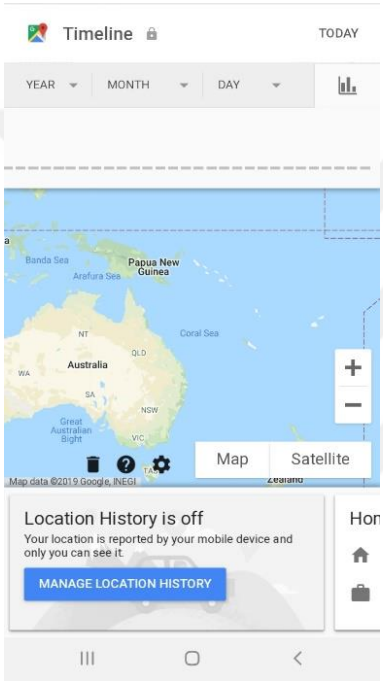
To begin with an example, "smartphone users who dip into the Account dashboard can gain control over what ads they see to a certain degree".[625] However, at the same time, many information and settings are spread throughout the dashboard, some of which are often truly challenging to find. This challenge is thoroughly discussed in the previously mentioned Norwegian Consumer Council report[626] on how users are deceived by design through the use of dark patterns. According to the report, "by giving users an overwhelming amount of granular choices to micro-manage, Google has designed a privacy dashboard that, according to the analysis, in fact, discourages users from changing or taking control of the settings or delete bulks of data. This report also underscores the importance of how the presence and claims of complete user control may incentivise users to share more personal data."[627]

Google does give a certain degree of control to the user through its Google account system. For example, as of May 1st, 2019, as mentioned before, Google now allows the automatic deletion of Location History. Previously, 'Location History' could only be manually deleted through the 'Location Timeline', and can be exported via the 'Takeout' tool.[628] Yet, the data extracted via 'Takeout' appears to be more

[625] 'Ad personalisation' (*Google)* <https://adssettings.google.com/authenticated> accessed 30 March 2019.
[626] 'Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy' (*Forbrukerradet*, 2018) 39 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 30 March 2019.
[627] ibid 39.
[628] 'Google Takeout: Download your Data' (*Google)* <https://takeout.google.com/settings/takeout?pli=1> accessed 30 March 2019.

elaborate than what is shown in the 'Location History' timeline.[629] As discussed in Chapter 1, location data is personal data, since it falls under the scope of being "information that directly or indirectly can identify a natural person".[630] So, Google is collecting personal data when it collects and processes information about a smartphone user's location and movement through its products and services.

Figure 7.1: Android Web-based Timeline



Source: Android Web Account Screenshot

The processing of personal data is lawful only if, and to the extent that, at least one

[629] Norway Policy Report (n 567) 26. This can be seen by using third party tools such as 'Location History Visualizer' <https://locationhistoryvisualizer.com/> accessed 30 March 2019.
[630] See Article 4 (1) GDPR.

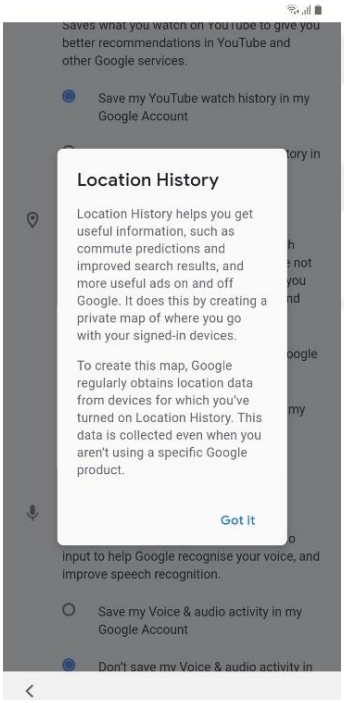
of the six general terms is fulfilled as stipulated in Article 6 of the GDPR.[631] This is why there is a need to identify the legal ground(s) that Google uses to collect and process personal data for advertising purposes. Looking at "Google's new Privacy Policy"[632], for many it may seem quite clear that Google uses consent and legitimate interests when processing data for advertising purposes. Therefore, on the basis of "Google's new Privacy Policy", this Section will only consider these two grounds out of six legal grounds provided in Article 6. The information given in the Privacy Policy is unclear, in terms of providing specific information on which legal grounds apply to what manners of processing. This ambiguity and the lack of precise information is, in itself, problematic. This is because Google has an obligation to specify the legal basis it is using for particular processing of personal data. But this problematic issue is not new, and definitely is not a surprise for Google. In 2012, after a thorough investigation, EU Data Protection Authorities explicitly and in clear language warned Google about its lack of disclosure, and asked for detail on how it processes personal data in each service and how it differentiates the purposes for each service and each category of data.[633] In the same report, Google was also given recommendations to adapt information to mobile users and ensure that passive users are appropriately informed about its data collection and processing.[634] Seven years later in 2019, the restricted committee observed that some of the information Google provides fails to be clear and comprehensive.

Furthermore, Norwegian Consumer Council argues that relying on legitimate

[631] See Article 6 and Recital 40 of the GDPR.
[632] 'Data transfers' (*Google)* <https://policies.google.com/privacy#enforcement> accessed 31 March 2019.
[633] CNIL, 'Working Party 29: Letter to Google' (n 404) 2.
[634] ibid. Also see CNIL, 'Google Privacy Policy: Main Findings and Recommendations' <https://www.cnil.fr/sites/default/files/typo/document/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 31 March 2019.

interest to process data, while the processing could have been based on another lawful basis, should also amount to a violation of transparency requirements.[635] Two months after this report was published, the information communicated to the users in Google's Privacy Policy was similarly not found to be "sufficiently clear to allow the user to understand that, the legal basis of processing operations for ads personalisation is the consent, and not the legitimate interest of the company".[636] However, the GDPR provides that the consent is "specific" only if it is given distinctly for each purpose.[637]

Figure 7.2: Android Location History – "Learn More" on Its Benefits



Source: Samsung Galaxy A10 2019 Screenshot

[635] See Article 5(1)(a) GDPR; also see ICO, 'Legitimate Interests' (n 16).
[636] ibid.
[637] ibid.

For the purposes of the GDPR, consent has to be opt-in. Since 'Location History' is based on users' opting in, it is off by default. Google claims that this data collection and processing are based on consent[638] and explicitly provides the following statement: "Location History" is turned off by default for your Google Account and can only be turned on if you opt in"[639]. It further adds potential benefits of turning it on for users:

> *"When you turn on Location History, you may see a number of benefits across Google products and services, including personalized maps, recommendations based on places you've visited, help finding your phone, real-time traffic updates about your commute, and more useful ads."*[640]

In this case, consent can be considered a legal ground for processing user's location data if the user has opted in, since the option to turn on 'Location History' is left to the data subject, without making a default setting that may undermine the free will of the users.[641] On the other hand, another tracking means used by Google, 'Web & App Activity,' is turned on by default. Thus, Google should not be able to rely on

---

[638] See Article 6 (1) (f) of the GDPR; see also Article 5(3) of the ePrivacy Directive, which requires consent to pull information from a user's device. As the ePrivacy Directive already requires consent for reading information (such as location data) from a user device, it makes most sense if the applicable legal basis under the GDPR is also consent in Location History.

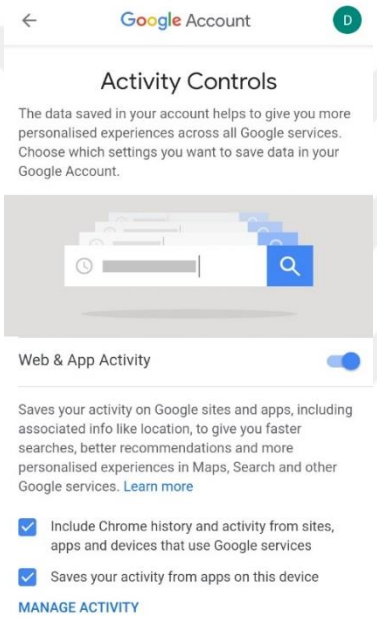
[639] Google, 'Manage Your Location History - Google Account Help' (n 135).

[640] ibid.

[641] 'Google accused of GDPR privacy violations by seven countries' (*The Verge*, 2018) <https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive> accessed 31 March 2019; also see 'Google still tracks you through the web if you turn off Location History' (*The Verge*, 2018) <https://www.theverge.com/2018/8/13/17684660/google-turn-off-location-history-data> accessed 31 March 2019.

consent as a legal ground. The Article 29 Working Party clearly state that, "pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement" is consent invalidated under the GDPR.[642] Hence, it could be concluded that processing of location data collected through 'Web & App Activity' is not based on consent, but it is based on legitimate interests.[643]

Figure 7.3: Activity Controls – Web & App Activity – Controls Default 'On'



Source: Samsung Galaxy A10 2019 Screenshot

As a possible suggestion, Google can inform its users about the reasons it chooses to change some of the wording or examples given in its Privacy Policy. By doing so, it would leave less room for interpretation and users would appreciate the effort

[642] Working Party 29, 'Guidelines on consent under Regulation 2016/679' (n 312) 16.
[643] See Article 6(1)(f) GDPR.

and possibly interpret it as good will.

Example

This section aims to provide a short analysis on the methods Google utilises when collecting consent for 'Location History'. The main objective of this section is to discuss whether the way Google collects consent from data subjects falls under the scope of the GDPR, or in other words, whether it is compliant with the requirements stipulated in the GDPR. This is followed by a discussion of the legal grounds for 'Web & App Activity' feature's collection of personal data and location data.

Transparency

Although 'transparency' deserves a chapter itself, since it is highly relevant and essential to include in the context of consent, this thesis evaluates this bedrock principle together with its lifelong inseparable companion, consent: One simply cannot exist without the other.

Consent

Even companies must take into account a consumer's expectation of how their data will be used and cannot infringe on the rights of other consumers, as guaranteed under the GDPR. In the digital realm, EU consumers have the added protection of a companion set of rules, namely the ePrivacy Regulation that governs electronic communication. Under these rules, which are in the process of being ratified into law, consent is the only legal basis for collecting personal data. There do exist potential loopholes in the law, which allow businesses to process personal data without consent for limited reasons. An example could be a business' "legitimate

interests," which the European Commission says include "direct marketing"[644] through mail, email or online ads.

The basic concept of consent remains similar to that under the Directive 95/46/EC, where consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR. As mentioned above, consent is defined in Article 4 (11) of the GDPR as "any freely given, specific, informed, and unambiguous indication" by a "statement" or by "clear affirmative action" from the data subject.[645] All of these conditions need to be met for a valid consent. As discussed previously in this thesis, Google uses the collected data for advertising purposes, which is crucial for its business model and profit making. The question that remains to be answered is, then, the following: "Does Google's use of 'Location History' data for advertising purposes fulfils these conditions?".

In Google's latest Privacy Policy – although this statement was the same in the previous one[646] – states under the title of "With your consent": *"We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads. We also ask for your consent to collect your voice and audio activity for speech recognition. You can manage these settings in your Google Account."*

It seems that Google gives consent as a legal basis for at least "some" of the collection and processing of the user's personal data. It is ironic to note that it provides targeted advertising services as an example implying the purpose of its

[644] European Commission, 'What does 'grounds of legitimate interest' mean?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en> accessed 31 March 2019.
[645] See also Recital (32) and Recital (33) GDPR.
[646] Google, 'Privacy Policy' (n 646).

processing of the collected data. Meanwhile, the question asked above remains unanswered.

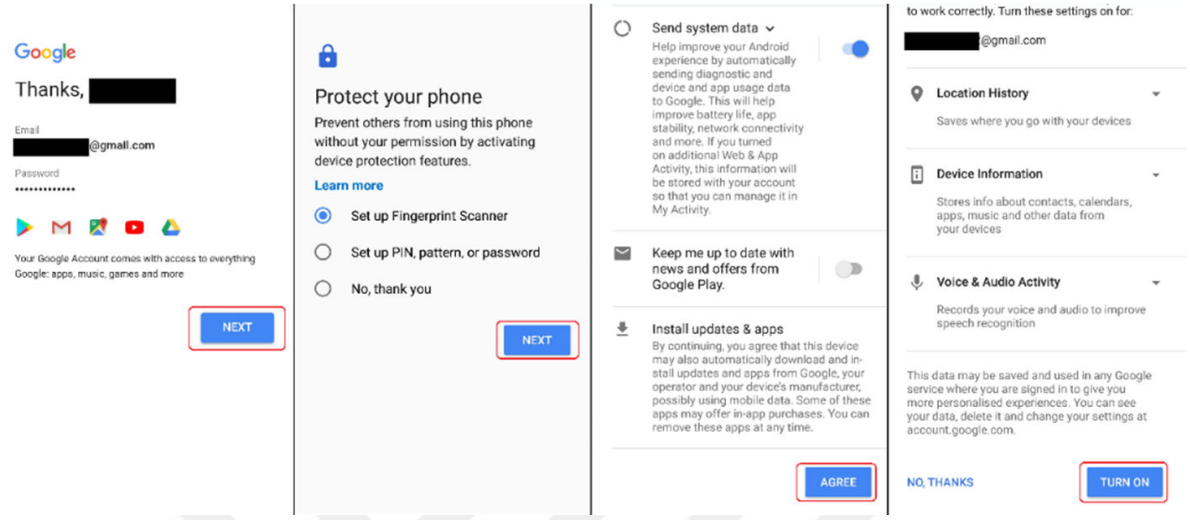
Is Consent Freely Given?

Google contends users to have to choose to opt in to 'Location History'[647], where the user should be freely giving his/her consent for Google's personal data collection via 'Location History', and therefore for the processing of that data. Put differently, this indicates that the user is provided with a real choice about whether he/she accepts Google processing such data, and that this data may be used for advertising purposes.[648] However, there is a considerable difference between iOS users and Android users regarding how Google collects consent for 'Location History'.

During the Android setup process, as shown in the 2019 versions of Android OS smartphones (Huawei and Samsung), the data subject is being provided guidance through a process which paves the way or 'encourages' the user to give consent to Google for processing his/her location data. More precisely, by making a time-saving, convenient way for the user to simply follow the click-flow, seems as if the setting is designed to facilitate the user's consent to opt in.

[647] Google, 'Manage Your Location History - Google Account Help' (n 135): *"If you opt in to Location History and your device is reporting location, the precise location of your signed-in devices will be collected and stored, even when you're not actively using a Google product or service."*
[648] Norway Policy Report (n 567) 35.

Figure 7.4: Google Account Setup Process



Source: Samsung Galaxy A10 2019 Screenshots

As observed both on Huawei and Samsung devices, Android OS provides a click-flow that makes the user likely to enable 'Location History' as a part of the process. However, the problem is that the user may actually give consent to Google without being made fully aware of what that entails[649]. If the data subject is not aware of what he/she consents to, it will be contestable whether consent has been "freely" given.

This reasoning is very similar to the intention to create legal relations, which is a necessary component establishing a contract under English contract law. Here, the offer is made by Google to the user. However, the user would not be considered to have accepted the offer – in our case, give consent to it – under contract law. This is because there is no consideration and no genuine intention to create legal

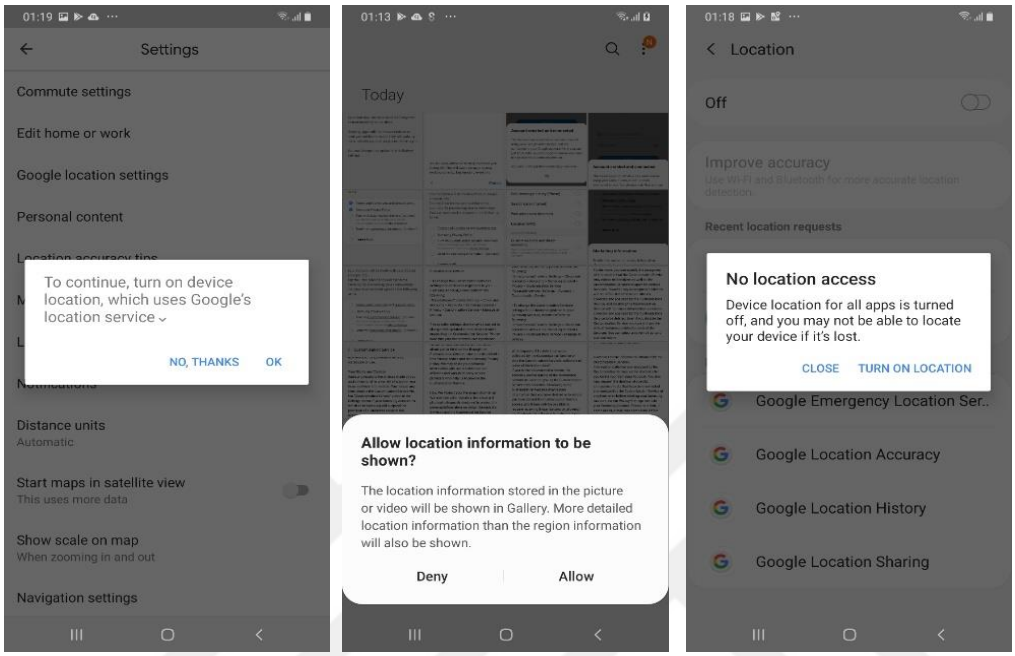
[649] ibid.

relations. In common law, this would be deemed void.[650] In fact, although the subject is not contract law, the consent requirements, and the reasoning behind them have great resemblance to contract law.

Additionally, if the user does not give consent to 'Location History' during the setup process, Android users are nudged toward enabling the setting on several other occasions. This could be considered as imposing on the user to give consent. In fact, this shows how these mildly pushy settings can affect the users psychologically.[651] The user may feel pressured into giving his/her consent, because of this recurrent nudging or pestering with consistently re-appearing consent requests. Therefore, considering consent should be freely given in order to be valid, this would not fall under the scope of consent for the purposes of fundamental rights in the EU and under the GDPR. Also, the Article 29 Working Party have stated that consent is not freely given, if there is "any element of compulsion, pressure or inability".[652]

[650] ibid.
[651] See 'An Analysis of the Effects of Smartphone Push Notifications on Task Performance with regard to Smartphone Overuse Using ERP' (2016) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4912993/> accessed 2 April 2019.
[652] "The Article 29 Working Party" was replaced by the European Data Protection Board (EDPB) on the 25th of May 2018. This is a group consisting of EU member state data protection authorities, who provide guidelines on how to interpret EU-regulation on data protection issues. (See 'Consent' (n 312)).

Figure 7.5: Repetitive Nudge/Notifications Pushing for Location History to be Changed From the Default 'Off' to 'On'



Samsung Galaxy A10 2019

Another service of Google which may be used as a "less presented" instrument to pave the user's way to giving consent is through Google Assistant. Schmidt categorises Google Assistant as one of the products with serious future potential for data aggregation. Google collects all Google Assistant queries, whether audio or typed, in addition to the location where the query occurred.[653] Norway opines that data subjects are "pushed into" giving consent to 'Location History' in order to gain access to Google Assistant[654] and other links such having photos get sorted based

[653] Schmidt (n 3) 32.
[654] *"Google Assistant is one of the products with high future potential for data aggregation Google has additional products that show future potential for market adoption and data*

on location.[655] There are also unclear and imprecise warnings about reduced functionality if the user disables 'Location History'.[656] These examples indicate that users who have been nudged into enabling 'Location History' have not "freely given" their consent, and consequently it does not constitute valid consent required under the GDPR. If this is the case, the processing of this personal data may lack a valid legal basis (See Figure 1.8 above).

Many users "consent" to the requests Google persistently exposes them to, for the sake of being able to benefit, and not being alienated, from the products and services that Google provides in return for accepting its offer. Is Google's offer so essential that data subjects cannot deny? The response of enabling and not rejecting Google's consent requests could be seen by psychologists and sociologists as a result of Google "passively" forcing end users. In fact, this interdisciplinary relationship is highly relevant for the purposes of Article 6 (1) (a) of the GDPR. When Google's passive data collection is combined with passive imposition, all lines become blurry. This reaches a point where such fundamental rights become underestimated. According to research, users who turn on location services, or enable Google's other services of the sort, do not want to do so to benefit from those services, and are in fact not willing. The act of asking for consent, in that case, almost becomes an imposition, an enforcement on, and a degradation of individuals and their rights, as a practice that is not yet frowned upon. Users practically give up some fundamental rights hoping to gain other 'rights', such as access to Google's

collection, including AMP, Photos, Chromebook, Assistant, and Pay. Additionally, Google is able to use third party data vendors to collect user information." "Google Assistant is enabled on various other speakers produced by 3rd-parties (e.g. Bose wireless headphones). Overall, Google Assistant is available on more than 400 million devices.92 Google can collect data via all these devices since Assistant queries go through Google's servers." For more information, see Schmidt (n 3) 30, 32, 33.

[655] Norway Policy Report (n 567) 36.

[656] ibid.

technology. This truly demonstrates the 'Google Technology Authority'.[657]

With respect to the dominant position of leading IT service providers, such as Google and Facebook, the following example is relevant. Going back to the fact-based legal analysis of consent, decided[658] that there is no effective consent pursuant to Art. 6(1a) of the GDPR, the Facebook case summary stated as follows:

"The reasons for this include the fact that, in view of Facebook's dominant position in the market, users consent to Facebook's terms and conditions for the sole purpose of concluding the contract, which cannot be assessed as their free consent within the meaning of the GDPR."[659]

7.3.2. Is consent "specific and informed"?

Consent must be specific and informed in order to be considered valid. To elaborate, the user must be presented with "any information that is necessary to understand what he/she is consenting to". Also it means that the potential consequences of giving consent should be made clear.

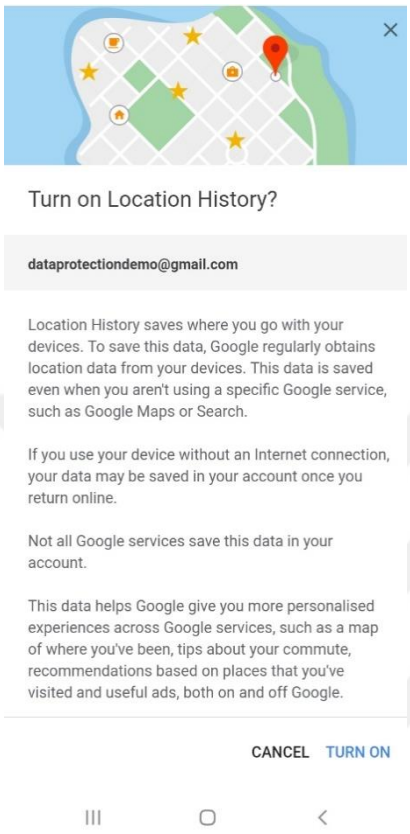
First of all, when users set up a Google account, they are told that they can control and will have a say in how Google collects and uses their data. Users are also informed that they can adjust the settings and withdraw their consent when they want to do so. This indicates that Google has provided information about rules, safeguards, as well as rights. Nevertheless, Google's provision of such information does not necessarily mean that the way this information is presented is sufficient. This is because data subjects have to click on "learn more" to be able to access important information about the purposes of the processing of data, and the options

[657] "These practices can be psychologically distressing users of Google's apps and services."
[658] Bundeskartellamt (n 436) 10.
[659] ibid.

they have. Therefore, it could be concluded that the way Google provides such information plays a crucial role for data subjects' enjoyment of their rights, without having need to make an extra effort to dig into "learn more" sections, where Google might put information crucial for the purposes of the notion of consent in scope of the GDPR.

Secondly, the sufficiency and clarity of the information Google provides about the purposes of the processing of location data may be problematic. As discussed earlier on in this thesis, Google gives some information about processing personal data for advertising purposes, but only if the user clicks "learn more". The information Google provides in "learn more" does not shed much light to help data subjects understand the depth of what is being asked. Ironically, clicking on "learn more" can make the information to which data subjects have right to access even more ambiguous. This is because, Google actually does provide more information, but not satisfying the expectations of data subjects when they click on "learn more". Whenever 'Location History' is presented to the user, the important details lying behind Google's location data collection are not revealed, whereby the user needs to click on "learn more" to see more information, which is, again, not very useful to understand the scope of this so-called "private map".

Figure 7.6: Location History Turn 'On' Notification and the Limited Details Provided



Source: Samsung Galaxy A10 2019 Screenshots

The description still seems to mislead the user about what he/she is actually agreeing to. For example, 'Location History' is often described as being a "private map", which may give the impression that the information is not used for other purposes, such as advertising, and many may not expect Google to save all the places they go to on their "private map" - especially, when they are not actively

using a Google product.[660] In addition to all this vagueness, as Norway claims, the choice of word used in its explanations such as "private map" could make data subjects even more sceptical. This time not resulting from the ambiguity, but more due to the phrasing, which could easily be misleading[661] to the data subject. In fact, Google has included "private map" into its "new Privacy Policy", which is in effect since the end of January 2019. There is no information regarding what a "private map" is, and it is very hard to understand why Google chose to use the following phrase: "*The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices."*[662] The implications of the word "private" is bewildering for a user especially living among today's soaring privacy-related debates.

Also, can this "private map" only be seen by the user himself/herself? If it is, is there a public map? No one can find out more without turning the 'Location History' on. In terms of 'Location History' explanations, Google's Privacy Policy is, arguably, a disappointment. When the user creates a private map, and believes it is private, he/she would naturally assume that it will neither be shared with others,

---

[660] When signing up for an account Google shows its "Privacy and Terms" page above its "Agree" button. In this Privacy and Terms statement, there is no information regarding the Location History unless the user clicks "More Options". After clicking "More Options" and going on the Location History section, and finally after the third "extra step" done by the user – clicking on "Learn More" – the following information is written: *"Location History helps you get useful information, such as commute predictions and improved search results, and more useful ads on and off Google. It does this by creating a private map of where you go with your signed-in devices."*

[661] See "Norway Policy Report (n 567). The privacy map was not included in Google's new Privacy Policy – ironically, apparently Google does not think the same way and so that in fact it changed its previous Privacy Policy (which became effective on May 2018). You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

[662] Google, 'When you use our services, you're trusting us with your information' (n 253).

nor will it be used for anything other than saving the locations that the user wants to be saved. Also, many could understand or assume that their private map would not be used for advertising. It would be ideal if Google could also work with language experts[663], as well as receiving public feedback, before changing its Privacy Policy.

This is because there are generally two documents, which govern the relationship between a consumer and a data-driven service provider: the terms of service and privacy policy.[664] Typically, the terms of service contain a variety of conditions while privacy policies describe the types of personal data collected and how these are used[665] These documents are very important since they determine the scope of the relationship of both parties, and their vagueness can cause more confusion leaving the target audience mostly more perplexed than before.[666] This applies especially to the above-laid out case, since Google is responsible for providing information that is most likely to be "unknown" to many users who are not coming

[663] For example, language qualifiers such as "may", "might", "some", "often" and "possible" could be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the Second language(s) so that the translated text does not have to be deciphered or re-interpreted. See more in: Working Party 29, 'Guidelines on transparency under Regulation 2016/679' (2018) 9.

[664] 'Terms of Service' are also known as conditions or terms of use and shrink, clickwrap or browsewrap licenses. See Mark A. Lemley, 'Terms of Use' (2006) 91 MINN. L. REV. 459, 460.

[665] See 'Passive Data Collection' <https://iapp.org/resources/article/passive-data-collection/> accessed 4 April 2019; also 'Privacy Policy' (n 646) (distinguishing between data "you create or provide to us" and data "we collect as you use our services"); and 'Data Policy' <https://www.facebook.com/full_data_use_policy> accessed 4 April 2019 (referring to "[t]hings others do and information that *they* provide about you"). Passive data is also sometimes referred to as "ambient data."

[666] Kolt (n 57) 8.

from a relevant technical background. Google needs to put in a better effort to be as straight-forward and precise as possible, as it does not have the luxury of relying on "implied terms", nor can it afford expecting the users to assume on their own. Having a higher threshold of transparency is also for the company's own good, especially in today's digital society when so many entities face the possibility to be influenced by "mis-information" or "dis-information" popping up increasingly more every day on media.

Neither Google, nor its users, can disregard the regulatory developments in the world. This is because, the world could come to a stage where each and every individual or organisation can be 'enslaved'[667] in a sense, becoming so accustomed to smartphones and other smart mobile devices to the point of addiction, to the loss of one's humanity, questioning the fundamental rights as data 'sources'. It is important to feed the ethical aspects of such discussions, in aiming to enhance the fundamental rights, while welcoming the changes that could result from the very devices that humankind itself invented.

Overall, the protection of data subjects' rights is crucial, especially in today's rapidly changing world, and this protection would surely contribute to the balance and healthy relationship between technology and fundamental rights, in addition to being a true investment in the future of the leaders of technology, with IT giants such as Google. Even if the user makes an extra effort clicking "learn more" to read the information given, it is likely that a considerable number of people will find it difficult to clearly figure out to what degree, how, and for what specific purposes their location data will be used. The information spread out in the Privacy and Terms, Privacy Policy, Privacy Principles, and FAQs on Google's website expects

[667] 'Phones should be 'slaves, not masters', says Samsung UK mobile chief' (*The Guardian*, 1 March 2018) <https://www.theguardian.com/technology/2018/mar/01/smartphone-obsessed-slaves-not-masters-samsung-uk-mobile-chief> accessed 5 April 2019.

data subjects to connect the dots themselves, and rise above the challenge Google is creating by making their use of data collection ambiguous to the rest of the world. For example, it is not rocket science to foresee that data subjects might not expect their location data to be collected when they use Google Assistant. Even if the user knows that his/her location data is being collected when he/she uses Google Assistant, the reasons lying behind this collection should be explained to the user in a satisfactory and clear manner. Since details of Google's data collection may not be evident to many users, especially in situations as in the given example, Google's data collection can be considered to run afoul of a "specific and informed" consent for the purposes of the GDPR.

7.3.3. Is consent "unambiguous"?

Under Article 4 (11) of the GDPR, one of the conditions for a consent to be considered valid is for it to be "unambiguous". In other words, data subjects are expected to be given an "unambiguous indication" through a "statement" or a "clear and affirmative action", showing that they consent to Google to collect and therefore process their personal data for the specific purposes Google processes that data for.

Going back to the 'Location History' example, this translates to the fact the data subject gives his/her consent to Google for it to be used for advertising purposes through 'Location History'.

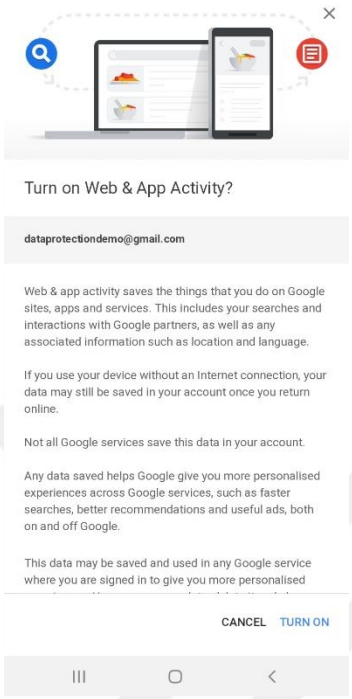
CNIL's landmark decision is the perfect example showing this reality. The finding states that Google made it too difficult for data subjects to understand and manage options on how their personal information is being used, in particular with regards to targeted advertising.

Firstly, it must be noted that if Google were to ground the personal data processing

in ‘Web & App Activity’ on consent, consent would not be considered “unambiguous”. This is because, as mentioned above, ‘Web & App Activity’ is turned on by default, meaning that Google allowed the personal data to be collected before asking for the user’s consent. The legal base behind this reasoning is that pre-ticked boxes and “blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data.”[668] In addition, Recital 32 stipulates, “silence, pre-ticked boxes or inactivity should not constitute consent”.[669] Also, in the context of Google Assistant, Google’s use of pre-ticked approvals must be checked for each personal assistant feature to see if it is off or on by default under Recital 32. Depending on the result, for the service to be compliant, “…consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.”

[668] Working Party 29, ‘Guidelines on consent under Regulation 2016/679’ (n 312).
[669] CNIL (n 132).

Figure 7.7: Web & App Activity Turn 'On' Notification



Source: Samsung Galaxy A10 2019 Screenshots

In addition, as Google adds in this respect, "if you have other settings like *Web & App Activity* turned on and you pause Location History or delete location data from Location History, you may still have location data saved in your Google Account as part of your use of other Google sites, apps, and services. For example, location data may be saved as part of activity on Search and Maps when your *Web & App Activity setting* is on, and included in your photos depending on your camera app settings."[670]

Google claims that "the data subject must opt in before it can process location data

[670] Google, 'Manage Location History' (n 135).

collected through 'Location History'". However, as Norway previously pointed out, even if the user gives consent to Google, this consent may not be considered as valid.[671] This is because "this consent is given after the user is exposed to click-flows and information that is not obvious". Consequently, it is susceptible whether the smartphone user has given an "unambiguous indication".[672] therefore, can be considered to have given his/her consent for Google's data collection activities.

Also, this problematic situation leads to questions about whether the consent is "obvious". Due to this, Google was found by CNIL to be in breach of the GDPR in relation to the processing of personal data for advertising purposes without valid authorisation. CNIL specifies that it is sanctioning Google over a "lack of transparency, inadequate information and lack of valid consent regarding the ads personalisation."[673] Put differently, it was found that Google was not seeking "unambiguous" consent for all of its products through which it collects and processes data, but limiting the steps by pre-ticking certain boxes, in violation of the GDPR principle by which users need to approve each specific use of their data.

Above and beyond, as shown above, the data subject may also have not chosen to opt in to turn on 'Location History' numerous times. Despite this, the data subject is continued to be pushed to turn the 'Location History' on in various settings. The user is given no other option than to perform extra actions and clicking "learn more" in order to get information about the purpose of the personal data collection. The presentation of this information is ambiguous, and consequently may not be in accordance with the requirements for an "unambiguous consent".[674] However, it is

[671] Norway Policy Report (n 567).
[672] ibid.
[673] 'Google fine launches new era in privacy enforcement' (2019) <https://www.politico.eu/article/google-fine-privacy-enforcement-france-gdpr/> accessed 5 April 2019.
[674] Working Party 29, 'Guidelines on consent under Regulation 2016/679' (n 312) 17.

worth mentioning that, within the requirements of the GDPR, controllers have the liberty to develop a consent flow they want that suits their organisation. In this regard, Google may argue that a consent flow was devised in the way it suits the organisation. Also, according to Working Party Article 29 guidelines, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.[675] Although this argument may seem to make sense and possibly be an acceptable ground for adoption in Google's defence, this ground hardly outweighs consent requirements, which become stronger with the bedrock principle of transparency.

Looking from another perspective, even if Google can explain its choice of putting details in the typical "learn more" sub-menu, its choice of continuously requesting the user's consent to opt in for sharing location data in different contexts would probably be deemed as an imposing act, and not a fair and honest consent flow for the purposes of "suiting the organisation". This is because, as many services need personal data to function; hence, "data subjects frequently receive multiple consent requests that need answers through clicks, which may result in a certain degree of click fatigue"[676]. This fatigue caused by repeated exposure may, in fact, affect the evaluation of consent, as the actual warning effect of consent mechanisms is diminishing.

This argument is especially of utmost importance for people with learning disabilities,[677] such as attention deficit disorders and dyslexia. It could be argued that the warnings are not only satisfactory to meet the requirements of getting an

[675] ibid 16.
[676] ibid.
[677] See Julia Angwin and Terry Parris Jr., 'Facebook Lets Advertisers Exclude Users by Race' (*ProPublica*, 28 October 2016) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> accessed 23 March 2019: *"Discrimination may present itself in various different forms. Facebook's system allows advertisers to exclude black, Hispanic, and other "ethnic affinities" from seeing ads."*

"unambiguous" consent, but also because it fails to be inclusive and non-discriminatory for the purposes of the fundamental human rights. The data controller is expected to reach out to as many people as possible, especially if a data controller is aware that their goods/services are availed of by, or targeted at, other vulnerable members of society, including people with disabilities".[678]

Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects, merits proper and careful consideration by the data controller in its assessment of how to ensure that it complies with its transparency obligations concerning such users. Google is involved more in education, students share their homework through Google drive and follow their classes on Google platforms. Google should evaluate all the possibilities, especially, students with learning disabilities such as dyslexia and ADHD and so on are diagnosed, and a large portion of its users consist of teenagers and young students, among whom these conditions are more prevalent.[679] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.[680] Also,

[678] Working Party 29, 'Guidelines on transparency under Regulation 2016/679' (n 663).
[679] Microsoft has taken progressive and great steps for the purposes of addressing people with disabilities (the scope of this e-book is inclusive and deserves to be appreciated not only for implementing the necessary measures to promoting equality, but also because of the awareness Microsoft creates). See 'Modern Marketing Is Accessible Marketing' (*Microsoft Azure Edge*) <https://advertiseonbing-blob.azureedge.net/blob/bingads/media/library/insight/moder-marketing-is-accessible-marketing/accessibility-marketing.pdf> accessed 14 May 2019; see also Laurie Sullivan, 'Microsoft Bing Ads UI Gets 'Massive' Upgrade, Better Access' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335118/microsoft-bing-ads-user-interface-gets-massive-u.html> accessed 16 May 2019.
[680] Accessibility is closely intertwined with the effective implementation and the full enjoyment of all the rights set out in other articles of the UNCRPD. Its importance is reiterated by the UNCRPD Committee in each of its General Comments and by the CoE Disability Strategy 2017-2023. Although disability and the equal rights are taken seriously across the globe including the EU, the

since persons with disabilities have the right "to enjoy legal capacity on an equal basis with others in all aspects of life"[681], following the enactment of the GDPR and the ePrivacy regulation, persons with disabilities have the same rights as any other data subject. Although it may be argued that the requirements of a valid consent are already inclusive, since Article 4 requires the consent to be given unambiguously, which is only possible if the data subject understands it. However, it is important to keep in mind that its users, including those with disabilities, are increasingly expecting Google to respect the GDPR, not only because it brought the novelty of accountability and fines, but also because, going back to the notions of privacy and data protection as fundamental rights, the GDPR itself touches upon other human rights. Google has already taken big steps towards helping people with disabilities, but can still do more.[682]

---

discussions concerning data protection and privacy are generally around keeping the disabled individuals' data secure, and respecting confidentiality. For example, see Article 22 UNCRPD ('Respect for privacy'). Also see the 'Convention on the Rights of Persons with Disabilities' <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-31-statistics-and-data-collection.html> accessed 31 March 2019; see OHCHR, 'Convention on the Rights of Persons with Disabilities' <https://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx#9> accessed 31 March 2019. Furthermore, see Article 31 of UNCRPD ('Statistics and data collection'); see FRA, 'EU CRPD Framework' <https://fra.europa.eu/en/theme/people-disabilities/eu-crpd-framework> accessed 31 March 2019; see Article 17 UNCRPD ('Protecting the integrity of the person') <https://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx#9> accessed 31 March 2019.

[681] See Article 12 UNCRPD ('Equal recognition before the law') <https://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx#12> accessed 31 March 2019; also see CoE, 'Accessibility of information, technologies and communication for persons with disabilities' <https://rm.coe.int/final-study-accessibility-of-information/168072b420> accessed 31 March 2019.

[682] Google has made Android completely usable by voice, teamed up with outside vendors to give Android eye-tracking capabilities, and launched the Google Impact Challenge, a $20 million fund to generate ideas on how to make the world more accessible to the billion-odd individuals in the world living with disabilities; see more in 'How Designing For Disabled People Is Giving Google An Edge' (*Fast Company*, 23 May 2016) <https://www.fastcompany.com/3060090/how-designing-for-the-disabled-is-giving-google-an-edge> accessed 3 April 2019.

Overall, Google "should design consent mechanisms in ways that are clear to data subjects. Google must avoid ambiguity and must ensure that, the action by which consent is given can be distinguished from other actions. Therefore, without all the necessary measures in place to make the statement clear and obvious, Google should not expect to see this as the data subject's indication of intent that signifies his/her will to a proposed processing operation, merely because he/she agreed to the "Privacy and Terms" when creating an account. This system is unfortunately paving the way for an unquestioning society that simply acts or follows, and Google seems ready to settle with fulfilling a bare minimum. Zuboff argues that this is one of the ways how digital capitalism is turning humans into objects, governing, and controlling them without them knowing that they are controlled.[683]

In this context, while individuals may 'consent' to having organisations aggregate their data and continue to use their services, individuals' choice, and control over their own personal data is nevertheless curtailed. Due to the risks present, consent in situations of power asymmetry must be treated with caution.[684] The GDPR has the potential to improve the status quo and to deliver individuals with more effective data control. However, as Shao argues, its provisions have yet to be interpreted by the courts.[685] To avoid the issue altogether, individuals are technically free to abstain from, for instance, using Google products and services, but, no doubt, such freedom requires considerable initiative and resources.

How should a consent request be presented?

The answer is that it should be offered "in a clear and concise way", using plain language facilitating to understand the content as well as making it reader friendly.

[683] Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (n 482).
[684] Sloot and Borgesius (n 262) 8.
[685] Shao (n 170).

Another crucial point is that the data subject should be able to separate the information given for each service and product available. For instance, Google's one Privacy Policy – although the last version is in many ways better than the previous ones, it is still too general and therefore might be too vague to grasp for many.[686]. If necessary, especially, in mobile apps, where the screens are smaller and not very ideal to read a lot of information at once, legal design thinking methods could be taken as a model in terms of delivering a complex jargon – legal topics in a plain language. Surely, no one would doubt how creative Google can be in coming up with attractive alternatives to its users. Legal design thinking is used in many ways and especially beneficial for those coming from outside of a particular field. It is a bull's eye scenario for Google. A similar approach can be used with the same simplification principle for technical purposes of better communication, using plain, concise, and clear language, while benefiting from visual aids where necessary. Although most of today's society has become familiar with data privacy and data protection notions, especially after incidents such as Cambridge Analytica[687], their legal and technical backgrounds may be ideal for users to understand the 'backstage' of issues surrounding personal data collection and processing by Google.

"Of course, the use of digital layered privacy statements/ notices is not the only

[686] See Google, 'Privacy Policy' (n 646).
[687] See 'Post-scandal Facebook: will the EU stop treating the tech giant as a trusted partner?' (*Corporate Europe*, May 2018) <https://corporateeurope.org/en/power-lobbies/2018/05/post-scandal-facebook-will-eu-stop-treating-tech-giant-trusted-partner> accessed 4 May 2019. However, on the updates related to the Cambridge Analytica incident, see: 'Judge rules against my liquidiation challenge'(*Crowd Justice*, 2019) <https://www.crowdjustice.com/case/scl/> accessed 5 May 2019; see also related cases such as the 'Cambridge Judgment' (2019) <https://www.judiciary.uk/wp-content/uploads/2019/04/17.04.19-cambridge-judgment.pdf> accessed 5 May 2019; see more in the High Court of Justice at Business and Property Courts of England and Wales [2019] EWHC954 (CH) <https://www.judiciary.uk/judgments/vincent-john-green-mark-newman-v-cambridge-analytica-uk-limited-others/> accessed 5 May 2019.

written electronic means that can be deployed by controllers. Other electronic means include "just in time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means, which may be used in addition to a layered privacy statement/notice, might include videos and smartphone or IoT voice alerts. "Other means", which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts.

Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

In sum, more innovative methods could be tried to achieve the purposes of the GDPR. The request has to specify what use will be made of user's personal data and include contact details of the company processing the data. Consent must be freely given, in a specific, informed, and unambiguous manner.[688] Informed consent means that the user must be given information about the processing of their personal data, including at least: the identity of the organisation processing data; the purposes for which the data is being processed; the type of data that will be processed; the possibility to withdraw consent (for example by sending an email to withdraw consent), where applicable; the fact that the data will be used solely for automated-based decision-making, including profiling; information about whether the consent is related to an international transfer of your data; and the possible risks of data transfers to countries outside the EU if those countries are not the subject of a

[688] European Commission, 'How should my consent be requested?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en> accessed 20 April 2019.

Commission adequacy decision and there are no adequate safeguards.[689]

Legitimate Interests

Pursuant to Article 6(1)(f), processing of personal data may in certain circumstances be based on the data controller's 'legitimate interests'.[690] Google states in its Privacy Policy the following:

> *"When we're pursuing legitimate interests, we process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for things like: […] Marketing to inform users about our services; Providing advertising to make many of our services freely available for users."*[691]

Data collected through 'Web & App Activity' is used for advertising purposes. As presented in earlier Chapters, the default setting is 'on', or in other words, unlike 'Location History' the setting is opt-out. Thus, it would be reasonable to assume that Google is not relying on consent. The only remaining ground left for processing the users' data is 'legitimate interests' according to its Privacy Policy.

Pursuant to Article 6(1)(f) of the GDPR, the processing of personal data is lawful

---

[689] See Articles 6 and 7 and Recitals (42) and (43) of the GDPR and EDPB Guidelines on Consent under Regulation (EU) 2016/679.

[690] For a discussion on the legitimate interests in the GDPR and ePrivacy Regulation, see 'Position Paper – ePrivacy Regulation' (2019) <https://www.bitkom.org/sites/default/files/2019-03/20190307_Bitkom%20Position%20Paper%20on%20ePrivacy.pdf> accessed 4 May 2019: *"Further processing of metadata and a legal basis for processing for legitimate interest (as provided for in the GDPR) must be made possible."*

[691] Google, 'When you use our services, you're trusting us with your information' (n 253).

if it is "necessary for the purposes of the legitimate interests of the controller". Nevertheless, if a data controller relies on legitimate interests for processing personal data, this should be proportionate and meaningful, as it must be balanced against the interests of the data subject or his/her fundamental rights. A legitimate interest must also be "lawful", "sufficiently clearly articulated", or in other words, it must be transparent and must "represent a real and present interest".[692]

The terms of service stipulate that Facebook process personal data as specified, in particular, in the data and cookie policies. Pursuant to these policies, Facebook also collects data on users and their devices outside of Facebook-related activities via Facebook Business Tools integrated by advertisers, app developers, and publishers. Facebook processes user data across other Facebook companies and products, and collects user and device-related data from its corporate services. As a legal basis for data processing, Facebook claims that the data are required to provide the service and to fulfil Facebook's legitimate interests.[693]

7.4. TRANSPARENCY

As illustrated in Chapters 1 and 2, the information provided about the specific purposes and exact scope of data collection via 'Web & App Activity' is unclear. The fact that location data is collected as a part of this setting is veiled behind extra clicks, and information stating that this data may be used for advertising is only available under limited circumstances. Additionally, the fact that 'Web & App Activity' is enabled by default is 'out of sight' when setting up a Google account. Likewise, in the limited contexts where Google actually provides information about this data being used for advertising, the description of how the data is used is

[692] Working Party 29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller' (n 450) 25, 52.
[693] Bundeskartellamt (n 436).

ambiguous:

> *"The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings you want to save data in your Google Account."*[694]

> *"Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services."*[695]

After clicking "Learn More" and choosing Android or iPhone/iPad:

> *"See & control your search activity: If Web & App Activity is turned on, your searches and activity from other Google services are saved to your Google Account, so you may get better search results and suggestions. You control what's saved. And you can delete your past searches and activity or turn off Web & App Activity at any time. Note: If you got your Google Account through work or school, you could*

[694] 'Activity controls' (*Google)* <https://myaccount.google.com/activitycontrols/search> accessed 3 May 2019.
[695] ibid.

need to contact your administrator to turn on the Web & App Activity service for your organization."[696]

Similarly, after clicking "Learn More" below the statements given above, there comes the heading of "How your saved activity is used", creating an expectation that the user will learn whether his/her the data is being used for advertising. Unfortunately, right below this heading, is where the disappointment comes – again leading the user to click once more to find out about how the data is being used by Google:

"Learn more about how Google uses your saved activity and helps keep it private. For more information about how Google treats search queries generally, see the Privacy Policy FAQ."

When the user clicks on "how Google uses your saved activity", he/she is being directed to the Google Safety website[697], where there is one huge statement written in blue: "Making technology for everyone means protecting everyone who uses it."

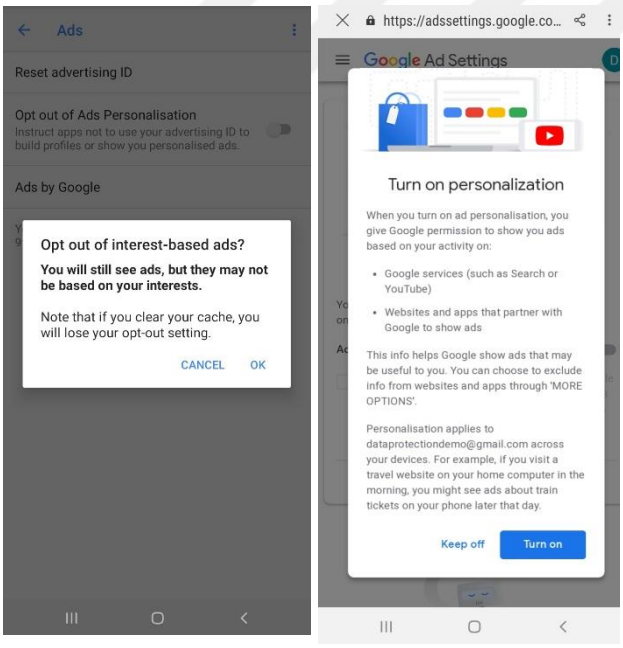
After scrolling down (another extra move only for the remaining users who are too dedicated to find out), there is absolutely nothing related to Google's use of collected data for advertising purposes. Still, if the user is persistent enough - or at that point would the correct word be 'obsessed' enough not to give up - or successfully managed to keep his/her concentration to see a third sub-menu next to the "Safety" section, to which Google directs the user offering to give information

[696] 'See & control your Web & App Activity' (*Google)* <https://support.google.com/websearch/answer/54068?p=web_app_activity&hl=en&authuser=0&visit_id=636919648712155099-2836341069&rd=1&co=GENIE.Platform%3DAndroid&oco=1> accessed 26 April 2019.
[697] 'Safety' (*Google)* <https://safety.google/> accessed 27 April 2019.

about Google's usage of the user's data. Then finally, there is a statement related to ads:

> *"ADS AND DATA: We do not sell your personal information to anyone; We use data to serve you relevant ads in Google products, on partner websites, and in mobile apps. While these ads help fund our services and make them free for everyone, your personal information is not for sale. And we also provide you powerful ad settings so you can better control what ads you see."*[698]

Figure 7.8: Ads Personalisation Opt-Out Request & Ads Personalisation Turn 'On' Page Content



Source: Samsung Galaxy A10 2019 Screenshots

[698] Google, 'Safety Center – Data Privacy' (n 467).

There is no information whatsoever related to how the data collected from 'Web & App Activity' are being used differently than other products. Moreover, this creates even more confusion if the user has turned off, or simply did not turn on, another one of Google's products search history, such as YouTube. The resulting statement is too general and definitely does not provide specific information regarding the use of data. However, there is no information stating that this is applicable to all the products.

There is a clear effort to generalise what Google does, and how it uses the data collected from data subjects. Is it extremely difficult to make a list of the products and to write what data is being collected, when, for what purposes, and how this data is being used? Google pushes its users to find out more about Google itself on research papers or newspapers, rather than its own online sources. For the purposes of right of access, there is a clear failure to allow data subjects to enjoy their rights under the GDPR. So to sum up, this phrasing appears "to be a blanket disclaimer that permits a wide range of purposes for using data collected through 'Web & App Activity'; consequently, as the purposes for the collection and use of personal data from 'Web & App Activity' are unclear, this does not seem to fulfil the requirement for legitimate interest as a legal basis."

7.5. BALANCING TEST

Keeping in mind the discussions held in the above Chapters, for the purposes of Article 6(1)(f) and Recital 47 of the GDPR, Google, as the data controller, should perform a balancing test. This balancing test requires a diligent consideration of whether Google has a legitimate interest that overrides the individual's interests, rights, and/or freedoms, for legitimate interest to be a valid legal basis for processing personal data.

There are a number of features that must be taken into account when carrying out a balancing test. These features are the nature of the interests of the controller; the possible prejudice suffered by the controller; the nature of the data; the status of the data subject; and how the data is processed. Also, the data controller should carefully consider and respect the data subjects' fundamental rights and/or interests that could be impacted.[699] As discussed in the beginning of this Chapter, rights to privacy and data protection are fundamental rights in the EU.[700] Therefore, there needs to be a high barrier that is set aside for individuals' rights and interests in privacy matters.[701]

As stated above, Google claims in its Privacy Policy that, it has a legitimate interest to provide "advertising to make many of its services freely available for users"[702]. Nonetheless, the extensive tracking done through the use of features, such as 'Web & App Activity', 'Location History' and products such as Google Assistant, is invasive and aggressive. This is particularly the case when taken into account the fact that the tracking happens regardless of user interaction, as both Android and Chrome send data to Google even in the absence of any user interaction, and that the collected data is retained on a seemingly indefinite basis[703].[704] Consequently, Google's collection of personal data through Google's features is privacy-adverse and detrimental, if not infringing upon, the rights and freedoms of individuals. This negates the possibility of balancing the interests of the organisation and that of the individual, in Google's case. As a result, any legitimate interest to provide

[699] Working Party 29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller' (n 450) 55.
[700] See Art. 8(1) of the Charter of Fundamental Rights of the European Union, Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU), art. 1(2) and Recital 1 GDPR.
[701] Norway Policy Report (n 567) 36.
[702] Google, 'When you use our services, you're trusting us with your information' (n 253).
[703] Norway Policy Report (n 567) 40.
[704] Schmidt (n 3) 32.

advertising could, and perhaps should be, overridden by data subjects' fundamental right to privacy.

7.5.1. Reasonable expectations

Pursuant to "Article 6(1)(f)" and "Recital 47 of the GDPR", in order for a legitimate interest to be valid, a consideration is needed as to whether the data subject had "reasonable expectations" at the time, and in the context of the collection of his/her personal data, to possibly be used for advertising and/or marketing purposes. This consideration should be done objectively, or in other words, without any bias, asking what a reasonable person could possibly expect and looking from an impartial perspective. In the context of the 'Web & Activity' example, whether data subjects have a "reasonable expectation" to believe that Google is tracking their location for marketing purposes is arguable. As discussed in Chapter 2, Google is largely collecting this information as users sign up for a Google account, and as previously demonstrated, Google does provide some information to the user. Nowadays, due to the increasing number of news in the media, informing the readers about data protection and privacy issues, more and more people are becoming aware of processing practices.

In contrast, many data subjects are most likely entirely unaware of this processing when they first create their Google account. In such a case, the data subject can be said to not have reasonable expectation for the personal data processing at the time when Google started collecting the data. Similarly, intendedly, or unintendedly, users who enable 'Location History' may not realise the scope, or may not be aware of the extent of Google's tracking, and how and for what purposes Google uses this data. This could especially be relevant in younger users, or with people who distinctly do not have any fundamental information regarding data processing for any reason.

Another question to ask is whether the context of personal data collection may give users reasonable expectations that their location data can be used for advertising purposes. This needs to be considered carefully, since as discussed throughout this thesis, the extent of personal data collection for the purposes of advertising is under-communicated and veiled in the presentation of 'Location History', 'Web & App Activity' and Google Assistant. In fact, this under-communication could be frustrating to a user who is, at the same time, constantly being nudged and pestered with "turn on" consent requests by Google, while actually he/she is not being given important information relevant to his/her own personal data by Google – the very party asking for his/her very request. This resistance by Google to provide data subjects with the necessary information, while undermining their rights under Chapter 3 of the GDPR, simply empowers media outcry or possible dis-information campaigns. As a result, this situation, if continued, is likely to cause more paranoia, in tarnishing the reputation of Google even further, regardless of the fact that such damage would most likely not have a considerable effect on Google's business in the short term.

However, it is noteworthy that escalating discussions about Google and other IT giants, when read together, may cause more confusion than reading Google's Privacy Policy. Some data subjects might prefer not to make any additional effort, and instead of being demanded to click on "learn more" again, they could simply decide to evade increasingly judging consent questions and convince themselves – even if temporarily – of the following: That, Google headlines on its support pages like "Google doesn't sell your personal information to anyone", or "You're in control" and "We build privacy that works for everyone", are simply untrue. This discussion does reflect that many data subjects may not necessarily have reasonable expectations for Google's data processing for advertising purposes. Moreover, because 'Web & App Activity' is turned on by default, they are likely to not see

any information about location data being collected. Therefore, the data subject could possibly not have reasonable expectations for Google's processing of their data on such a comprehensive scale.[705]

In the context of balancing interests, data controllers – in this case, Google – are recommended by the Article 29 Working Party to demonstrate the reasons they have for claiming that their own interest overrides the data subject's interests and rights.[706] This should be demonstrated in a clear and user-friendly way, and applicable grounds must be established, otherwise the data subject has the right to object under Article 21 GDPR.[707] Moreover, in reverse, in situations where the data subject does not have reasonable expectations of personal data processing, for the purposes of Recital 47, this will imply that the data subject's interests and rights will override the controller's interests. As the Norway report and Schmidt's landmark research show, for Google to collect users' personal data, the users do not necessarily have to be using the app. Google can perform its personal data collection through passive means, in the background and without an active user of the app at the time of collection.[708] In other words, as discussed in Chapter 2, for Android users this is the case when their mobile phone are dormant, or at the same place as stationary, while the user is neither touching the Android phone nor carrying it.[709] Putting all such information together, as Norway opines[710], it could be concluded that it is likely for the lack of a reasonable expectation at the time of data collection to tip the balance in favour of data subjects' interest.

[705] Norway Policy Report (n 567) 41.
[706] Working Party 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 292).
[707] ibid 42; also see Art. 21 GDPR.
[708] See Norway Policy Report (n 567) (Chapters 3.1 and 3.4. 7-9); also Schmidt (n 3) 3.
[709] Schmidt (n 3) 3, 21.
[710] Norway Policy Report (n 567) 41.

7.6. SAFEGUARDS

The implementation of safeguards has a crucial part in the context of legitimate interests. This is because they can directly affect the scope of the legitimate interests by modifying the legal basis for processing personal data via the use of legitimate interests.[711] These include, but are not limited to the safeguards of anonymization, opting out of the processing of personal data and specific transparency measures, like simple, user-friendly deletion tools.

Google claims to anonymise data. However, as discussed in the previous Chapters, according to Schmidt's report, anonymous data can be easily re-identified as long as the user connects to their Google account.[712] As presented in Chapter 2, Google also carries out its data collection through publisher and advertiser products, and associate such data with numerous identifiers that are described to be "semi-permanent" and "anonymous." Schmidt shows that Google has the ability to associate such identifiers with a user's personal information.[713] This report is quite recent, but coincidentally, Google changed its Privacy Policy right afterwards. Despite this change, when both versions are looked into, it can be observed that Schmidt's comments are still applicable, since the changes shown in Figure 7.9 and Figure 7.10 could be seen as trivial in terms of data collection. In fact, Google, itself, proves this true in its statement where it expresses that, Google has not changed anything in its practice, but this amendments in the Privacy Policy is to improve service[714].

According to Schmidt, Google's ability to associate anonymised data with user's personal information is insinuated by the statements made in Google's previous

[711] ibid.
[712] Norway Policy Report (n 567) 19.
[713] Schmidt (n 3) 19.
[714] Google, 'When you use our services, you're trusting us with your information' (n 253).

Privacy Policy, as mentioned before. Nothing has changed, in this sense, in Google's novel Privacy Policy, excerpts of which are shown in below. The comparison of "your activity on other sites and apps" sub-menu is as follows:

> *"your activity on other sites and apps"*[715]*: This activity might*[716] *come from your use of Google services (previously, "Google products"), like from syncing your account with Chrome (previously, "like Chrome Sync") or your visits to sites and apps that partner with Google (previously, "or from*[717] *your visits to sites and apps that partner with Google"). "Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it*

[715] 'Your activity on other sites and apps' (*Google)* <https://policies.google.com/privacy/example/your-activity-on-other-sites-and-apps> accessed 30 April 2019.

[716] Also see Working Party 29, 'Guidelines on transparency under Regulation 2016/679' (n 663) 9. Also, the power of the English language in legal drafting difference between May and might – which may be applicable to Google's choice of words. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the Second language(s) so that the translated text does not have to be deciphered or re-interpreted.

[717] Although it may not be relevant for the purposes of this Section, the difference in the use of linking words is worth mentioning for the purposes of consent and transparency, there is a clear amelioration of English grammar and usage – parallelism (showing Google's efforts in making the text as short – simple and also correct as possible). Such practices show how big companies, blogs, newspapers or leading figures', both as individuals and companies, can educate and affect people's education or use of language.

might embed other content (such as videos from YouTube)". These services (previously, "products"), MAY[718] (previously, there was no use of "may") share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may[719] be associated with your personal information."

The left text box states in a plain language, clearly, that Google may associate data from advertising services and analytics tools with the data subject's personal information, depending on his/her account settings. As discussed before in this Chapter, Google employs the use of "Web & App Activity" in order to collect data.

[718] Their practices have not changed since they were already NOT selling the users' data. Therefore, it could be concluded that since their practice did not change in terms of business and sharing as well, whether they mis-wrote the previous statement in their Privacy page before, or they still do share it, but chose to add the word "may" for some purpose, which is not apparent since it was not announced. Another argument related to this statement, could be that, the use of word "may" made the statement sneakier or suspicious or pretentious since telling the users that they DO SHARE their information may be more straightforward for most of the readers. However, on the other hand, when the whole phrase is taken into consideration, the previous version did inform the users that Google shares their information – is the activity information can be considered as personal data? These products share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with users' personal information. For the previous version, see Google, 'Your activity on other sites and apps' (n 715). For more information: *"Examples: This activity might come from your use of Google products like Chrome Sync or from your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These products share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information. Learn more about how Google uses data when you use our partners' sites or apps."*

[719] The use of "may" here did not change.

This arrangement is enabled by default. This is why anonymization can be considered as not very effective. It could even be argued that anonymization is basically a façade, holding back the meaning of the word and working against its main objective[720] of being a safeguard, under which circumstances, it cannot be used for the purposes of legitimate interest – meaning that Google may lack a valid ground recognised by law in order to process location data for marketing purposes via "Web & App Activity".

This seems to almost be in reminder of, and agree with, the Working Party 29's statement previously shared in 2014, especially,

> *"for tracking[721] and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."*[722]

CNIL furthers this conclusion in its 2019 decision, and states that, in the interest of:

[720] For anonymization's objective, see ENISA (n 18).
[721] Ryan (n 449). As previously noted, *"This stickiness is due to the tracking IDs and other information specific to you and your device, which is routinely included in ad auction 'bid requests'. Tracking IDs and other personally specific information are not strictly necessary for ad targeting, but they make it easy for companies to re-identify and profile you."*
[722] Working Party 29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 450): *"when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, inadequate information and lack of valid consent…the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company."*

> *"inadequate information and lack of valid consent…the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company."*[723]

This function saves user activity on Google sites and apps, including associated information like location, to give users faster searches, better recommendations and more personalised experiences in Maps, Search and other Google services.

Another change, which should be pointed out, is in the 'Web & App Activity' section in the setting of "My Account". Unfortunately, this change is not publicly available on the website link provided in Schmidt's report, unlike the Privacy Policy changes and the Privacy Page website link. The latter, on which Schmidt has provided (see Figure 7.10) the left text box[724], shows a clear warning written on the top of the page, stating:

> *"This content is from an archived version of our Privacy Policy. See here725 for our current Privacy Policy."*

As it can be seen, the statement directs the user to the updated version of the Privacy Policy. Whereas, in the right text box, the link does not direct, nor does it show the user the new version of the statement. To the contrary, the link opens up the new content without mentioning any changes occurred, and the user is not given any

[723] This Figure is taken from page 19 of Google's Data Collection and the Privacy Policy is archived. However, it can still be found in the following: Google, 'Your activity on other sites and apps' (n 715); also see Google, 'Activity controls' (n 694).
[724] ibid.
[725] Google, 'Privacy' (n 646).

information related to the reason or the date of this change. Thanks to previous research papers and reports[726], the change can be observed to some extent as far as the previously studied information and examples allow. The current content states that 'Web & App Activity'[727]:

> *"Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services."*[728]

The above statement specifies that the activity is saved on Google sites and apps, whereas, in the old version as shown in Figure 7.10, there is no mention of Google in terms of the saving activity[729]. Thus, the scope of the places where the user's activity is saved may have led to some confusion, resulting in questioning the extent of Google's reach. The old version stated the following:

> *"Web & App Activity save your search activity on apps and in browsers to make searches faster and get customized*

[726] Norway Policy Report (n 567).
[727] Google, 'Your activity on other sites and apps' (n 715); Google, 'Activity controls' (n 694).
[728] ibid.
[729] Whether this information was provided in the "Learn More" sub-menu of the old version – not the previous one because there is no proof showing that the content on this website had not been changed between August 2018 and April 2019 – is not available for access to users. Therefore, this thesis assumes that the information was not provided, even if it was, again, it could have been argued that the fact that the lack of the precision about the "apps" and "browsers" and Google's choice of delivering this information on the sub-menu is not logical for the purposes of making the statement as accurate and precise as possible nor understandable for the purposes of transparency.

experiences in Search, Maps, Now, and other Google products."

No user has to naturally know, or make an extra effort to connect the dots when he/she reads "browser" to make an assumptions or understand the meaning behind what is not being said about the privacy of his/her data. This is an unrealistic, and even slightly "discriminatory"[730] expectation of all users that log in to Google services. However, it is worth mentioning that, the most updated statement relatively clarified some details for users, by specifying that "Web & App Activity save your search activity on apps and in browsers." Related to tracking of browser history, Google also mentions the following in both sections dedicated to Android and iPhone users:

"Browser History: in the Activity controls page, you can also check the box to "Include Chrome browsing history and activity from websites and apps that use Google services." When this box is checked, you can control whether activity from your device is saved. Your searches and the sites you visit may also be stored in your browser or the Google Toolbar. Learn how to delete your history on Chrome, Toolbar, Safari, Internet Explorer, or Firefox."

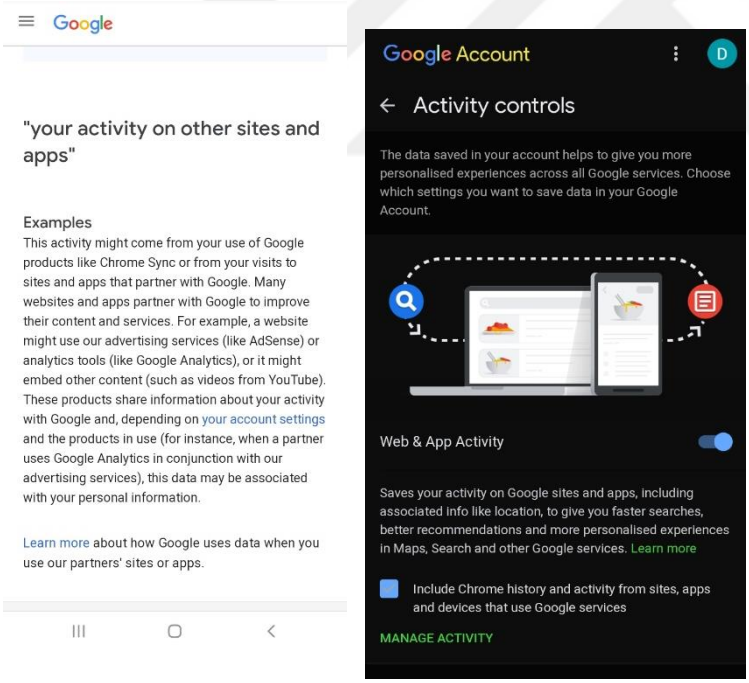
Google provides the following regarding the data saved under the heading "What's saved as Web & App Activity" when the user clicks on "Info about your searches

[730] For more information on the interlink between discrimination against individuals with disabilities and "ethical and privacy" rights, see: Abelardo Pardo and George Siemens, 'Ethical and privacy principles for learning analytics' (2014) British Journal of Educational Technology 45(3).

& more":

> *"When Web & App Activity is on, Google saves information like: Searches and other things you do on Google products and services, like Maps Your location, language, IP address, referrer, and whether you use a browser or an app Ads you click, or things you buy on an advertiser's site Information on your device like recent apps or contact names you searched for Note: Activity could be saved even when you're offline."*[731]

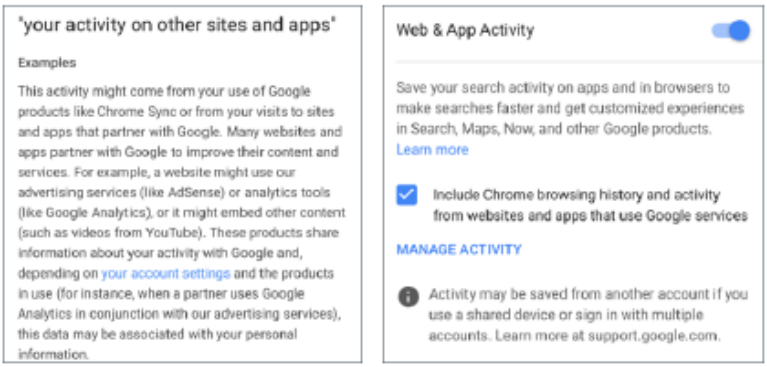
Figure 7.9: Current Web & App Activity Settings



Source: Samsung Galaxy A10 2019 Screenshots

[731] Google, 'See & control your Web & App Activity' (n 696).

Figure 7.10: Previous Web & App Activity Settings



Source: Android from Schmidt (n 3).

Previously on Android, with respect to 'Web & App Activity' controls, when giving consent, the user consents to "Include Chrome browsing history and activity from websites and apps that use Google services" – where the statement itself does not include the fact that data are also saved onto shared devices. However, there is an informational note below that shows "activity may be saved from another account if you use a shared device or sign in with multiple accounts." (Schmidt 19). However now on Android, as can be seen in the screenshot, the user is not provided such an additional information when being asked for consent – while the term 'device' itself is included in the statement the user consents to, where it says, "Include Chrome history and activity from sites, apps and devices that use Google services."

The last note stating that user activity could be saved, even when the user is offline, does not provide any further information, nor does it include a "learn more" link. For the purposes of consent, showing a user that offline access is possible, does not necessitate automatically activating this feature, without the explicit consent of the

user to decide whether he/she requests offline capabilities. Also, this content is taken as a given by Google, even without a detailed explanation of what this feature entails, as a "learn more" link is not even included. Overall, this is also in violation of the purposes of consent as protected under GDPR.

Secondly, regarding the data saved under the heading, "What's saved as Web & App Activity", when the user clicks on "Info about your browsing & more", the information below appears:

"Google can save information like: Websites and apps you use; Your activity on websites and in apps that use Google services; Your Chrome browsing history To let Google, save this information: Web & App Activity must be on. The box next to "Include Chrome browsing history and activity from websites and apps that use Google services" must be checked. Your Chrome history is saved only if you're signed in to your Google Account and have Chrome Sync turned on. Learn about Chrome Sync."

Note: If you use a shared device or sign in with more than one account, activity might be saved to the default account on the browser or device you use."[732]

It is noted here that the above-given information provided by Google, regarding the data saved under the heading, "What's saved as Web & App Activity," are the same for both Android and iPhone platforms. For Android users, Google provides the following statement under the "Turn Web & App Activity on or off" heading after the user clicks on "Learn More" [733]:

"If you turn the switch on, you can check the box next to "Include Chrome browsing

[732] The information is the same for Android and iOS users, for which, see: Google, 'See & control your Web & App Activity' (n 696).
[733] Google, 'Activity controls' (n 694).

history and activity from sites, apps, and devices that use Google services." When this box is checked, you can control whether app activity from your device is saved. Optional: To choose whether app activity from your device is saved, tap Data from this device, then tap the switch or checkbox.

Note: Some browsers and devices may have more settings that affect how this activity is saved."[734]

On the other hand, for iPhone users, Google provides the following information under the "Turn Web & App Activity on or off" heading:

> *"If you turn the switch on, you can check the box next to "Include Chrome browsing history and activity from websites and apps that use Google services." Note: Some browsers and devices may have more settings that affect how this activity is saved."*[735]

As it was previously shown, data subjects can pause the setting and opt out of "Web & App Activity". Yet, it is questionable whether most of the users would ever "opt out" of "Web & App Activity"; this is because, the users might be unaware of the fact that the setting is turned-on by default. Additionally, everyday users will not be aware of that location data is being collected, that this data is used for advertising purposes, or even that "Web & App Activity" exists in the first place.[736] The Norway Report states that, because of the higher threshold to protect individuals' rights and interests in privacy issues, Google's interests do not override the data

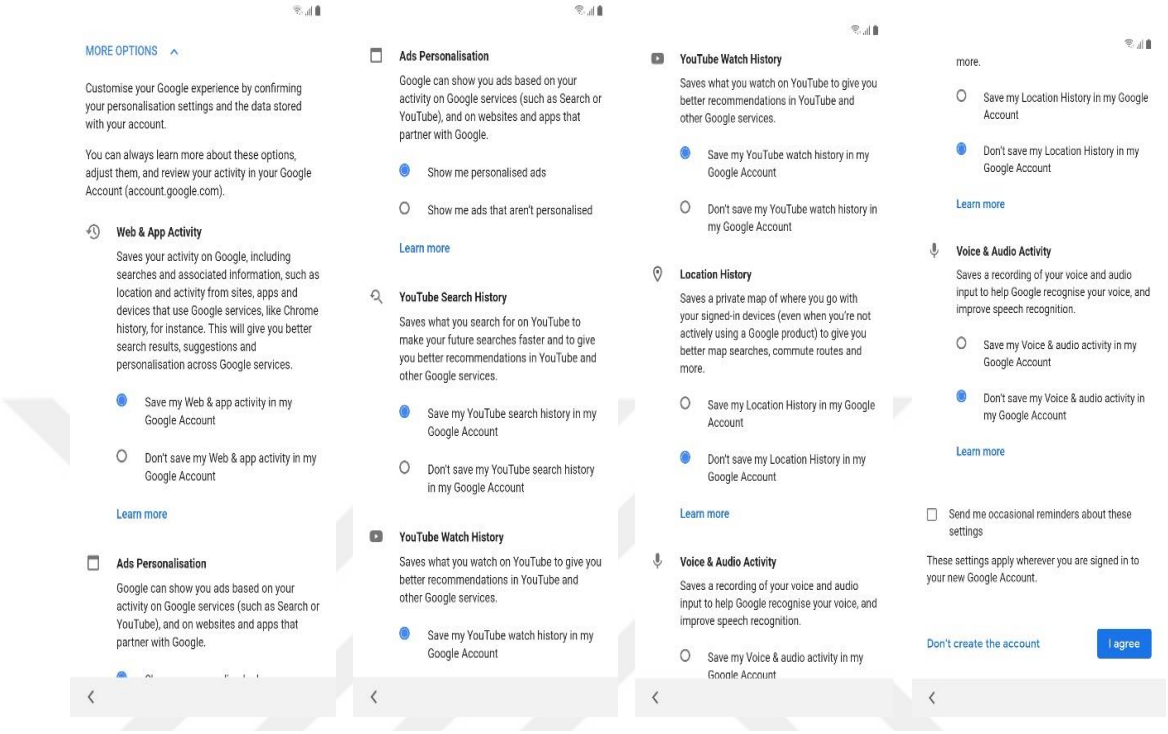
[734] Google, 'See & control your Web & App Activity' (n 696).
[735] ibid.
[736] Norway Policy Report (n 567) 42.

subject's interests and rights in this case.

However, at the same time, it could be argued that this reason may not be considered as a compelling one in time, because if this is primarily a problem of transparency and communication, then by simple changes to be carried out on Google's website and policy, Google could potentially have legitimate grounds. It could be suggested that Google openly and concisely inform its users about the means in which it processes their data. However, for Google to fully achieve to value the acquisition of a "freely given", "informed", "specific" and "unambiguous" indication of users' intent, it needs to resolve its issues around the GDPR. It needs to fully accept that consent and transparency are vital for the purposes of rights to privacy and data protection, which are fundamental rights, and as such, the rights and interests of the user will continue, only to grow exponentially in value, to be treasured in data privacy issues.

Moreover, it could be assumed that Google offers more options to its users with smartphones running Android OS, as opposed to Google users with smartphones running iOS. This also delineates Google's inclusion in the Android platform, as discussed in Chapter 2. However, with regard to a timing comparison between the prior and current statements, as the previous versions of these statements are not publicly available to users, further commentary might not be relevant or accurate.

Figure 7.11: Google Account Setup - All Default Permission Sets



Source: Samsung Galaxy A10 2019 Screenshots

Children's Rights

As pointed out in Chapter 3, several further requirements are delineated in the GDPR with respect to children's data, for reasons set out in Recital 38. In addition to the GDPR, other laws and regulations aim to enhance children's protection and safeguard their rights, especially with the increasing use of mobile devices and video-games or apps being preferred to the point where such devices are seen as a replacement of old-times' toys.

This theory holds much value, since it represents the first example of EU's

interpretation of children's data as definitively qualifying for its protection.[737] However, it does introduce certain issues regarding the concept itself, as well as its practice – namely due to a lack of more compelling empirical foundation. These issues concern the following:

Firstly, children's media literacy, in the sense that, their "level of awareness of the risks associated with personal data processing and of their rights in this regard is unclear"[738]; second issue to look into concerns the harm that the regulation pursues to escape from. As Livingstone explains, such harm encapsulates particularly harm arising from profiling conducted for commercial purposes.[739] Lastly, as Livingstone draws attention and further discusses "the implied nature of family relations, including parental responsibility, parental media literacy, children's need for privacy from parents, and the readiness of families to act as assumed by the regulation"[740] are of high importance and deserve scrutiny when children's rights and possible harms that data protection laws aim to evade are taken into account.

The EU's AVMSD, revised in November 2018, with its wired provisions to reinforce the enhancement of children's protection and safeguard of their rights targeted inappropriate audio-visual commercial communications for foods threatening their health and well-being[741]. Such provisions also support the enhancement and encouragement of codes of conduct at EU level regarding such matters, where necessary. For the purposes of this thesis, AVMSD's most relevant

[737] For more information on children's rights against advertising practices, see Sonia Livingstone, 'Children's digital rights' (2015) Intermedia 42(4/5) 20-24.
[738] See more information in YouTube, 'YouTube Kids Privacy Notice' (n 259).
[739] Livingstone, *Children: a special case for privacy?* (n 313) 19, 23.
[740] ibid.
[741] See also OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) 195-98 <http://www.oecd-ilibrary.org/deliver/9789264229358-en.pdf?itemId=/content/book/9789264229358-en&mimeType=application/pdf> accessed 13 May 2019.

content concerns video-sharing platforms. This is because, since November 2018, video-sharing platforms are expected

> *"To respect certain obligations for the commercial communications they are responsible for and to be transparent about commercial communications that are declared by the users when uploading content that contains such commercial communications."*[742]

Last, it is important to denote that UNICEF stresses, "Obtaining free and informed consent is the approach most consistent with children's rights" even though there may be other legally recognised grounds for data processing.[743]

However, as Livingstone states UNICEF's statement may, however, most likely to result in an unwanted outcome, more specifically, a restriction of children's participation and use of social media despite its provision of a strengthened protection of children's data.[744] The protection of children's rights is becoming increasingly effective over time, and the awareness growing from its imperative nature is openly reflected upon the regulations it has induced, as well as the shifting approach of the relevant authorities.

---

[742] See AVMSD (n 558). Regarding the revision of AVMSD, see also 'Revision of the Audiovisual Media Services Directive (AVMSD)' <https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd> accessed 30 March 2019. See more in Articles of the AVMSD that address children's rights as per Art. 9/11/20/47/60/61 ('on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services.

[743] UNICEF, 'Industry Toolkit: Children's Online Privacy and Freedom of Expression' (2018) <https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf> accessed 17 February 2019. See also Livingstone, 'Children's digital rights' (n 737).

[744] Livingstone, *Children: a special case for privacy?* (n 313) 22, 23: *"an age of consent deliberated would apply to teenagers' use of all of a social networking service, as originally expected by many, in most countries, thereby protecting them but also restricting their participation for longer."*

CHAPTER EIGHT

8. THE WAY FORWARD

As discussed above, the "freemium"[745] business model of Google is concentrated on offering "free services". These services are also underwired to gather personal data and optimize information in order to feed Google's advertising business.[746]

Details from the iOS platform were previously mentioned to underscore important differences. Android and iOS platforms have their differences, which are often reflective of the business model and approach of their respective parent organisations.[747] Google prioritises complimentary services and software that are programmed to gather and optimise data for advertisement purposes, whereas Apple largely focuses on device or hardware sales as the main driver of business. It is significant to include comparisons with the iOS platform and underline divergences wherever applicable. However, it is noteworthy that iOS and other mobile platforms must be prioritised for future research and analysis to gain a better understanding of the practices analysed in the field of data protection.[748]

Also, the opinions and reports of ENISA, EDPS should be revisited and updated regularly even if the essences of the points they make do not change, as the technology improves, the need for new examples covering today's practical means show up. Although they do not have binding effect, they provide a great understanding with the plain language and examples used.

---

[745] See Chapter 3; also see Medium (n 279).
[746] "Whereas, Apple's business model depends predominantly on the sale of physical devices." See ENISA (n 18) 25.
[747] Yerukhimovich et al (n 7) 9.
[748] ENISA (n 18) 25.

CONCLUSION

This thesis aimed to answer the below given questions:

1 – To what extent Google's data collection practices on mobile platforms coincide with the requirements prescribed by the principles of data minimisation, purpose limitation, and accountability?

2 – Does Google's Privacy Policy undermine data subject rights?

3 – Overall, is Google at odds with the GDPR?

In order to answer these interlinked questions, this thesis, first identified and further discussed the personal data collected by Google on mobile operating systems, by specifically focusing on the definition and scope of personal data. Secondly, principal data collection methods used by Google are presented to prepare the discussion for the purposes of data collection before delving into the chosen "core principles". Third, purposes of data collection were explained and the core principles of data minimisation, purpose limitation, and accountability were evaluated bearing the main purposes of Google in mind by providing relevant examples from Google's data collection practices on mobile platforms.

The evaluation then moved to Google's practices in scope of its "latest Privacy Policy" and the tensions they create with data subjects' rights, and mainly the notion of transparency with a focus on location and activity data collected through Google's products and services on mobile platforms. Lastly, this research concludes by underscoring the importance of the role of tech giants, including Google, is enhancing rights to privacy and data protection by providing further guidance and clarification to different stakeholders of the mobile ecosystem regarding their practices. Another finding is Google's Privacy Policy needs to be further improved,

especially; in terms of examples given and language used by being, more specific and providing elaborate examples in order to explain the data collection process. These shortcomings, overall, affect Google's compliance in terms of transparency and accountability as well as the two strongly interlinked principles: purpose limitation and data minimisation. Also, the fact that pre-installed apps are still being imposed on the data subjects is underscored in addition to other consent related issues regarding Google's data collection. This thesis points out that, especially, the fact that apps such as Facebook comes automatically when setting up the phone could be seen as intrusive and imposing. However, looking at the big picture, it is an undeniable fact that Google makes considerable efforts in terms of compliance especially concerning its Terms and Privacy statements and features such as automatic delete of location history. Finally yet importantly, mass media's effect on data subjects should not be underestimated. The recent CNIL decision as well as the everyday resurfacing privacy and data protection related rumours when combined with Google's lack of announcements might damage Google's reputation even more. Google needs to be more transparent and vocal about its practices and engagement with data subjects' personal data; this would benefit both Google and data subjects while silencing adamantly claimed accusations against Google.

To sum up, it could be concluded that Google's data collection practices on mobile platforms coincide with the requirements prescribed by the principles of data minimisation, purpose limitation, and accountability to a limited yet better (ameliorating) extent as discussed in Chapters 4, 5, and 6. In addition, this thesis finds that Google's latest Privacy Policy does undermine data subjects' rights to a certain extent, calling for further clarification and elaboration. Overall, Google is not at odds with the GDPR; yet, it certainly is not fully on great terms with it despite Google's recently shown great efforts.

Given the continued growth of mobile technologies, and their ubiquity and digital advertising tools, it is easy to envision that Google is going to collect an increasing amount of personal data. Located in the centre of the data protection combat field, players of smartphone ecosystems whether data subjects or tech giants – having internalised different legal systems, different priorities in terms of values and principles – will find the adaptation difficult and might not easily adopt, not even understand what is being expected with a solid rationale, to a full extent. This could create a different "unbalanced" or in other words "asymmetric" power balance, where dealing with data is brought to being something to be negotiated. This can be very backbreaking since data protection – as much as it constitutes a fundamental right – it also lies at the heart of today's leading data-driven economy. In terms of Google's Privacy Policy – it is unfortunate to see the disappointing results even when taking into account Google's significant efforts in the past few years in light of the GDPR, the fact that progress remains little is disheartening especially in terms of transparency and clarity in its statements. Transparency is the ultimate door opening to building trust and making tech giants life easier in long term. Google should see the GDPR both as a short and long term investment since it compels it to do things by the book, and in fact urges Google to be more "legitimate", "open", and "trustworthy". Google also should remember its position and role as one of the world's top companies, with its tentacles, its reach is endless, its impact on other tech companies as well as society is not even open to question. In fact, Google can try to revolutionize the current perceptions on personal data driven economy, simply by explaining and asking consent for it.

Google has been living Stalin's dream of being everywhere and watching everyone, now, with the increasing awareness created following the GDPR, is the best time to find middle ground. Also, the fact that the GDPR created such an upheaval shows how people globally were ready and in fact needed such a change. Such protection

was a necessity, and therefore it influenced many countries' laws resulting in heated debates. Thus, the GDPR was only the beginning of a new era, where everyone puts their cards on the table trying to balance different rights. The interdisciplinary nature of this field, the emergence of collaboration of legal experts, academics, engineers, and professionals from other disciplines shows how challenging but at the same time how real and fulfilling the task of enhancing data protection right can be. It would be beneficial for the emergence of global data protection standards if the international community would commit more to shaping areas of conjunction between standards in varying jurisdictions all over the world. A common understanding about the different cultural and legal perspectives to data protection around the world would help create the conditions for ultimate development and compliance of an international framework, whereby Google's as well as other tech giants' stance plays an essential role.

BIBLIOGRAPHY

'2 CFR § 200.79 - Personally Identifiable Information (PII)' (*Cornell Law School Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/2/200.79> accessed 15 March 2019

'5Rights Foundation's Response to the Information Commissioner's Call for Evidence' (*5Rights Foundation*) <https://5rightsfoundation.com/static/5Rights_Response_IC_Call_for_Evidence_v2.pdf> accessed 25 February 2019

'Accountability and Governance' (*ICO*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 27 March 2019

'Ad Personalisation' (*Google*) <https://adssettings.google.com/authenticated> accessed 30 March 2019

'Advertising – How Google Uses Cookies in Advertising' (*Google*) <https://policies.google.com/technologies/ads?hl=en-US> accessed 8 April 2019

'Advertising Policies Help – Political Content' (*Google*) <https://support.google.com/adspolicy/answer/6014595?hl=en&ref_topic=1626336> accessed 30 March 2019

'Advertising Policies Help: Personalized Advertising' (*Google*) <https://support.google.com/adwordspolicy/answer/143465?hl=en> accessed 23 March 2019

'Adwords Help: About Customer Match' (*Google*) <https://support.google.com/adwords/answer/6379332?hl=en> accessed 18 April 2019

'Adwords Help: About Demographic Targeting' (*Google*) <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en> accessed 18 April 2019

'Adwords Help: About Remarketing Lists for Search Ads' (*Google*) <https://support.google.com/adwords/answer/2701222?hl=en> accessed 18 April 2019

'Adwords Help: About Similar Audiences on the Display Network' (*Google*) <https://support.google.com/adwords/answer/2676774?hl=en)> accessed 18 April 2019

'Adwords Help: About Targeting Your Ads by Audience Interests' (*Google*) <https://support.google.com/adwords/answer/2497941?hl=en> accessed 18 April 2019

'Adwords Help: Target Customers near an Address with Location Extensions' (*Google*) <https://support.google.com/adwords/answer/2914785?hl=en&ref_topic=3119074> accessed 18 April 2019

Allcott H, Gentzkow M, 'Social Media and Fake News in the 2016 Election' (2017) 31 Journal of Economic Perspectives

Almeida V, Doneda D, Rossini C, 'How Do App Stores Challenge the Global Internet Governance Ecosystem?' (2016) 20 IEEE Internet Computing <https://ieeexplore.ieee.org/document/7781550> accessed 5 April 2019

'An Analysis of the Effects of Smartphone Push Notifications on Task Performance With Regard To Smartphone Overuse Using ERP' (2016) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4912993/> accessed 2 April 2019

'Analytics Help – Sdks' (*Google*) <https://support.google.com/analytics/answer/7373305?hl=en> accessed 24 March 2019

'Analytics Help - Sunsetting the Google Analytics Services Sdks' (*Google*) <https://support.google.com/analytics/answer/9167112?hl=en> accessed 30 March 2019

'Android 1.1 Version Notes' (*Android Developers*, 2009) <https://developer.android.com/about/versions/android-1.1> accessed 23 February 2019

'Android In Europe Benefits To Consumers And Business - Prepared For Google' (*Oxera.com*, 2018) <https://www.oxera.com/wp-content/uploads/2018/10/Android-in-Europe-1.pdf> accessed 4 May 2019

'Anonymisation: Managing Data Protection Risk Code of Practice' (*ICO*, 2018) <https://ico.org.uk/media/1061/anonymisation-code.pdf> accessed 22 February 2019

'Answer to Question No E-007611/17' (*Europarl.europa.eu*, 2018) <http://www.europarl.europa.eu/doceo/document/E-8-2017-007611-ASW_EN.html> accessed 5 May 2019

'Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising' (*European Commission Press Release Database*, 2019) <http://europa.eu/rapid/press-release_IP-19-1770_en.htm> accessed 27 March 2019

'Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service' (*European Commission Press Release Database*, 2017) <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> accessed 27 March 2019

'Antitrust: Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine' (*European Commission*, 2018) <http://europa.eu/rapid/press-release_IP-18-4581_en.htm> accessed 2 February 2019

'Apple Developer Documentation' (*Apple*) <https://developer.apple.com/documentation> accessed 30 April 2019

'Apps/Mobile' (*ePrivacy*) <https://www.eprivacy.eu/en/industries/apps-mobile/> accessed 4 April 2019

Aragon R, 'How Should We Regulate Facial-Recognition Technology?' (*IAPP*, 2019) <https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/> accessed 1 April 2019

Årnes AC Nes, 'What Does Your App Know About You?' (*Datatilsynet*, 2019) <http://www.datatilsynet.no/Global/english/APPrapp_english.pdf> accessed 5 April 2019

Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679'' (2016) <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826> accessed 21 February 2019

Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 28 March 2019

Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 28 March 2019

Article 29 Data Protection Working Party, 'Opinion 02/2013 On Apps on Smart Devices' (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> accessed 10 February 2019

Article 29 Data Protection Working Party, 'Opinion 03/2013 On Purpose Limitation' (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 10 February 2019

Article 29 Data Protection Working Party, 'Opinion 04/2014 On Surveillance of Electronic Communications for Intelligence and National Security Purposes' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf> accessed 24 April 2019

Article 29 Data Protection Working Party, 'Opinion 06/2014 On the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 10 February 2019

Article 29 Data Protection Working Party, 'Opinion 2/2010 On Online Behavioural Advertising' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 20 February 2019

Article 29 Data Protection Working Party, 'Opinion 3/2010 On the Principle of Accountability' (2010) <https://www.dataprotection.ro/servlet/ViewDocument?id=720> accessed 10 April 2019

Article 29 Data Protection Working Party, 'Update Of Opinion 8/2010 On Applicable Law In Light Of the CJEU Judgement in Google Spain' (2015) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf> accessed 30 March 2019

Ashford W, 'Mind the Overlap between GDPR and Epd, Warns Privacy Lawyer' (*Computer Weekly*, 2019) <https://www.computerweekly.com/news/252460345/Mind-the-overlap-between-GDPR-and-ePD-warns-privacy-lawyer> accessed 4 April 2019

Auletta K, *Googled: The End of the World As We Know It* (Penguin Books 2009)

Balducci A and others, ‘A new phase in European privacy law enforcement – CNIL fined Google LLC 50 million euros!’ (DLA Piper Blogs) <https://blogs.dlapiper.com/privacymatters/france-a-new-phase-in-european-

privacy-law-enforcement-cnil-fined-google-llc-50-million-euros/> accessed 25 March 2019.

Baras K and others, 'Supporting Students' Mental Health and Academic Success through Mobile App and IoT' (2018) 9 International Journal of E-Health and Medical Communications <https://www.researchgate.net/publication/320895755_Supporting_Students'_Mental_Health_and_Academic_Success_Through_Mobile_App_and_IoT> accessed 6 May 2019

Bayamlıoğlu I and others, *Being Profiled Cogitas Ergo Sum* (1st edn, Amsterdam University Press BV 2018)

Benedek W, 'Understanding Human Rights' (2012) European Training and Research Centre for Human Rights and Democracy <http://www.manual.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/manual/versionen/english_3rd_edition/Manual_2012_FINAL.pdf> accessed 23 March 2019

'Best Mental Health Apps for Sleep In 2019' (*Mobile App Daily*, 2018) <https://www.mobileappdaily.com/best-mental-health-apps-for-sleeping> accessed 23 February 2019

Binns R and others, 'Third Party Tracking in the Mobile Ecosystem' (*ACM*, 2018) <https://arxiv.org/pdf/1804.03603.pdf> accessed 22 February 2019

'Boletin Oficial Del Estado' (*BOE*, 2019) <https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf> accessed 30 March 2019

Borgesius F, Poort J, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 SSRN Electronic Journal <https://link-springer-com.ezphost.dur.ac.uk/article/10.1007/s10603-017-9354-z> accessed 4 March 2019

'Bringing You the Next-Generation Google Assistant' (*Google*, 2019) <https://www.blog.google/products/assistant/next-generation-google-assistant-io/> accessed 10 May 2019

Broughton Micova S, 'The Playing Field Between YouTube And Television Will Be A Bit Fairer, But Still Far From Level' [2018] LSE Media Policy Project Blog <https://blogs.lse.ac.uk/mediapolicyproject/2018/10/09/the-playing-field-between-youtube-and-television-will-be-a-bit-fairer-but-still-far-from-level/> accessed 25 April 2019

'Browse In Private - Computer - Google Chrome Help' (*Google*) <https://support.google.com/chrome/answer/95464> accessed 15 April 2019

Bu-Pasha S and others, 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' (2016) 2 European Data Protection Law Review <https://edpl.lexxion.eu/article/edpl/2016/3/7> accessed 5 April 2019

'Business Redressal Complaint Form' (*Google*, 2019) <https://support.google.com/business/contact/business_redressal_form> accessed 6 May 2019

'Businesses And Data – We Are Committed To Complying With Applicable Data Protection Laws' (*Google*)

<https://privacy.google.com/businesses/compliance/#!?modal_active=none> accessed 28 April 2019

Buttarelli G, 'The Urgent Case for a New Eprivacy Law' (*EDPS*, 2018) <https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en> accessed 24 March 2019

Bygrave L, 'Data Privacy Law: An International Perspective' (2014) 5 Oxford University Press

'Cambridge Analytica Controversy Must Spur Researchers to Update Data Ethics' (*Nature*, 2018) <https://www.nature.com/articles/d41586-018-03856-4> accessed 15 April 2019

'Campaign Manager Help: About Floodlight' (*Google*) <https://support.google.com/dcm/answer/2823388?hl=en&ref_topic=4241549&visit_id=636927650664772867-2089473498&rd=2> accessed 18 April 2019

Christl W, 'Corporate Surveillance In Everyday Life' [2017] Institute for Critical Digital Culture <https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 24 April 2019

Chu G, N ApthorpeN Feamster, 'Security And Privacy Analyses Of Internet Of Things Children'S Toys' [2018] IEEE Internet of Things Journal <https://arxiv.org/pdf/1805.02751.pdf> accessed 30 March 2019

Clarke R, *A 'Future Trace' On Dataveillance: The Anti-Utopian And Cyberpunk Literary Genres* (Xamax Consultancy Pty Ltd 1993)

Clearwater A, Philbrook B, 'Privacy By Design And GDPR: Putting Policy Into Practice' (*CPO Magazine*,, 2018) <https://www.cpomagazine.com/data-privacy/privacy-by-design-and-gdpr-putting-policy-into-practice/> accessed 17 April 2019

Cluley G, 'Windows Mobile Terdial Trojan Makes Expensive Phone Calls' (*Naked Security by Sophos*, 2010) <https://nakedsecurity.sophos.com/2010/04/10/windows-mobile-terdial-trojan-expensive-phone-calls> accessed 5 March 2019

'CNIL Fines GOOGLE €50M for GDPR Violations | The GDPR Guys' (*The GDPR Guys*, 2019) <https://gdprguys.co.uk/cnil-fines-google-50m-gdpr-violations/> accessed 11 May 2019

CNIL, 'Article 29 Data Protection Working Party: Letter to Google' (2012) <https://www.cnil.fr/sites/default/files/typo/document/20121016-letter_google-article_29-FINAL.pdf> accessed 28 January 2019

CNIL, 'Compliance Package: Connected Vehicles and Personal Data' (2017) <https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_en.pdf> accessed 30 April 2019

CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction against GOOGLE LLC.' (CNIL 2019) <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> accessed 15 May 2019

CNIL, 'Google Privacy Policy: Main Findings and Recommendations' <https://www.cnil.fr/sites/default/files/typo/document/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 31 March 2019

Cohen J, 'Your IPhone Has a Hidden List of Every Location You'Ve Been' (*OneZero*, 2019) <https://onezero.medium.com/your-iphone-has-a-hidden-tracking-list-of-every-location-youve-been-c227a84bc4fc> accessed 20 March 2019

Cole A, 'Internet Advertising After Sorrell V. IMS Health: A Discussion on Data Privacy & the First Amendment' (2012) 30 Cardozo Arts & Entertainment Law Journal

Comandé G, 'Opinions · the Rotting Meat Error: From Galileo to Aristotle in Data Mining?' (2018) 4 European Data Protection Law Review <https://edpl.lexxion.eu/article/EDPL/2018/3/4> accessed 2 May 2019

'Compliance | How Google Complies With Data Protection Laws' (*Google*) <https://privacy.google.com/businesses/compliance/#!?modal_active=none> accessed 2 May 2019

'Concerning The Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation On Privacy And Electronic Communications)' (2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010> accessed 20 February 2019

Constantiou I, Kallinikos J, 'New Games, New Rules: Big Data and The Changing Context Of Strategy' (2015) 20 Journal of Information Technology

Convention on the Rights of Persons with Disabilities <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-31-statistics-and-data-collection.html> accessed 31 March 2019

Couldry N, Mejias U, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2018) 20 Television & New Media <https://journals.sagepub.com/doi/abs/10.1177/1527476418796632?journalCode=tvna> accessed 7 May 2019

Council of Europe, 'Convention 108+: Convention for the Protection of Individuals With Regard To the Processing of Personal Data' (2018) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 13 February 2019

Council of Europe, 'Explanatory Report To The Protocol Amending The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data (Council Of Europe Treaty Series - No. 223)' (2018) <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 14 January 2019

Council of Europe, 'Regulation (EU) 2016/679 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC' (2016)

'Counting down to 25 May 2018: Mapping The GDPR Age Of Consent Across The EU: May 2018' (2018) <https://biblio.ugent.be/publication/8561253/file/8561256.pdf> accessed 30 March 2019

Crawford S, Zittrain J, Brem L, 'Game Changers: Mobile Gaming Apps and Data Privacy' [2012] Harvard Law School Case Studies <https://casestudies.law.harvard.edu/game-changers-mobile-gaming-apps-and-data-privacy/> accessed 3 April 2019

Cyphers B, Kelley J, 'Facebook Got Caught Phishing for Friends' (*Electronic Frontier Foundation*, 2019) <https://www.eff.org/deeplinks/2019/04/facebook-got-caught-phishing-friends> accessed 10 April 2019

'Data Collection - Analytics Help' (*Google*) <https://support.google.com/analytics/answer/6318039?hl=en> accessed 15 April 2019

'Data Masking: Anonymisation or Pseudonymisation?' (*GDPR.Report*, 2017) <https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/> accessed 15 March 2019

'Data Protection Authorities From Over 50 Countries Approve The "Madrid Resolution" On International Privacy Standards' (*Privacy Conference 2009*, 2009) <http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf> accessed 26 March 2019

'Data Protection Guidelines on Apps' (*Data Protection*) <http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Guidelines%20on%20apps.pdf> accessed 19 February 2019

'Data Protection Practitioners' Conference 2019 - Elizabeth Denham's Speech at the Data Protection Practitioners' Conference On 8 April 2019' (*ICO*, 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/04/data-protection-practitioners-conference-2019/> accessed 28 April 2019

'Data Subject Rights And Personal Information: Data Subject Rights under the GDPR' <https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr> accessed 30 March 2019

'Data Transfers' (*Google*) <https://policies.google.com/privacy#enforcement> accessed 31 March 2019

Datta A, Tschantz M, Datta A, 'Automated Experiments On Ad Privacy Settings' (2015) 1 Proceedings on Privacy Enhancing Technologies

De Corniere AG Taylor, 'On the Economics of the Google Android Case' (*Oxford Law Blog*, 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/economics-google-android-case> accessed 2 April 2019

De Hert P and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review <https://www.sciencedirect.com/science/article/pii/S0267364917303333> accessed 12 May 2019

'Deceived By Design: How Tech Companies Use Dark Patterns To Discourage Us from Exercising Our Rights to Privacy' (*Forbrukerradet*, 2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 30 March 2019

'Délibération N°SAN-2019-001 Du 21 Janvier 2019: Délibération De La Formation Restreinte N° SAN – 2019-001 Du 21 Janvier 2019 Prononçant Une Sanction Pécuniaire À L'encontre De La Société GOOGLE LLC' (2019) <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1> accessed 20 February 2019

'Detecting suspicious activity on your account Google' (*Google*) <https://support.google.com/accounts/answer/140921?hl=en> accessed 15 May 2019

Dinant J and others, 'Application of Convention 108 to the Profiling Mechanism: Some Ideas for the Future Work of the Consultative Committee (T-PD): Final Version' (2008) <http://www.crid.be/pdf/public/5945.pdf> accessed 30 April 2019

Directorate of the Jurisconsult, 'Guide on Article 8 of the European Convention On Human Rights (Updated 2018)' (Council of Europe/European Court of Human Rights 2016)

'Do You Protect The Personal Data On Your Smartphone?' (*Eurostat*, 2019) <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20190128-1> accessed 15 February 2019

Doyle S, 'Android Smartphones Collect Ten Times More Data Than iOS Phones, Study Reveals' (*Engineering and Technology*, 2018) <https://eandt.theiet.org/content/articles/2018/09/android-smartphones-collecting-ten-times-more-data-than-ios-phones-study-reveals/> accessed 22 March 2019

'ECtHR MS V. Sweden [1997] (Application No. 20837/92) Para. 41 (“The Protection Of Personal Data Is Of Fundamental Importance To A Person's Enjoyment Of His Or Her Right To Respect For Private And Family Life As Guaranteed By Article 8”).'

'EDPB Releases Opinion on Interplay between the Eprivacy Directive and the GDPR and a Statement on the Eprivacy Regulation' (*Hunton Privacy Blog*, 2019) <https://www.huntonprivacyblog.com/2019/03/19/edpb-releases-opinion-on-interplay-between-the-eprivacy-directive-and-the-gdpr-and-a-statement-on-the-eprivacy-regulation/> accessed 15 April 2019

EDPB, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities' (2019)

<https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> accessed 30 March 2019

EDPS, 'Ethics Advisory Group: Report 2018' (2018) <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> accessed 21 April 2019

EDPS, 'Guidelines on The Protection of Personal Data in IT Governance and IT Management of EU Institutions' (2018) <https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf> accessed 16 February 2019

EDPS, 'Guidelines on the Protection of Personal Data in Mobile Devices Used by European Institutions' (2015) <https://edps.europa.eu/sites/edp/files/publication/15-12-17_mobile_devices_en.pdf> accessed 1 May 2019

EDPS, 'Guidelines on the Protection of Personal Data Processed by Mobile Applications Provided by European Union Institutions' (2016) <https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf> accessed 30 March 2019

EDPS, 'Opinion 3/2018 On Online Manipulation and Personal Data' (2018) <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 10 April 2019

Elvy S, 'Paying For Privacy and the Personal Data Economy' (2017) 117 Columbia Law Review

ENISA, 'Guidelines for Smes on the Security of Personal Data Processing' (2016) <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed 23 April 2019

ENISA, 'Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR' (2017) <https://publications.europa.eu/ro/publication-detail/-/publication/5d1a8d45-0af0-11e8-966a-01aa75ed71a1> accessed 15 January 2019

ENISA, 'Recommendations on Shaping Technology according To GDPR Provisions - Exploring the Notion of Data Protection by Default' (2019) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> accessed 30 April 2019

ENISA, 'Recommendations on Shaping Technology according To GDPR Provisions: An Overview on Data Pseudonymisation' (2018) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions/at_download/fullReport> accessed 15 January 2019

ENISA, 'Threat Landscape Report 2018: 15 Top Cyber Threats and Trends' (2019) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 2 March 2019

Entman L, 'Study of Google Data Collection Comes amid Increased Scrutiny over Digital Privacy' (*Physorg*, 2018) <https://phys.org/news/2018-11-google-scrutiny-digital-privacy.html> accessed 2 March 2019

Esayas S, 'The Idea Of ‘Emergent Properties’ In Data Privacy: Towards A Holistic Approach' (2017) 25 International Journal of Law and Information Technology

Estrada-Jiménez J and others, 'Online Advertising: Analysis of Privacy Threats and Protection Approaches' (2017) 100 Computer Communications <https://www.sciencedirect.com/science/article/pii/S0140366416307083> accessed 18 March 2019

'EU User Consent Policy' (*Google*) <https://www.google.com/about/company/user-consent-policy.html> accessed 24 April 2019

'European Economic Area (EEA) / Relations with the EU' <https://www.efta.int/eea> accessed 30 March 2019

European Union Agency for Fundamental Rights, 'Handbook on European Data Protection Law - 2018 Edition' (2018) <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 15 February 2019

'Evidence-Based Consumer Policy' (*European Commission*) <https://ec.europa.eu/info/policies/consumers/consumer-protection/evidence-based-consumer-policy_en> accessed 30 April 2019

'Facebook, Exploitative Business Terms Pursuant To Section 19 (1) GWB for Inadequate Data Processing' (*Bundeskartellamt*, 2019) <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4> accessed 9 May 2019

Farzad R, 'Google At $400 Billion: A New No. 2 in Market Cap' (*Bloomberg*, 2014) <https://www.bloomberg.com/news/articles/2014-02-12/google-at-400-billion-a-new-no-dot-2-in-market-cap> accessed 17 February 2019

Fernee H, Sonck N, Scherpenzeel A, 'Data Collection with Smartphones: Experiences in a Time Use Survey' [2013] The Netherlands Institute for Social Research <https://ec.europa.eu/eurostat/cros/system/files/NTTS2013fullPaper_204.pdf> accessed 28 April 2019

Finamore E, Dutta K, 'Tesla Boss Elon Musk Warns Artificial Intelligence Development Is 'Summoning the Demon' (*The Independent*, 2014) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/ tesla-boss-elon-musk-warns-artificial-intelligence-development-is-summoningthe-demon-9819760.html> accessed 14 March 2019

Floridi L, 'The Onlife Manifesto: Being Human in a Hyperconnected Era' (2015) 64 Library Review <https://www.emeraldinsight.com/doi/abs/10.1108/LR-04-2015-0034> accessed 3 January 2019

Forbrukerrådet ("Norway Policy Report"), 'Every Step You Take - How Deceptive Design Lets Google Track Users 24/7' (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf> accessed 20 February 2019

FRA, 'Preventing Unlawful Profiling Today and in The Future: A Guide' (2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf> accessed 25 March 2019

FTC, 'FTC Approves Final Order in Vulcun Deceptive App Installation Case' (2016) <https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-order-vulcun-deceptive-app-installation-case> accessed 20 April 2019

FTC, 'In The Matter Of General Workings Inc., A Corporation, Also D/B/A Vulcun, And Ali Moiz And Murtaza Hussain Individually And As Officers Of General Workings Inc.' (2019) <https://www.ftc.gov/system/files/documents/cases/1604vulcundo.pdf> accessed 20 April 2019

FTC, 'Self-Regulatory Principles for Online Behavioural Advertising' (2009) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf> accessed 30 April 2019

Gamba J and others, 'An Analysis of Pre-Installed Android Software' (*IMDEA Networks Institute*, 2019) <http://eprints.networks.imdea.org/1959/1/An_Analysis_of_Pre-installed_Android_Software_2019_EN.pdf> accessed 30 March 2019

Gare E, 'Profiling And Online Behavioural Advertisement Under The GDPR: Has The New Regulation Succeed In Assuring The Protection Of Fundamental Rights Without Hindering Innovation And Economic Interests In The Digital Economy?' (LLM, University of Oslo 2016)

Garifova L, 'Infonomics and the Value of Information in the Digital Economy' (2015) 23 Procedia Economics and Finance <https://www.sciencedirect.com/science/article/pii/S2212567115004232> accessed 11 April 2019

'Gartner Says Global Smartphone Sales Stalled in the Fourth Quarter Of 2018' (*Gartner*, 2019) <https://www.gartner.com/en/newsroom/press-releases/2019-02-

21-gartner-says-global-smartphone-sales-stalled-in-the-fourth-quart> accessed 1 May 2019

Goode L, 'Google's New Privacy Dashboard Makes It Easier to See What Google Knows about You' (*The Verge*, 2017) <https://www.theverge.com/2017/9/8/16276000/google-dashboard-my-account-privacy-security-redesign> accessed 21 April 2019

'Google Accused of GDPR Privacy Violations by Seven Countries' (*The Verge*, 2018) <https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive> accessed 31 March 2019

'Google Ads Help – About Store Visit Conversions' (*Google*) <https://support.google.com/google-ads/answer/6100636?co=ADWORDS.IsAWNCustomer%3Dtrue&hl=en> accessed 29 April 2019

'Google Ads User Data Retention Policy' (*Google*) <https://privacy.google.com/businesses/retention> accessed 30 March 2019

'Google Ads Vs Google Marketing Platform: Which Is Best For Your Display Ads?' (*Bannerflow*, 2018) <https://blog.bannerflow.com/google-ads-vs-google-marketing-platform/> accessed 24 March 2019

'Google Analytics – Measurement Protocol Overview' (*Google*) <https://developers.google.com/analytics/devguides/collection/protocol/v1/> accessed 25 March 2019

'Google Bans Crypto-Mining Apps from Play Store' (*BBC Technology*, 2018) <https://www.bbc.com/news/technology-44980936> accessed 2 March 2019

'Google Chrome Privacy Whitepaper – Autofill and Password Management' (*Google*) <https://www.google.com/chrome/privacy/whitepaper.html#autofill> accessed 30 April 2019

'Google Chrome Privacy Whitepaper – Payments' (*Google*) <https://www.google.com/chrome/privacy/whitepaper.html#payments> accessed 30 April 2019

'Google Chrome Privacy Whitepaper – Translate' (*Google*) <https://www.google.com/chrome/privacy/whitepaper.html#translate> accessed 30 April 2019

'Google Give Keys Of Android Automotive OS To Third Party Mobile App Developers' (*MobileAppAaily*, 2019) <https://www.mobileappdaily.com/google-opens-android-automotive-os-to-third-party-app-developers> accessed 5 May 2019

'Google Help' (*Google*) <https://support.google.com/google> accessed 15 April 2019

'Google Maps Timeline - Computer - Google Maps Help' (*Google*) <https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en> accessed 15 April 2019

'Google Maps/Earth Additional Terms Of Service – Google' (*Google*) <https://www.google.com/help/terms_maps/> accessed 10 May 2019

'Google Play – Monetization and Ads' (*Google Play*) <https://play.google.com/about/monetization-ads/ads/ad-id/> accessed 30 April 2019

'Google Play Help: Review App Permissions Android 5.9' (*Google*) <https://support.google.com/googleplay/answer/6014972?co=GENIE.Platform%3DAndroid&oco=1> accessed 7 March 2019

'Google Privacy Policy – We Use Data to Build Better Services' (*Google*) <https://policies.google.com/privacy#whycollect> accessed 30 April 2019

'Google Privacy Policy - When You Use Our Services, You're Trusting Us with Your Information. We Understand This Is a Big Responsibility and Work Hard to Protect Your Information and Put You in Control' (*Google*) <https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en_eu.pdf> accessed 30 March 2019

'Google Still Tracks You through the Web If You Turn off Location History' (*The Verge*, 2018) <https://www.theverge.com/2018/8/13/17684660/google-turn-off-location-history-data> accessed 31 March 2019

'Google Taken to Court in UK over Claims of Improper Data Collection' (*Engineering and Technology*, 2018) <https://eandt.theiet.org/content/articles/2018/05/google-taken-to-uk-court-over-claims-of-improper-data-collection/> accessed 22 March 2019

'Google Takeout: Download Your Data' (*Google*) <https://takeout.google.com/settings/takeout?pli=1> accessed 30 March 2019

'Google Terms of Service' (*Google*) <https://policies.google.com/term> accessed 30 April 2019

'Google Tracks User Location Even When Forbidden, Investigation Finds' (*Engineering and Technology*, 2018)

<https://eandt.theiet.org/content/articles/2018/08/google-tracks-user-location-even-when-forbidden-investigation-finds/> accessed 21 March 2019

'Google's Allowing Users to Automatically Delete Location and Activity Data' (*Android Central*, 2019) <https://www.androidcentral.com/google-auto-delete-feature-announced> accessed 3 May 2019

Government Gazette Staatskoerant – Republic of South Africa, 'Protection of Personal Information Act, 2013 (Act No. 4 of 2013) Regulations Relating To the Protection of Personal Information' (2018) <https://www.michalsons.com/wp-content/uploads/2017/11/PoPI-Regulations-Final-14-Dec-2018-3-languages-42110_14-12.pdf> accessed 30 March 2019

Gresham J, 'Is Encrypted Data Personal Data under the GDPR?' (*IAPP*, 2019) <https://iapp.org/news/a/is-encrypted-data-personal-data-under-the-gdpr/> accessed 15 April 2019

Gu J, Zhang V, Shen S, 'Coin Miner Mobile Malware Returns, Hits Google Play' (*Trendmicro Security Intelligence Blog*, 2017) <https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/> accessed 1 March 2019

'Guide To The General Data Protection Regulation (GDPR): Principle (C): Data Minimisation'' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/?q=%22data+minimisation%22> accessed 2 February 2019

'Guidelines for Representing Your Business On Google - Google My Business Help' (*Google*) <https://support.google.com/business/answer/3038177> accessed 4 May 2019

Gutwirth S, Leenes R, De Hert P, *Reloading Data Protection Multidisciplinary Insights And Contemporary Challenges* (S Gutwirth, R Leenes and P De Hert, 1st edn, Springer 2014)

Hahn M, 'Why the OpenRTB Does NOT Violate the GDPR' (*Digital News Daily*, 2019) <https://www.mediapost.com/publications/article/331879/why-the-openrtb-does-not-violate-the-gdpr.html> accessed 30 March 2019

Hannak A and others, 'Measuring Price Discrimination And Steering On E-Commerce Web Sites' [2014] Proceedings of the 2014 Conference on Internet Measurement Conference

Hansen M, 'Data Protection By Default In Identity-Related Applications' [2013] 3rd Policies and Research in Identity Management <https://hal.inria.fr/hal-01470500/document> accessed 21 April 2019

Hartzog W, Selinger E, 'Why You Can No Longer Get Lost in the Crowd' (*The New York Times*, 2019) <https://www.nytimes.com/2019/04/17/opinion/data-privacy.html> accessed 20 April 2019

Hautala L, 'These Android Apps Have Been Tracking You, Even When You Say Stop' (2019) <https://www.cnet.com/news/these-android-apps-have-been-tracking-you-even-when-you-say-stop/> accessed 23 February 2019

Heimes R, 'Top 10 Operational Impacts of the GDPR: Part 5 – Profiling' (*IAPP*, 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling> accessed 26 March 2019

Helberger N, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law'' (2016) 6 IVIR <https://www.ivir.nl/publicaties/download/1747.pdf> accessed 6 April 2019

Hickman T, Gabel D, 'Chapter 5: Key Definitions – Unlocking the EU General Data Protection Regulation | White & Case LLP International Law Firm, Global Law Practice' (*Whitecase.com*) <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation> accessed 1 May 2019

Hildebrandt M, Gutwirth S, *Profiling The European Citizen: Cross-Disciplinary Perspectives* (Springer Publishing Company 2008)

Hilsum L, 'Kenyans Bombarded with Fake News in Presidential Election' (*Channel 4 News*, 2018) <https://www.channel4.com/news/kenyans-bombarded-with-fake-news-in-presidential-election> accessed 3 May 2019

Hilts A, Parsons C, Crete-Nishihata M, 'Approaching Access: A Look at Consumer Personal Data Requests in Canada' (*CitizenLab*, 2018) <https://citizenlab.ca/2018/02/approaching-access-look-consumerpersonal-data-requests-canada> accessed 22 March 2019

Hogan M, 'Facebook And the 'Fear of Missing Out' (Fomo)' (*Psychology Today*, 2015) <https://www.psychologytoday.com/us/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo> accessed 20 April 2019

Hollis N, 'Ten Years of Learning on How Online Advertising Builds Brands' (2005) 45 Journal of Advertising Research <https://www.researchgate.net/publication/4733801_Ten_Years_of_Learning_on_How_Online_Advertising_Builds_Brands> accessed 30 March 2019

Hoofnagle C, Whittington J, 'Free: Accounting For the Costs of the Internet's Most Popular Price' (2014) 61 UCLA L. Rev

Horling B, Kulick M, 'Personalized Search for Everyone' (*Google Blog*, 2009) <https://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html> accessed 23 March 2019

Houser K, Voss G, 'Can Facebook and Google Survive the GDPR?' (*Oxford Law Faculty*, 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr> accessed 3 May 2019

'How Does Google Know My Location?' (*Policies.google.com*, 2019) <https://policies.google.com/technologies/location-data?hl=en#how-find> accessed 4 May 2019

'How Google Retains Data We Collect' (*Google*) <https://policies.google.com/technologies/retention> accessed 30 March 2019

'How Google Uses Location Information?' (*Policies.google.com*, 2019) <https://policies.google.com/technologies/location-data> accessed 15 May 2019

'ICO: Business Falling Short on GDPR Accountability' (*Out-Law*, 2019) <https://www.out-law.com/en/articles/2019/april/ico-businesses-fail-gdpr-accountability-/> accessed 28 March 2019

'In-App Purchases: ABC of Freemium App Monetization' (*Medium*, 2018) <https://medium.com/@aprofita_co/in-app-purchases-abc-of-freemium-app-monetization-e742043927d2> accessed 30 March 2019

'In-Market Audiences' (*Think with Google*, 2014) <https://www.thinkwithgoogle.com/products/in-market-audiences> accessed 18 April 2019

Interactive Advertising Bureau (IAB), 'IAB Internet Advertising Revenue Report: 2018 Full Year Results' (2019) <https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf> accessed 14 May 2019

International Working Group on Data Protection in Telecommunications ("IWGDPT"), 'Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy' (2013) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2013/2013-WP-Personal_Data_Web.pdf> accessed 26 April 2019

'Introducing Auto-Delete Controls for Your Location History and Activity Data' (*Google*) <https://www.blog.google/technology/safety-security/automatically-delete-data/> accessed 1 May 2019

Jain A, Kanhangad V, 'Exploring Orientation And Accelerometer Sensor Data For Personal Authentication In Smartphones Using Touchscreen Gestures' (2015) 68 Pattern Recognition Letters <https://www.sciencedirect.com/science/article/abs/pii/S0167865515002056> accessed 8 March 2019

Karch M, 'What Is The Difference Between Google And Alphabet?' (*Lifewire*, 2019) <https://www.lifewire.com/understanding-google-and-alphabet-4116085> accessed 20 February 2019

Kelly K, *New Rules for the New Economy* (Penguin Books 2000)

'Key Terms' (*Google*) <https://policies.google.com/privacy/key-terms#toc-terms-unique-id> accessed 24 March 2019

Kindt E, *Privacy and Data Protection Issues of Biometric Applications* (1st edn, Springer 2013)

Kobie N, 'How to Delete Your Google Search History and Stop Tracking' (*Wired*, 2019) <https://www.wired.co.uk/article/how-to-delete-google-search-history-tracking> accessed 15 May 2019

Koch Z, 'Product Updates Based on Your Feedback' (*The Keyword by Google*, 2018) <https://www.blog.google/products/chrome/product-updates-based-your-feedback> accessed 19 April 2019

Kohli P, 'CoinMiner and Other Malicious Cryptominers Targeting Android' (*Sophos*, 2018) <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-coinminer-and-other-malicious-cryptominers-tpna.pdf?la=en> accessed 2 March 2019

Kolt N, 'Return on Data' (2019) 38 Yale Law & Policy Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362880> accessed 7 May 2019

Kuchler H, 'Advertisers Stick by Facebook despite Privacy Scandal' (*Financial Times*, 2018) <https://www.ft.com/content/eb6dac28-48e5-11e8-8ae9-4b5ddcca99b3> accessed 11 May 2019

Kuner C, ‘The European Union and the Search for an International Data Protection Framework’ (2014) Groningen Journal of International Law 2(1) <http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf> accessed 20 February 2019

Lab K, 'From Crypto Currency Mining To Ddos Attacks: The New Multi-Featured Mobile Trojan Loapi Discovered' (*Kaspersky Content Hub*, 2019) <https://www.kaspersky.com/about/press-releases/2017_new-multi-featured-mobile-trojan-loapi-discovered> accessed 2 March 2019

Lab K, 'KSN Report: Ransomware and Malicious Crypto Miners 2016-2018' (*Kaspersky Content Hub*, 2018) <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf> accessed 1 March 2019

Lambert P, *The Data Protection Officer: Profession, Rules, And Role* (1st edn, Auerbach Publications 2016)

Lanier J, *Who Owns the Future?* (Simon & Schuster 2013)

Lardinois F, 'Google Says There Are Now 2 Billion Active Chrome Installs' (*TechCrunch*, 2016) <https://techcrunch.com/2016/11/10/google-says-there-are-now-2-billion-active-chrome-installs/> accessed 20 March 2019

Laurita M, Maklakova A, 'Google's Fine and the French Data Protection Authority's Far-Reaching GDPR Compliance Measures' [2019] Journal Mondaq Business Briefing

Leenes R and others, *Data Protection And Privacy: (In)Visibilities And Infrastructures* (Springer International Publishing 2017)

'Legitimate Interests' (*Ico.org.uk*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 2 May 2019

Lerman R, O'Brien M, 'Experts Aren't Impressed With Google's New Privacy Tools' (*Time*, 2019) <http://time.com/5585676/google-new-privacy-tools/> accessed 10 May 2019

Levy S, 'Secret of Googlenomics: Data-Fueled Recipe Brews Profitability' (*Wired*, 2009) <https://www.wired.com/2009/05/nep-googlenomics> accessed 20 March 2019

Liu Y, 'Privacy-Preserving Targeted Advertising for Mobile Devices' (PhD, University of Oxford 2017)

Liu Y, Simpson A, 'Privacy-Preserving Targeted Mobile Advertising: Requirements, Design and a Prototype Implementation' (2016) 46 Software: Practice and Experience <https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2403> accessed 20 April 2019

Liverani R, Freeman N, 'Abusing Firefox Extensions' [2009] DefCon Security Assessment <https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-roberto_liverani-nick_freeman-abusing_firefox.pdf> accessed 6 April 2019

Livingstone S, 'Children: A Special Case for Privacy?' (*Iicom.org*, 2018) <http://www.iicom.org/images/iic/intermedia/july-2018/im-july2018-childrenspecialcaseforprivacy.pdf> accessed 18 February 2019

Location Forum, 'Location Data Privacy: Guidelines, Assessments and Recommendations' (2013) <https://docplayer.net/9241139-Location-data-privacy-guidelines-assessment-recommendations.html> accessed 23 February 2019

'Location History Visualizer' <https://locationhistoryvisualizer.com/> accessed 30 March 2019

Lopez-Tarruella A, 'Google and the Law' (2012) 22 Information Technology and Law Series <https://link.springer.com/book/10.1007%2F978-90-6704-846-0#toc> accessed 18 January 2019

Luca E and others, 'Touch Me Once and I Know It's You! Implicit Authentication Based on Touch Screen Patterns' (*Core*, 2012) <https://core.ac.uk/display/22192389> accessed 15 May 2019

Maheshwari S, 'YouTube Is Improperly Collecting Children's Data, Consumer Groups Say' (*The New York Times*, 2018) <https://www.nytimes.com/2018/04/09/business/media/youtube-kids-ftc-complaint.html> accessed 30 March 2019

'Making It Easy to Understand What Data We Collect and Why' (*Google*) <https://safety.google/privacy/data/> accessed 19 April 2019

'Manage Your Android Device's Location Settings - Google Account Help' (*Google*, 2019) <https://support.google.com/accounts/answer/3467281?hl=en> accessed 15 May 2019

'Manage Your Location History - Google Account Help' (*Google*, 2019) <https://support.google.com/accounts/answer/3118687?hl=en> accessed 15 May 2019

Matwyshyn A, Aral S, 'What the EU's GDPR Rules Mean For U.S. Consumers' (*Knowledge@Wharton*, 2018) <https://knowledge.wharton.upenn.edu/article/how-the-gdpr-rules-will-impact-data-protection/> accessed 6 May 2019

McDaniel P, 'Bloatware Comes to the Smartphone' (2012) 10 IEEE Security and Privacy <http://patrickmcdaniel.org/pubs/mcd12.pdf> accessed 2 March 2019

Meek A, 'Google Tracking Is Even Creepier Than You Thought, Study Finds' (*NYPost*, 2019) <https://nypost.com/2018/08/21/google-tracking-is-even-creepier-than-you-thought-study-finds/,> accessed 3 May 2019

Mehrnezhad M and others, 'NFC Payment Spy: Privacy Attacks On Contactless Payments Using NFC-Enabled Mobile' [2016] 3rd International Conference on Research in Security Standardisation <https://www.researchgate.net/publication/309611581_NFC_Payment_Spy_A_Privacy_Attack_on_Contactless_Payments> accessed 19 April 2019

Mehrnezhad M, Hao F, Shahandashti S, 'Tap-Tap and Pay (TTP): Preventing The Mafia Attack In NFC Payment' [2015] International Conference on Research in Security Standardisation <https://www.researchgate.net/publication/300132931_Tap-Tap_and_Pay_TTP_Preventing_the_Mafia_Attack_in_NFC_Payment> accessed 18 April 2019

Mehrnezhad M, Toreini E, 'What Is This Sensor and Does This App Need Access to It?' (2019) 6 Informatics <https://www.researchgate.net/publication/330606893_What_Is_This_Sensor_and_Does_This_App_Need_Access_to_It> accessed 4 May 2019

Mehrotra K, 'Google Aims at Privacy Law after Facebook Lobbying Failed' (*Bloomberg.com*, 2018) <https://www.bloomberg.com/news/articles/2018-04-24/google-takes-aim-at-privacy-law-after-facebook-lobbying-failed> accessed 6 May 2019

Menchen-Trevino E, 'Collecting Vertical Trace Data: Big Possibilities and Big Challenges for Multi-Method Research' (2013) 5 Policy & Internet <http://blogs.oii.ox.ac.uk/policy/tracing-our-every-move-big-data-and-multi-method-research/> accessed 2 February 2019

Metz R, 'Smartphone App Monitors Mental Health Status' (*Privacy International*, 2018) <https://privacyinternational.org/examples-abuse/2513/smartphone-app-monitors-mental-health-status> accessed 23 February 2019

Mikians J and others, 'Detecting Price and Search Discrimination on the Internet' [2012] Proceedings of the 11th ACM Workshop on Hot Topics in Networks

Miller C, 'Calendar 2 Made $2K in 3 Days Mining Cryptocurrency, But Apple Says It Violated Mac App Store Guidelines'' (*9to5Mac*, 2018) <https://9to5mac.com/2018/03/13/crypto-mining-calendar-app-ios/> accessed 1 March 2019

Miller D, 'The Unpredictable Mobile Phone' (*UCL Anthropology*) <https://www.ucl.ac.uk/anthropology/people/academic-and-teaching-staff/daniel-miller/unpredictable-mobile-phonei> accessed 29 April 2019

'Mobile Apps: U.S. Smartphone Audience Reach 2019 | Statistic' (*Statista*, 2019) <https://www.statista.com/statistics/281605/reach-of-leading-us-smartphone-apps/> accessed 14 May 2019

'Modern Marketing Is Accessible Marketing' (*Advertiseonbing-blob.azureedge.net*) <https://advertiseonbing-blob.azureedge.net/blob/bingads/media/library/insight/moder-marketing-is-accessible-marketing/accessibility-marketing.pdf> accessed 14 May 2019

'Monero-Mining Hiddenminer Android Malware Can Potentially Cause Device Failure' (*Trendmicro Security Intelligence Blog*, 2018) <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure> accessed 2 March 2019

Morse J, 'Your Android Phone Pings Google A Lot More Than You Might Think' (*Mashable*, 2018) <https://mashable.com/article/google-android-data-collection-study/> accessed 29 March 2019

Mourby M and others, 'Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review <https://www.sciencedirect.com/science/article/pii/S0267364918300153> accessed 15 February 2019

Nakashima R, 'AP Exclusive: Google Tracks Your Movements, Like It or Not' (*Associated Press*, 2018) <https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb> accessed 22 March 2019

'Napoleon Patacsil, Individually, And On Behalf Of Other Persons Similarly Situated, Plaintiff, V. Google Inc., Defendant. FTC California Case [2018] Case 3:18-Cv-5062.'

Naughton J, 'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism' (*The Guardian*, 2019) <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> accessed 20 February 2019

Newman N, 'The Costs Of Lost Privacy: Consumer Harm And Rising Economic Inequality In The Age Of Google' (2014) 40 Wm. Mitchell L. Rev.

Nield D and others, 'All the Ways Google Tracks You—And How to Stop It' (*WIRED*, 2019) <https://www.wired.com/story/google-tracks-you-privacy/> accessed 27 May 2019

Nield D, 'All the Ways Your Smartphone and Its Apps Can Track you' (*Gizmodo*, 2018) <https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704> accessed 19 February 2019

Norval C and others, 'Reclaiming Data: Overcoming App Identification Barriers For Exercising Data Protection Rights' [2018] 4th Workshop on Legal and Technical Issues in Cloud and Pervasive Computing (IoT) <https://arxiv.org/pdf/1809.05369.pdf> accessed 24 February 2019

OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) 195-98 <http://www.oecd-ilibrary.org/deliver/9789264229358-en.pdf?itemId=/content/book/9789264229358-en&mimeType=application/pdf> accessed 13 May 2019

OECD, 'Issues Related To Security Of Information Systems And Protection Of Personal Data And Privacy' (OECD 1996) <http://www.oecd.org/internet/ieconomy/2094252.pdf> accessed 19 February 2019

OECD, 'The OECD Privacy Framework' (2013) <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 13 February 2019

O'Flaherty K, 'This Is Why People No Longer Trust Google and Facebook with Their Data' (2018) <https://www.forbes.com/sites/kateoflahertyuk/2018/10/10/this-is-why-people-no-longer-trust-google-and-facebook-with-their-data/#2b7712f44b09> accessed 10 March 2019

Online Behavioural Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles (FTC) <https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf> accessed 9 May 2019

'Opinion 02/2013 On Apps on Smart Devices' (*Pdpjournals.com*, 2013) <https://www.pdpjournals.com/docs/88097.pdf> accessed 11 May 2019

Palmer M, 'Data Is the New Oil' (*ANA Marketing Maestros*, 2006) <http://ana.blogs.com/maestros/2006/11/data_is_the_new.html> accessed 25 April 2019

Papakyriakopoulos O and others, 'Social Media and Micro targeting: Political Data Processing and the Consequences for Germany' (2018) 5 SAGE Journals: Big Data & Society <https://journals.sagepub.com/doi/full/10.1177/2053951718811844> accessed 20 March 2019

Pentland A, 'The Global Information Technology Report 2008-2009: Reality Mining of Mobile Communications: Toward a New Deal on Data' [2009] World

Economic Forum & INSEAD <https://hd.media.mit.edu/wef_globalit.pdf> accessed 23 March 2019

Perez S, 'Apple's Latest Crackdown: Apps Pulling the Advertising Identifier, But Not Showing Ads, Are Being Rejected from App Store' (*TechCrunch*, 2014) <https://techcrunch.com/2014/02/03/apples-latest-crackdown-apps-pulling-the-advertising-identifier-but-not-showing-ads-are-being-rejected-from-app-store> accessed 14 April 2019

Pierce C and others, 'Recommendations on the Use of Mobile Applications for the Collection and Communication of Pharmaceutical Product Safety Information' (2019) 42 US National Library of Medicine - Drug Safety <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6450855> accessed 3 April 2019

Politou E, Alepis E, Patsakis C, 'Forgetting Personal Data And Revoking Consent Under The GDPR: Challenges And Proposed Solutions' (2018) 4 Journal of Cybersecurity <https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056> accessed 3 May 2019

Porter Felt A, Greenwood K, Wagner D, 'The Effectiveness Of Application Permissions' [2011] University of California, Berkeley – 2nd USENIX Conference on Web application Development <https://people.eecs.berkeley.edu/~daw/papers/perms-webapps11.pdf> accessed 3 April 2019

'Privacy & Terms' (*Google*) <https://policies.google.com/privacy?hl=en-US#infocollect> accessed 27 March 2019

Privacy International, 'A Guide for Policy Engagement on Data Protection: The Keys to Data Protection' (Privacy International 2018) <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> accessed 2 January 2019

Privacy International, 'Comments to the Article 29 Working Party Guidelines on Automated Individual Decision Making and Profiling' (2017) <https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20submission%20on%20profiling%20guidance.pdf> accessed 6 April 2019

Privacy International, 'Further Questions On Cambridge Analytica's Involvement In The 2017 Kenyan Elections And Privacy International's Investigations' (2018) <https://privacyinternational.org/feature/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy> accessed 7 May 2019

Privacy International, 'How Apps on Android Share Data with Facebook' (Privacy International 2018) <https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report> accessed 15 April 2019

Privacy International, 'State Of Privacy Mexico' (2019) <https://privacyinternational.org/state-privacy/1006/state-privacy-mexico> accessed 30 April 2019

'Protecting Personal Data World Wide: Convention 108+' (*EDRi*) <https://edri.org/protecting-personal-data-world-wide-convention-108/> accessed 8 May 2019

'Proximity Beacon API – Overview' (*Google*, 2017) <https://developers.google.com/beacons/proximity/guides> accessed 20 March 2019

'Pseudo' (*Cambridge Dictionary*, 2019) <http://dictionary.cambridge.org/dictionary/english/pseudo> accessed 1 January 2019

'Pseudonymisation Is Helping Firms Comply with a New EU Privacy Law' (*The Economist*, 2018) <https://www.economist.com/science-and-technology/2018/04/05/pseudonymisation-is-helping-firms-comply-with-a-new-eu-privacy-law> accessed 15 November 2018

Purtova N, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 15 February 2019

Ram A and others, 'How Smartphone Apps Track Users and Share Data' (*Financial Times*, 2018) <https://ig.ft.com/mobile-app-data-trackers/> accessed 3 January 2019

'Regulating The Internet Giants 4. Regulating the Internet Giants: The Worid's Most Valuable Resource Is No Longer Oil, But Data' (*The Economist*, 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 23 March 2019

'Regulation (EU) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016: On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And

Repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> accessed 30 March 2019

'Request For An Assessment Notice/Invitation To Issue Good Practice Guidance Re "Behavioural Advertising"' (ICO 2019) <https://brave.com/ICO-Complaint-.pdf> accessed 15 May 2019

Ritchie R, 'Android Sucks 10X More Data than iPhone' (*iMore*, 2018) <https://www.imore.com/android-sucks-10x-more-data-iphone?_ga=2.98283034.426741244.1554988833-1448611976.1552437390> accessed 20 March 2019

Roig A, 'Safeguards For The Right Not To Be Subject To A Decision Based Solely On Automated Processing (Article 22 GDPR)' (*Ejlt.org*, 2018) <http://ejlt.org/article/view/570/771> accessed 27 May 2019

'Runtime Permissions' (*Android Source*) <https://source.android.com/devices/tech/config/runtime_perms.html> accessed 7 March 2019

Rutherford ST Jones, 'Google Has Lawsuit in Illinois over Facial Recognition Scanning in Google Photos Dismissed' (*Gizmodo Australia*, 2019) <https://www.gizmodo.com.au/2019/01/google-has-lawsuit-in-illinois-over-facial-recognition-scanning-in-google-photos-dismissed/> accessed 4 May 2019

Ryan J, 'Update on GDPR Complaint (RTB Ad Auctions)' (*Brave*, 2019) <https://brave.com/update-rtb-ad-auction-gdpr> accessed 14 February 2019

Ryan J, 'Why GDPR Is Kryptonite to Google & Facebook on Anti-Trust' (*Brave Insights, GDPR, Policy, Research, Security & Privacy*, 2018) <https://brave.com/vestager/> accessed 10 March 2019

'Safety Center – Data Privacy' (*Google*) <https://safety.google/privacy/data> accessed 29 March 2019

'Safety Center – We Do Not Sell Your Personal Information to anyone' (*Google*) <https://safety.google/privacy/ads-and-data/> accessed 30 April 2019

'Scalable Policy-Aware Linked Data Architecture for Privacy, Transparency and Compliance' (*Specialprivacy.eu*) <https://www.specialprivacy.eu/images/documents/SPECIAL_D1.2_M6_V1.0.pdf> accessed 6 May 2019

Schmarzo B, 'The Value of Data: Google Gets It!' (*EMC InFocus*, 2014) <https://infocus.emc.com/william_schmarzo/the-value-ofdata-google-gets-it> accessed 12 March 2019

Schmidt D, 'Google Data Collection' (*FTC*, 2018) <https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0074-d-0018-155525.pdf> accessed 15 October 2018

Schmidt E, 'A Chance for Growth' (*Frankfurter Allgemeine Zeitung*, 2014) <http://www.faz.net/aktuell/feuilleton/debatten/eric-schmidtabout-the-good-things-google-does-a-chance-for-growth-12887909.html> accessed 22 March 2019

Schwartz P, Solove D, 'Reconciling Personal Information in The United States And European Union' (2014) 102 California Law Review

'Search & Browse Privately - Android - Google Search Help' (*Google*) <https://support.google.com/websearch/answer/4540094?authuser=0&co=GENIE.Platform%3DAndroid&oco=1> accessed 5 May 2019

Seriot N, 'iPhone Privacy' [2010] Black Hat DC <http://seriot.ch/resources/talks_papers/iPhonePrivacySlides.pdf> accessed 5 March 2019

Shao J, 'Strategic Signals in the App Economy: An Empirical Study Of Google Play Store.' (PhD, Nottingham University 2016)

Simon L, Anderson R, 'PIN Skimmer: Inferring Pins through the Camera and Microphone' [2013] 3rd ACM Workshop on Security and Privacy in Smartphones Mobile Devices <https://www.cl.cam.ac.uk/~rja14/Papers/pinskimmer_spsm13.pdf> accessed 13 April 2019

'Smartphone Addiction: Should Children Kick The Habit?' (*Study International*, 2018) <https://www.studyinternational.com/news/smartphone-addiction-should-children-kick-the-habit/> accessed 5 January 2019

'Smartphone Solutions for Smarter, Greener Urban Mobility' (*Horizon 2020 - European Commission*, 2017) <https://ec.europa.eu/programmes/horizon2020/en/news/smartphone-solutions-smarter-greener-urban-mobility> accessed 15 April 2019

Solove D, *Understanding Privacy* (Harvard University Press 2008)

'Some Changes to Our Service Model in Europe' (*Google*, 2018) <https://www.blog.google/around-the-globe/google-europe/some-changes-our-service-model-europe> accessed 30 March 2019

Song C and others, 'Limits of Predictability in Human Mobility' (2010) 327 Journal of Science <https://science.sciencemag.org/content/327/5968/1018> accessed 30 March 2019

'Spain DPA Limits the Use of Data in Political Campaigning' (*GDPR Today*, 2019) <https://www.gdprtoday.org/spain-dpa-limits-the-use-of-data-in-political-campaigning/> accessed 12 May 2019

Spreitzer R, 'PIN Skimming: Exploiting The Ambient-Light Sensor In Mobile Devices' [2014] 4th ACM Workshop on Security and Privacy in Smartphones Mobile Devices <https://graz.pure.elsevier.com/en/publications/pin-skimming-exploiting-the-ambient-light-sensor-in-mobile-device> accessed 19 April 2019

Srikrishna B and others, 'White Paper of the Committee of Experts on a Data Protection Framework for India' (2018) 4 Ministry of Electronics and Information Technology <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> accessed 20 February 2019

'Store Visit Conversion Tracking In Google Ads (Adwords)' (*Optimize Smart*) <https://www.optimizesmart.com/store-visit-conversion-tracking-google-adwords> accessed 29 April 2019

Sullivan L, 'Google Maps Opens Fraud Complaint Forum' (*Mediapost*, 2019) <https://www.mediapost.com/publications/article/332582/google-maps-opens-fraud-complaint-forum.html> accessed 13 May 2019

Sullivan L, 'Google To Let Users Delete Mobile Auto-Tracking Data' (*MediaPost*, 2019) <https://www.mediapost.com/publications/article/335301/google-to-let-users-delete-mobile-auto-tracking-da.html> accessed 5 May 2019

Sullivan L, 'Microsoft Bing Ads UI Gets 'Massive' Upgrade, Better Access' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335118/microsoft-bing-ads-user-interface-gets-massive-u.html> accessed 16 May 2019

Sullivan L, 'Page Load Times, Technology Are Major Ranking Factors In Google Search Results' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335987/page-load-times-technology-are-major-ranking-fact.html?edition=113918> accessed 15 May 2019

Sullivan L, 'Transparency for Leads in Open Exchange Boosts Publisher Count Past 500' (*Mediapost*, 2019) <https://www.mediapost.com/publications/article/334821/transparency-for-leads-in-open-exchange-boosts-pub.html> accessed 15 May 2019

Sullivan L, 'Watching Ads Verified By Facial Recognition Earns Moviegoers Free Ticket' (*MediaPost*, 2019) <https://www.mediapost.com/publications/article/334864/watching-ads-verified-by-facial-recognition-earns.html> accessed 3 May 2019

'Synced with Your Google Account' (*Google*) <https://policies.google.com/privacy#footnote-chrome-sync> accessed 15 May 2019

'The Article 29 Working Party Ceased to Exist as of 25 May 2018' (*EC*, 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492> accessed 27 February 2019

'The CNIL'S Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC' (*CNIL*, 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 10 February 2019

The EU Audio-visual Media Services Directive (AVMSD), ''On the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive)' (2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013&from=EN> accessed 20 April 2019

'The Great Data Race: How Commercial Utilisation of Personal Data Challenges Privacy'' (*Datatilsynet*, 2015) <https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf> accessed 24 February 2019

'The Keyword - As G Suite Gains Traction in the Enterprise, G Suite'S Gmail and Consumer Gmail to More Closely Align' (*Google*) <https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/> accessed 20 April 2019

'The Keyword - Introducing Auto-Delete Controls for Your Location History and Activity Data' (*Google*, 2019) <https://www.blog.google/technology/safety-security/automatically-delete-data/> accessed 5 May 2019

'The Matter Ofpolyðore International. Inc.. Case No. 9327' (*Ftc.gov*, 2009) <https://www.ftc.gov/sites/default/files/documents/cases/2009/01/090114variousarticles.pdf> accessed 15 March 2019

'The WPA-Lancet Psychiatry Commission On The Future Of Psychiatry' (2017) 4 Lancet Psychiatry <https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(17)30333-4/fulltext> accessed 6 April 2019

Thornhill J, 'Should We Think Of Big Tech As Big Brother?' (*Financial Times*, 2019) <https://www.ft.com/content/43980f9c-0f5b-11e9-a3aa-118c761d2745> accessed 20 March 2019

Thurm SY Kane, 'Your Apps Are Watching You' (*The Wall Street Journal*, 2010) <https://www.wsj.com/articles/SB10001424052748704694004576020083703574602> accessed 12 March 2019

Tighe J and others, 'Ibobbly Mobile Health Intervention for Suicide Prevention in Australian Indigenous Youth: A Pilot Randomised Controlled Trial' (2017) 7 BMJ Open <https://bmjopen.bmj.com/content/7/1/e013518> accessed 6 April 2019

Tiku N, 'Privacy Groups Claim Online Ads Can Target Abuse Victims' (*Wired*, 2019) <https://www.wired.com/story/privacy-groups-claim-online-ads-can-target-abuse-victims/> accessed 3 March 2019

Torous J and others, 'New Dimensions and New Tools to Realize the Potential of Rdoc: Digital Phenotyping via Smartphones and Connected Devices' (2017) 7 Transnational Psychiatry <https://www.ncbi.nlm.nih.gov/pubmed/28267146> accessed 6 April 2019

Toubiana V and others, 'Adnostic: Privacy Preserving Targeted Advertising' [2010] 17th Annual Network and Distributed System Security Symposium <https://www.isoc.org/isoc/conferences/ndss/10/pdf/05.pdf> accessed 24 March 2019

'Transcript of Mark Zuckerberg's Senate Hearing' (*The Washington Post*, 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.e0ec05ef3cc2> accessed 23 March 2019

'Trust, Security And Privacy – Smartphones' (*Eurostat*, 2019) <http://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-1021385_QID_-47A4BBBC_UID_-3F171EB0&layout=INDIC_IS,L,X,0;GEO,L,Y,0;IND_TYPE,L,Z,0;TIME,C,Z,1;UNIT,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-1021385IND_TYPE,IND_TOTAL;DS-1021385UNIT,PC_IND_MPP;DS-1021385TIME,2018;DS-1021385INDICATORS,OBS_FLAG;&rankName1=TIME_1_0_-1_2&rankName2=UNIT_1_2_-1_2&rankName3=INDICATORS_1_2_-1_2&rankName4=IND-TYPE_1_2_-1_2&rankName5=INDIC-IS_1_2_0_0&rankName6=GEO_1_2_0_1&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23> accessed 10 May 2019

Tsukayama H, 'Don't Want Google Tracking You? You Have Almost No Choice, According To A Study' (*The Washington Post*, 2019) <https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-

tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.1de6726f6450> accessed 13 April 2019

'Types of Cookies Used by Google' (*Policies.google.com*, 2019) <https://policies.google.com/technologies/types?hl=en-US> accessed 16 May 2019

U.S. House of Representatives Committee on Energy and Commerce, 'Hearing Entitled ‘Algorithms: How Companies’ Decisions about Data and Content Impact Consumers' (2017) <http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf> accessed 10 April 2019

UN Committee on Economic, Social and Cultural Rights (“CESCR”), 'General Comment No. 20: Non-Discrimination in Economic, Social and Cultural Rights (Art. 2, Para. 2, Of the International Covenant on Economic, Social and Cultural Rights) E/C.12/GC/20' (2009) <http://www.refworld.org/docid/4a60961f2.html> accessed 27 April 2019

Urquhart L, Lodge T, Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2018) 264 International Journal of Law and Information Technology <https://www.research.ed.ac.uk/portal/files/78865742/eay015.pdf> accessed 24 April 2019

Vaidhyanathan S, *The Googilization Of Everything* (University of California Press 2011)

Valentino-DeVries J and others, 'Your Apps Know Where You Were Last Night, And They’Re Not Keeping It Secret' (*Nytimes.com*, 2018)

<https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> accessed 11 May 2019

Van der Sloot BF Zuiderveen Borgesius, 'Google and Personal Data Collection' [2012] Google and the Law <https://link.springer.com/chapter/10.1007%2F978-90-6704-846-0_4> accessed 5 April 2019

Vidas T, Votipka D, Christin N, 'All Your Droid Are Belong to Us: A Survey of Current Android Attacks' [2011] 5th USENIX Conference on Offensive Technologies <https://www.researchgate.net/publication/262290609_All_your_droid_are_belong_to_us_A_survey_of_current_android_attacks> accessed 3 March 2019

'Views and Interactions with Content and Ads' (*Policies.google.com*, 2019) <https://policies.google.com/privacy#footnote-content-views> accessed 15 May 2019

Voigt P, von dem Bussche A, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017)

Walsh E, Brinker J, 'Is SMS Appropriate? Comparative Properties of SMS and Apps for Repeated Measures Data Collection' (2016) 35 European Journal of Psychological Assessment <https://econtent.hogrefe.com/doi/abs/10.1027/1015-5759/a000376> accessed 6 April 2019

'We Read Your Wearable Tech's Privacy Policy So You Don't Have To' (*Wareable*, 2019) <https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765> accessed 19 May 2019

Weprin A, 'U.S. Digital Ad Revenue Passes $100 Billion, Driven by Video, Mobile' (*Digital News Daily*, 2019) <https://www.mediapost.com/publications/article/335528/us-digital-ad-revenue-passes-100-billion-drive.html> accessed 10 May 2019

Weprin A, 'YouTube Ads Are Getting Longer' (*Mediapost.com*, 2019) <https://www.mediapost.com/publications/article/335989/youtube-ads-are-getting-longer.html?edition=113918> accessed 17 May 2019

'What Are Identifiers And Related Factors?' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/> accessed 15 February 2019

'What Are My Rights?' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en> accessed 25 March 2019

'What Does ‘Grounds Of Legitimate Interest’ Mean?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en> accessed 17 May 2019

'What Does The Google Block Mean For Huawei Phone Owners?' (*Evening Standard*, 2019) <https://www.standard.co.uk/tech/huawei-google-ban-latest-what-does-block-mean-for-phone-users-a4156301.html> accessed 1 June 2019

'What Is Considered Personal Data Under The EU GDPR?' (*GDPR.eu*, 2019) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 15 March 2019

'What Is Legal Design Thinking - Visual Contracts, A Strategic Business Advantage' (*Visual Contracts*) <https://www.visualcontracts.eu/community/what-is-legal-design-thinking> accessed 15 March 2019

'What Is Personal Data?' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> accessed 10 February 2019

'When You Use Our Services, You're Trusting Us With Your Information. We Understand This Is A Big Responsibility And Work Hard To Protect Your Information And Put You In Control' (*Google*, 2019) <https://policies.google.com/privacy#footnote-unique-id> accessed 30 January 2019

'Why Is Google A "Controller" Under The GDPR As Opposed To A "Processor" Of Data? GDPR Faqs - Google Ad Manager Help' (*Support.google.com*, 2019) <https://support.google.com/admanager/answer/9035987?hl=en> accessed 10 May 2019

Wiebe A, Dietrich N, 'Open Data Protection: Study on Legal Barriers to Open Data Sharing – Data Protection and PSI' (2017) <https://www.ouvrirlascience.fr/wp-content/uploads/2018/09/Data-protection-Study-on-legal-barriers-to-open-data-sharing_wiebe_.pdf> accessed 28 April 2019

Willison S, 'Understanding the Greasemonkey Vulnerability' (*Simon Willison*, 2005) <http://simonwillison.net/2005/Jul/ 20/vulnerability> accessed 6 April 2019

World Economic Forum, 'Unlocking the Value of Personal Data: From Collection to Usage' (World Economic Forum 2013)

<http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf> accessed 15 April 2019

Wright D et al, *Safeguards in a world of ambient intelligence* (Springer 2010)

Yanofksy D, 'If You're Using an Android Phone, Google May Be Tracking Every Move You Make' (*Quartz*, 2019) <https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/> accessed 4 March 2019

'YouTube Help: Update the YouTube App For Android 5.0 And 5.1' (*Google*) <https://support.google.com/youtube/answer/7370539?hl=en&co=GENIE.Platform=Android> accessed 24 February 2019

'YouTube Kids Privacy Notice' (*YouTube*) <https://kids.youtube.com/t/privacynotice> accessed 30 April 2019

Zallone R, 'Here, There and Everywhere: Mobility Data In The EU (Help Needed: Where Is Privacy?)' (*Digitalcommons.law.scu.edu*, 2014) <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&amp=&article=1576&context=chtlj> accessed 8 May 2019

Zhao Y and others, 'Mvsec: Multi-Perspective and Deductive Visual Analytics on Heterogeneous Network Security Data' (2014) 17 Journal of Visualization <https://netsec.ethz.ch/publications/papers/mvsec-tr-2014.pdf> accessed 9 April 2019

Zu Z, Bai K, Zhu S, 'Taplogger: Inferring User Inputs On Smartphone Touchscreens Using On-Board Motion Sensors' [2012] 5th ACM Conference on Security and

Privacy in Wireless and Mobile Networks <http://www.cse.psu.edu/~sxz16/papers/taplogger.pdf> accessed 19 April 2019

Zuboff S, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology

Zuboff S, *the Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1st edn, PublicAffairs 2019)