Profiling through Ultrasound Technology, the Right to Privacy and the Right to Data Protection

Anna Lonka

Thesis in Juristprogrammet (Swedish Master of Law), 30 HE credits
Examiner: Cecilia Magnusson Sjöberg
Stockholm, Spring term 2018
Abstract

The right to private and family life and the right to the protection of personal data are two fundamental rights of the EU. The protection of these rights is addressed in the new General Data Protection Regulation (GDPR), the Directive on Privacy and Electronic Communications (ePrivacy Directive) and the upcoming new Regulation on Privacy and Electronic Communications (draft ePrivacy Regulation). In this thesis these three legal acts are evaluated in light of profiling through ultrasound tracking technology. Their technology neutrality and their functioning as safeguards of the two fundamental rights against the use of profiling through ultrasound tracking technology is tested. The GDPR is found to differentiate between profiling in the context of automatic decision-making and profiling in other contexts.

The process of profiling is described in general terms. It is shown how tracking technologies in general and ultrasound tracking technology in particular have a central role in the profiling process. It is found that ultrasound tracking technology enables far wider tracking and data collection than the other tracking technologies. Differences and similarities between ultrasound tracking technology and other tracking technologies are described.

According to the findings, the three legal instruments, the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation, all live up to their aim of technology neutrality on theoretical level, since profiling through ultrasound tracking technology is within the material scope of all of them. An exemption is Article 8(2) of the draft ePrivacy Regulation that, unlike Article 9 of the ePrivacy Directive, does not stretch to cover location tracking through ultrasound technology. However, as will be shown, there are risks related to the practical implementation of these legal frameworks.
5.3.1 General Applicability of the ePrivacy Directive and the Draft ePrivacy Regulation to Ultrasound Tracking Technology .............................................................. 60
5.3.2 Location Tracking through Ultrasound Technology ............................................. 61
5.3.3 Article 5(3) of the ePrivacy Directive and uBeacons ............................................. 61
6 Conclusions .............................................................................................................. 64
6.1 Technology Neutrality of the GDPR, the ePrivacy Directive and the Draft ePrivacy Regulation .................................................................................................................. 64
6.2 Safeguards to the Right to Privacy and the Right to Data Protection .................. 66
6.3 Summary .................................................................................................................. 68
References ..................................................................................................................... 69
1 Introduction

Privacy can be seen as a precondition for a functioning democracy.¹ A society without a certain amount of freedom cannot call itself a democracy. Only free individuals can make free choices and having the freedom to hide one's thoughts, habits and other facts about oneself is an essential part of this freedom. Privacy is not only understood as the right to be let alone,² but also as the right to personal integrity,³ secrecy⁴ or intimacy,⁵ and as the right to control information about oneself.⁶ In the modern information society, where information is easily accessible and easily shared, privacy is constantly challenged.⁷ One big challenge to privacy is the wide-spread use of tracking technologies in order to allow the creation of profiles. One of the most recent, and alarming, tracking technologies is ultrasound tracking.

As a private individual living in Europe in 2018 it is more or less impossible to escape profiling. This is due to the extensive use of targeted advertising both online and offline. Online advertisements are the primary source of income for many service providers. Without advertisements many free Internet services would require a payment. Another aspect is that service providers aim for a better user experience and want to offer services that are tailored and customised to the individual user. Targeted advertisement and tailored services make a private person's Internet use more convenient when the person is shown advertisements and information that he/she finds useful. However, as convenient it is to only see 'relevant' information and avoid seeing anything unnecessary, many people would still want to avoid giving away their private data needed to make this targeting possible.⁸ On top of this comes the fact that not all the 'relevant' information private persons are shown is information they need. There is a risk that the thoughts and desires of an individual are unnecessarily directed in a way that only benefits the marketing actors and not the individual, or the society. There has been claims that Russian hackers have used Facebook advertisements for spreading of misinformation and 'fake news' in order to influence

⁷ For discussion about different ways of intruding privacy, see e.g. Solove Daniel J., *Understanding Privacy*, Harvard University Press, 2008.
elections in other countries. The profiles can also be used for differential pricing, i.e., for adjusting the offers and prices according to the person who is looking for the specific product. This is hardly in the interests of the consumer. Even the bare existence of profiles, or the storage of raw data in itself, can be a privacy risk since the data can be used for uncovering highly personal information.

To be able to generate the profiles that enable the offering of targeted advertisements and 'relevant information' the marketing actors need to have knowledge of the interests and personality of the user. This knowledge is more readily available because of the rapid technological development and the digitalisation of our lives. Cookies, device fingerprinting, wifi-tracking and user accounts, among many others, are examples of technologies and techniques that are present in our daily lives, collecting information about us. Cookies and device fingerprinting technologies are part of the basic functioning of websites but they also track and record user's movements and behaviour on the Internet. Wifi-tracking is used for tracking physical movements of a user in e.g. shopping malls. User accounts, such as Google gmail and Apple IDs, collect all the information from different devices in one place. Ultrasound tracking technology is one of the most recent tracking technologies to raise concerns among the privacy and information security communities. The ultrasound tracking technology enables a new, wider tracking of users via mobile and other electronic devices. The microphone and audio functions of mobile and other electronic devices are exploited for sending and receiving ultrasonic signals, i.e. inaudible signals. By listening and interpreting these signals a mobile application can gather a lot of information about the surroundings of a device, including information about other devices. This technology makes it possible to get more precise location data of devices, and consequently of users, and to connect different devices to one user, just to mention a few of its possibilities. Several privacy threats are connected to the ultrasound technology: media tracking (e.g. the tracking of TV viewing habits), cross-device tracking (i.e.

---


10 See Mavroudis et. al. p. 97 on user profiling. On real time bidding (RTB), see Olejnik L., Castellucia C., et. al. *Selling off privacy at auction*, Network and Distributed System Security Symposium (NDSS), San Diego, California, United States, November 2014. See also the Preambel of CM/Rec(2010)13, where this use of profiling is considered to violate the principle of non-discrimination.


12 For further description about these technologies, please see sections 1.4 and 2.2 beneath.


14 Mavroudis et. al. and Arp et. al.
tracking the same user across different devices), location tracking, de-anonymization and, above all, lack of transparency.\textsuperscript{15} The user is in most cases unaware of the use of the technology and does not know what information is collected and when. Most likely the user does not even know that this kind of tracking is possible at all.\textsuperscript{16} Concerns have been voiced that the current use of the ultrasound technology, especially when combined with other tracking techniques, has serious effects on the user's privacy.\textsuperscript{17}

Applications and companies that are currently using the ultrasound technology are e.g. Shopkick and Lisnr which give rewards to the user based on location,\textsuperscript{18} SilverPush, Signal360 and Audible Magic which use ultrasound beacons embedded into websites or TV advertisements,\textsuperscript{19} and the Google Cast application that uses ultrasound to pair the user's mobile device to his/her Google Chromecast.\textsuperscript{20} Of all the uses of ultrasound only tracking of location is currently in use in Europe.\textsuperscript{21} Media tracking is technically feasible since Silverpush has been selling their product to various companies, but there is no evidence of it having been deployed yet.\textsuperscript{22} Other applications using the technology are increasing in number, though. Despite the fact that ultrasound technology has had small significance until now, it is clear that the technology is existing, plausible and in use. The trend is also rising: 'Our findings strengthen our concerns that the deployment of ultrasonic tracking increases in the wild and therefore needs serious attention regarding its privacy consequences.'\textsuperscript{23}

Together with the increased use of profiling and tracking of individuals the right to private and family life (the right to privacy), together with the right to the protection of personal data (the right to data protection), has become of greater importance and a matter of serious consideration. Privacy and data protection today are important issues, not only for concerned individuals but for communities and legislators, too. The right to private and family life and the right to the protection of personal data have long been codified in several international conventions, such as the International Covenant on Civil and Political Rights (ICCPR) Article 17 and the European Convention on Human Rights (ECHR)\textsuperscript{24} Article 8. The rights are also fundamental rights of the European Union (EU) according to the Charter of Fundamental Rights of the European Union (EU)

\textsuperscript{15} See Arp et. al. p. 5-6 and Mavroudis et. al. p. 101.
\textsuperscript{16} See Arp et. al. p. 15 and FTC letter.
\textsuperscript{17} Mavroudis et. al. p. 96.
\textsuperscript{18} Arp et. al. p. 3, Mavroudis et. al. p. 96.
\textsuperscript{19} Arp et. al. pp. 3-4, Mavroudis et. al. p. 96.
\textsuperscript{20} Mavroudis et. al. pp. 95-96.
\textsuperscript{21} E.g. Lisnr and Shopkick.
\textsuperscript{22} Arp. et. al. pp. 19-20.
\textsuperscript{23} Ibid. p. 25.
\textsuperscript{24} The Convention for the Protection of Human Rights and Fundamental Freedoms 1950.
Charter) Articles 7 and 8, respectively. They are specified in the Data Protection Directive and its successor, the new General Data Protection Regulation, the Directive on Privacy and Electronic Communications and the upcoming new Regulation on Privacy and Electronic Communications of the EU.

It is widely acknowledged that the technological development is proceeding faster than the legislative development. To ensure that the rights and duties of individuals are not jeopardised due to the inertia of the legislative system, legislation is often formulated to be as technology neutral as possible. Technology neutrality is understood here as the opposite of technology-specific. Legislation that is technology-specific covers only a certain technology. A good example of a technology-specific legislation is the Satellite and Cable Directive of the Council, which only covers broadcasts by cable or satellites. The GDPR, the ePrivacy Directive and the draft ePrivacy Regulation all aim to be technology neutral, but when it comes to tracking and profiling, the greatest concern and focus so far has been on the use of cookies. Cookies are one of the most commonly used technologies what comes to Internet browsing. They are sometimes necessary for the function of the Internet sites but they are also widely used for tracking of browsing habits of individuals. The special legislation on cookies in Article 5(3) of the ePrivacy Directive is written for cookies and 'similar technologies'. It is unclear what are the other technologies covered by the rule.

The only 'similar technology' that has exclusively been named so far is device fingerprinting. Even though there are many similarities between these two technologies and the ultrasound tracking technology, it is unclear whether Article 5(3) of the ePrivacy Directive covers the ultrasound technology.

27 Regulation 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), hereafter GDPR.
31 See WP29 Opinion 2/2010 where the focus is on cookies.
It is relevant to ask whether the GDPR and the ePrivacy Directive, and the draft ePrivacy Regulation, have become technology dependent despite of all the efforts to create technology neutral legislation. The shared goal of these pieces of legislations is to protect individuals against privacy intrusion. Restrictions are one of the means to achieve the goal. However, restrictions should not prohibit or restrict only some of the technologies. If the laws are technology neutral they will cover the use of ultrasound tracking technology. Should the opposite be the case, then they will probably fail to achieve their main goal, which is protection of the right to privacy and the right to data protection.

1.1 Subject and Delimitations

The subject of this thesis is to assess the applicability of the GDPR and the ePrivacy Directive together with the draft ePrivacy Regulation to profiling via ultrasound tracking technologies. The focus will be on the individual consumer perspective, the right to private and family life and the right to protection of personal data. Particular interest will focus on whether the GDPR and the ePrivacy Directive together with the draft ePrivacy Regulation provide adequate protection against the risks of profiling based on data collection through ultrasound tracking technology.

The focus of interest in this thesis is solely on profiling for commercial purposes. Profiling today is performed by many actors and it is used for crime prevention and law enforcement purposes, and other purposes within public interest. It would, however, take considerably more time and space to discuss all the aspects of profiling. The question whether profiling for commercial purposes should be regulated and how it should be regulated divides opinion, which is well illustrated by the legislation process of the GDPR. The drafts to the GDPR included a prohibition on all kinds of profiling in a draft Article 20(1) but the final version only prohibits profiling in the context of individual decision-making (Article 22(1) of the GDPR). Profiling for purely commercial purposes seems thus to be a more controversial topic than profiling for other purposes.

This thesis work will focus on the new and upcoming EU legislation since the GDPR will come into force soon, 25 May 2018. The ePrivacy Directive, however, is discussed together with the draft ePrivacy Regulation. The upcoming ePrivacy Regulation is meant to replace the ePrivacy Directive and to be in better compliance with the GDPR.\(^3^3\) Many of the ideas presented in the GDPR will also

\(^{33}\) See the draft ePrivacy Regulation Explanatory Memorandum, under 1.1 Reasons for and objectives of the proposal.
be found in the ePrivacy Regulation, such as the new definition of consent. It is therefore relevant to take into account the draft ePrivacy Regulation. There is, however, no final decision on the draft ePrivacy Regulation and the ePrivacy Directive will be likely to remain in force for some period of time. It is thus necessary to discuss the ePrivacy Directive as current legislation. It should also be noted that the revised data protection and privacy legislation of the EU includes also the Data Protection Directive on Police Matters. Although this directive is highly relevant when discussing the right to privacy and the right to data protection, it is not discussed here since it does not directly affect the profiling and tracking performed by private marketing actors.

Since ultrasound tracking technology has not been directly addressed by the legislator the technology is compared to similar, already regulated technologies. As becomes clear in chapter 2, the technologies that most resemble ultrasound tracking technology are cookies, device fingerprinting and wifi-tracking. Focus is therefore on these three technologies and their regulation. Other tracking and profiling technologies are described and discussed only when understanding them is relevant for comprehending the subject and the argumentation of the thesis.

1.2 Aim of the Thesis and Research Questions

The aim of this thesis is to determine the applicability of the GDPR and the ePrivacy Directive together with the draft ePrivacy Regulation to the technology of profiling by means of ultrasound tracking and to evaluate the extent to which these legal instruments provide safeguards for the right to privacy and the right to data protection. Consequently, the following questions will be addressed:

1) What is ultrasound tracking technology, how does it relate to profiling and in what manner does it differ from other tracking technologies?

2) To what extent are profiling and tracking technologies regulated in the EU?

3) Is the EU regulation on profiling and tracking technologies technology neutral to the extent that ultrasound tracking is regulated by these legal instruments?

34 Article 9(1) of the draft ePrivacy Regulation.
35 Directive 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
1.3 Material and Method

The material and method of this thesis are affected by two aspects of the subject. Firstly, the subject of this thesis, profiling via ultrasound tracking technology, is essentially related to information communication technology (ICT). It should be studied with a methodology that takes the special aspects of ICT related legal research into account. Secondly, the questions and problems related to the subject are harmonised in the EU. The material consists of EU law. The European legal method must therefore also be applied. As a result of these two considerations, a method that is found relevant is the legal method for solving issues of Internet regulation as provided by Dan Jerker B. Svantesson. Svantesson's method will be applied *mutatis mutandis* since the topic and the research question of this thesis are somewhat different from those of Svantesson's. The special aspects of the European legal system, as well as the different emphasis it has on sources and their hierarchy when compared to the national legal system and national legal sources, has been taken into account when handling the material. The European legal method is applied as it is described in Hettne & Otkén Eriksson.

Research on legal questions related to ICT differs from other legal research in several ways. Svantesson has identified four themes that are characteristic to legal research related to ICT. Firstly, the technological development is always faster than legislative processes. The question of whether the legislation should be technology neutral or technology specific is an important one. Technology neutrality is a prevalent theme even in the current work. Secondly, the fact that many legal practitioners struggle to understand the technology is a great challenge to the legal research and development. According to Svantesson, 'research findings must be presented in an as simple and accessible manner as possible, so as to ensure they reach the audience'. Simple and accessible representation of the technology, as well as the problems and findings related to it, has been one of the goals of this thesis. Thirdly, our world is increasingly globalised and this applies especially to the Internet. According to Svantesson, legal problems related to the Internet cannot be effectively addressed without international cooperation.

---

36 The European legal method here refers to the legal dogmatism that is applied in legal issues related to EU-law and that differs from the national legal dogmatism by its different approach to the legal sources.


39 Svantesson pp. 1-3.


41 Ibid p. 2.

42 Ibid.
reflected in how the data protection issues have long been regulated in the EU at the union level and not left for the member states to regulate for themselves.\textsuperscript{43} Fourthly, the Internet and e-commerce have not yet reached their full potential. According to Svantesson, this is due to the fears of the risks involved in the use of the Internet and e-commerce that businesses and consumers have.\textsuperscript{44} The law should help to establish confidence in the Internet so that its full potential can be reached.\textsuperscript{45}

Svantesson's method consists of three phases.\textsuperscript{46} In the first phase one must identify the problem and the constraints related to the problem.\textsuperscript{47} The problem identified in this thesis is the extensive profiling which is possible by the use of ultrasound tracking technology. The right to private and family life, the right to the protection of personal data and technology neutrality are the three constraints fundamentally related to the problem. They represent the outer limits for the solution of the problem.\textsuperscript{48}

The second phase consists of information gathering and critical evaluation of the identified approaches.\textsuperscript{49} In this thesis the legislation on profiling and on tracking technologies in the GDPR, in the ePrivacy Directive and in the draft ePrivacy Regulation are presented and discussed.

In the context of the second phase of the method it is relevant to say a few words about the material used in this thesis and about the European legal method. The EU is often described as something between a state and an inter-governmental organisation (\textit{sui generis}).\textsuperscript{50} The legal sources are therefore also described differently from those of a national and of an inter-governmental legal system. The European legal method means determining the applicable EU law by using the European legal sources: primary law, general principles, international conventions between the EU and third parties, binding and non-binding secondary law and case-law by the Court of Justice of the European Union (the EU Court).\textsuperscript{51} Preparatory papers, or \textit{travaux preparatoires}, as well as recitals of the legal acts and doctrine are often used as a support for interpretation of the law.\textsuperscript{52} The

\begin{footnotesize}
\begin{itemize}
\item[43] See Recitals 7 and 8 of the Data Protection Directive which state that the differing national legislation on data protection issues and on the right to privacy may prevent the free flow of data from one member state to the other, hence establishing the need for legislation on the union level.
\item[44] Svantesson p. 2.
\item[45] Ibid.
\item[46] Ibid p. 9.
\item[47] Ibid pp. 9, 10, 11-13, 24, 26.
\item[48] Ibid p. 11.
\item[49] Ibid pp. 9, 28-29, 40-41.
\item[50] Hettne & Otken Eriksson p. 44.
\item[51] Hettne & Otken Eriksson p. 24.
\end{itemize}
\end{footnotesize}
general principles of law, of which the ECHR is part of,\textsuperscript{53} form the base for interpretation of the law.\textsuperscript{54} The EU primary sources relevant for this thesis, such as the ECHR and the EU Charter, form the basis for the argumentation and analysis of the thesis. The secondary law, such as the GDPR and the ePrivacy Directive, are discussed and analysed in the light of the primary sources. The subject of this thesis is new technology that has not been directly addressed in the EU legislation. There is also little or no case-law on the subject. The emphasis is therefore on the relating legislation, recitals of the relevant legal acts, preparatory papers and the opinions and guidelines of the Article 29 Working Party\textsuperscript{55} (WP 29). Doctrine is also a valuable source in the interpretation.

The draft ePrivacy Regulation is also addressed and used as a basis for the argumentation, even though it is not yet applicable law. This is due to the fact that the ePrivacy Directive is to be repealed in the near future and will be replaced by the draft ePrivacy Regulation. The ePrivacy Directive was adopted as a special legislation to the Data Protection Directive.\textsuperscript{56} Now that the latter has been replaced by the GDPR, the ePrivacy Directive must also be replaced.\textsuperscript{57} At the time of writing, the ePrivacy Directive is not in full coherence with the GDPR. To fill the gaps between the GDPR and the ePrivacy Directive it is necessary to address the draft ePrivacy Regulation as well.

In the third and final phase of Svantesson's method one must construct the solution and test it against the constraints identified in phase one and against future technological developments.\textsuperscript{58} The solution should more or less provide an adequate response to the identified problem which is the subject of the research.\textsuperscript{59} The validity of the solution must, according to Svantesson, be assessed in the light of the constraints of the problem and of the relevant likely technological developments.\textsuperscript{60} This thesis addresses the problems concerning the privacy risks related to the use of profiling via ultrasound tracking technology. The solution to the problem is based on the evaluation of the legal


\textsuperscript{55} The Data Protection Working Party established by Article 29 of Directive 95/46/EC, hereafter the WP 29. The WP 29 is an independent advisory organ that provides advice and guidance on data protection matters. The WP 29 is composed of representatives of the national supervisory authorities, a representative of the European Data Protection Supervisor (EDPS) and of a representative of the European Commission.

\textsuperscript{56} Article 1(2) of the ePrivacy Directive.

\textsuperscript{57} See Recital 173 of the GDPR.

\textsuperscript{58} Svantesson pp. 9, 48-49, 53, 54-55.

\textsuperscript{59} Ibid p. 48.

\textsuperscript{60} Ibid p. 9.
acts the GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation. The solution is tested against the right to private and family life and against the right to the protection of personal data.

1.4 Definitions of the Central Terms

There are some central terms that must be defined before one can start discussing the topic of the thesis. These terms are shortly described here in alphabetical order.

Algorithm is mentioned several times in the context of profiling. Algorithm is defined in the Merriam-Webster dictionary as a procedure, or as a step-by-step procedure, for solving a mathematical problem or accomplishing some end.⁶¹

Big data is an abstract term used in analytic sciences. According to the Merriam-Webster dictionary, big data is 'an accumulation of data that is too large and complex for processing by traditional database management tools'.⁶² Despite the name, big data does not necessarily need to be 'big' in amount, even though it often is. According to Laney: 'Big Data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision-making, insight discovery and process optimization.'⁶³

Cookies are described in detail in chapter 2 of this thesis. A cookie is a small data amount generated by a website and saved by a web-browser.⁶⁴

Data protection as a legal term originates from the right to privacy.⁶⁵ It is about protecting personal information of an individual, such as names, date of birth and photographs, but also IP addresses and content of communications, among other.⁶⁶

---

⁶⁶ Ibid.
Device fingerprinting means using combinations of the individual characteristics of a device in form of operating system, browser version, browser settings, location and time settings, among others, in order to identify a single device that visits a website.\footnote{Zawadziński Maciej, \textit{What Is Device Fingerprinting And How Does It Work?}, Clearcode, https://clearcode.cc/blog/device-fingerprinting/, last accessed 6 February 2018.}

Knowledge discovery in data-bases, KDD, consists of computational theories and tools that assist humans in extracting useful information (knowledge) from digital data.\footnote{Fayyad et. al., p. 1.} KDD is described in more detail in chapter 2.

Traffic data is defined in Article 2(b) of the ePrivacy Directive: "'[T]raffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.' It is to be noted that the draft ePrivacy Regulation uses the term 'metadata' instead of traffic data.\footnote{Article 4(3) (c) of the draft ePrivacy Regulation.} Metadata is defined as data that describes other data and provides information about the content of a certain item.\footnote{Tech Terms - The Tech Terms Computer Dictionary, https://techterms.com/definition/metadata, last accessed 23 February 2018.} In this thesis the term 'traffic data' is used as a collective term for both traffic data and metadata.

Privacy as a legal term is understood as a sub-notion to human dignity, as a right to be let alone and to be in control of one's own personal information.\footnote{European Data Protection Supervisor, \textit{Data Protection}, https://edps.europa.eu/data-protection_en, last accessed 6 February 2018.} It is seen mostly as an individual liberty, but also as a social value.\footnote{Ibid.} Privacy is discussed in chapter 3.

Profiling is one of the two most central terms of this thesis. There are several meanings and definitions for the term profiling. According to the GDPR Article 4(4) profiling 'means any form of automated processing of personal data consisting of using those 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'. The Council of Europe talks about 'an automatic data processing technique that consists of applying a “profile” to an individual',\footnote{CM/Rec(2010)13 appendix 1(d).} which is very similar to the description formulated by the WP 29.\footnote{WP29 Opinion 2/2010 p. 7.} The Merriam-Webster dictionary defines profiling as 'the
act or process of extrapolating information about a person based on known traits or tendencies.\textsuperscript{75} For the purpose of this thesis, profiling can be defined as a process where information is gathered and analysed and then predictively applied to an individual or to an individual case. The process involves two kinds of profiles. A \textit{group profile} consists of predictions about behaviour and characteristics of a certain group of individuals that is generated by analysing data from several individuals.\textsuperscript{76} An \textit{individual profile} consists of predictions about behaviour and characteristics of a single individual and is based on both data about the individual and on group profiles.\textsuperscript{77}

Ultrasonic beacon, an uBeacon, is a small coded piece of information, or a single signal, sent in via sound in the frequencies above the human hearing range.\textsuperscript{78} An uBeacon can be used as an identifier.\textsuperscript{79}

Ultrasound technology in the context of this thesis is technology that uses the ultrasonic (inaudibly high) sound frequencies for transformation of information. Ultrasound technology is described in detail in chapter 2.

\textbf{1.5 Disposition}

The second chapter will shortly describe profiling for commercial purposes and the technology behind it. Focus will be especially in ultrasound technology and how it differs from other tracking technologies. The third chapter will represent the right to private and family life and the right to the protection of personal data and how they are established in the human rights instruments and in the EU sources. Technology neutrality will be addressed in this context. The fourth and fifth chapter will discuss the EU legal acts on profiling and tracking technologies, the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation, and their applicability to profiling through ultrasound tracking technology. This will be followed with conclusions about the technology neutrality of the three laws and their function as safeguards against the privacy risks of the technology. The thesis will end with a short summary.

\textsuperscript{76} Hildebrandt & Gutwirth pp. 20 and 35-36.
\textsuperscript{77} Ibid. pp. 22-23 and 35-36.
\textsuperscript{78} Mavroudis et. al. p. 97.
\textsuperscript{79} Ibid.
2 Profiling and Tracking Technologies

New technologies make it easier to collect and use data of private individuals. To be able to understand the scale and the accuracy in which tracking and profiling can be done today it is necessary to describe the technology itself. This chapter will first describe in general terms what profiling and targeted advertising is. After that comes a short description of the technologies that can be used to collect the data the profiling is based on, in other words the tracking technologies. The 'traditional' tracking technologies, i.e. tracking technologies that have been in use for a longer time than ultrasound tracking technology, such as cookies, user accounts and device fingerprinting, are described on a general level while ultrasound technology will be discussed in more detail. The different tracking technologies will also be compared to each other.

2.1 From KDD and Profiles to Targeted Advertising and Customised Content

The amount of data stored in today's databases is enormous and growing all the time.\(^\text{80}\) Finding any useful information out of the big data without the help of algorithms and computers is almost impossible. The process where data is converted to useful knowledge is called knowledge discovery in databases, or KDD. The process from data to knowledge is described differently depending on who does the description.\(^\text{81}\) There are, however, some steps that they can be said to have in common: 1) data selection, 2) data-analysis and 3) interpretation/evaluation.

In the KDD process the data collected through, e.g., user accounts can be converted into behavioural patterns and predictions about individual behaviour. The data of one individual is used in two phases.\(^\text{82}\) First, when the general behavioural profiles (group profiles) are created the individual's data is put together with the existing data (step 1). Secondly, the individual's data is


\(^{81}\) Compare Fayyad et. al. p. 41 and Hildebrandt & Gutwirth p. 53.

\(^{82}\) See here Hildebrandt & Gurtwirth p. 34 ff. where David-Olivier Jaquet-Chiffelle talks about individual profiling and group profiling in the context of indirect and direct profiling.
compared to the group profiles to predict the behaviour of that individual and to make an *individual profile* (steps 2 and 3). The individual's data has an effect on the whole process. When it does not fit to the group profile the group profile is lightly modified; when it does fit the group profile it confirms the group profiles validity. On the other hand, if the individual's data does not fit in the group profile it is harder to guess the individual's thoughts and behaviour. The validity of the profiling process correlates with the data that is put in. It is therefore important to have enough data and also to have the right data. There are several methods to collect sufficient data and they are often combined. Tracking technologies are essential part of data collection.

One of the common uses of KDD based profiling is targeted advertising. An advertisement can be more effective when it is tailored for a special group of consumers (a target group) and when as many members as possible of the group see the advertisement. Some products are only meant for men and others for women, some products are thought to be sold in big quantities for an affordable price while others are luxury products for a limited group of individuals. Reaching the target group is important in the era of Internet. It is no use to show diaper advertisements to people without children. But, to get the best effect for a diaper advertisement, you should start showing it as soon as a person or a couple is expecting a child. People are more open to influence at certain times. The consuming habits of individuals are most likely to change when their life situation changes. Having children is such a change of life situation. It is important to send advertisements to people at the right time, the time when they are more likely to be influenced by the advertisements.

How do marketers know that a couple with children is interested in diapers? The answer is quite obvious, but needs to be worded out in order to understand the process of profiling. Children use diapers but they do not buy them themselves, parents are the ones who buy the diapers. This is *group profiling*. There is a correlation between people with children and consumption of diapers. When an individual has young children one can predict that he or she will most likely buy diapers.

The advertisement should be put in a place where its target group, in the current example the new or expecting parents, most likely will see it. On the Internet this would mean having diapers advertised on a family blogger's site. People who read a family blog are most likely the same people who have children and are thus interested in buying diapers. There would still be quite many readers who

---

84 Hildebrandt & Gurtwirth pp. 23-24.
86 Ibid.
87 See the definitions on group profiling and individual profiling in section 1.4 above and WP 29 Opinion 2/2010 p. 7.
have older children and do not really need diapers any more. They might be interested in children's sport clothes instead. If the marketer knows who the reader is he or she might also know when the children were born and how old they are. This is individual profiling. He or she might then be able to show different advertisements to different readers based on the age of their children. What is required is that the marketer can track single individuals and knows even which one of them is reading the blog. This can be done e.g. with the help of cookies, or with ultrasound tracking.

Making profiles is becoming more and more easy today. We leave a lot of information about ourselves and our interests on the Internet. In fact, it is almost impossible not to do so. Almost everything one does online, both on computer and on a mobile device, leaves traces with the help of technologies like cookies. Every use of a credit card or a bonus card is recorded and information stored by the company issuing the cards. Using methods of KDD it is nowadays possible to make precise predictions of our behaviour, our thoughts and our needs.

### 2.2 Collecting Data for Profiling - the 'Traditional' Tracking Technologies

Profiling cannot be done without relevant data. The collection of the data is therefore crucial for creation of profiles and targeted advertising. Tracking technologies play a central role in the whole process. The more accurate the collector is, the more accurate is the data collected and the better and the more accurate are the profiles created based on that data. The most well known tracking technologies today are cookies and user accounts. The combination of these two technologies makes the collection more effective: cookies from different devices can be collected under certain user account to create more accurate picture of a person or a group. This information can be further combined with location data. There are numerous other tracking techniques, too. E.g., Facebook connects peoples by analysing smudges on photographs to see if they were taken with the same camera lens. There are many creative ways of gathering information about private individuals. The

---

88 See the definitions on group profiling and individual profiling in section 1.4 above and WP 29 Opinion 2/2010 p. 7.
91 A good example is how Target in the U.S. learned to predict when its customers where expecting by analysing their shopping data, see Hill Kashmir, How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, Forbes, published 16 February 2012, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#634b39e26668, last accessed 24 January 2018.
92 Pettit Harry, Facebook can track who you know using the DUST on your camera: Creepy patent reveals how the site can connect people by studying smudges in photos to see if they were taken by the same lens, Daily Mail, published 12 January 2018, http://www.dailymail.co.uk/sciencetech/article-5262297/Facebook-track-using-dust-
most commonly known and used tracking technologies, cookies, device fingerprinting, user accounts and location tracking, are presented in this section.

2.2.1 Cookies and Device Fingerprinting

Cookies are character combinations or small data files that a website sends to a web browser to be saved in the browser.\(^93\) When the same web browser visits the site again the file is send back to the website. In this way the website can 'remember' that the user has been on the site before and eventually even what the user did on the site last time.\(^94\) Cookies can be everything between meaningless character combinations and full information of the user's actions, when they took place and even where they took place.\(^95\)

Cookies are used for e.g. login and shopping cart functions on e-commerce sites.\(^96\) These cookies are called *session cookies* as they are usually deleted after the user leaves the website. Without session cookies it would be impossible to have any such functions on the Internet. There are, however, cookies that are not deleted and that can follow or track the same user across different websites.\(^97\) These so called *third party cookies* are used by e.g. Google Adsense and Facebook.\(^98\) By using third party cookies it is possible to gather a lot of information about a single user.

Using cookies is not the only way to recognise users on a website. Device fingerprinting is a technique where a website remembers IP address, operating system or other characteristics of the user's browser or device and connects this with the user's data.\(^99\) There is thus no need to send or store data on the user's device, it is enough for the website to remember how the device of the user 'looks'.

\(^93\) [camera-lens.html](http://camera-lens.html), last accessed 1 February 2018.
\(^94\) [Tech Terms - The Tech Terms Computer Dictionary](https://techterms.com/definition/cookie), last accessed 1 February 2018.
\(^95\) Ibid.
\(^96\) Ibid.
\(^97\) Ibid.
Using cookies and fingerprinting has one flaw: they are bound to one web browser. Activity on other browsers and other devices is left outside the profiling data. One web browser can also be used by several persons which makes the data, and the profiles created on the data, inaccurate.

2.2.2 User Accounts

One way to collect data from several devices at the same time and to make sure that the data is related to one individual only is to make the individual create and use a user account. Apple and Google are two of the biggest marketing actors to rely on user accounts. When a consumer buys an iPhone or an iMac he or she is required to create an 'Apple id'. This id is then used on all of the Apple devices the consumer has. When the consumer gets a Gmail account Google can track him or her whenever he or she is logged in to Gmail and is browsing at the same time. By using a user account one can track the same individual not only through third party cookies but also through combining these cookies on different devices. In principle, everything one does with an iPhone is sent to Apple and can be used for marketing profiling. This includes data about consuming behaviour, interests and hobbies, family, friends and even about location and movements of the user.

2.2.3 Location Data

It is possible to know the location of a device, and therefore even the location of the individual using that device, by using the GPS on the device. It is nowadays possible for a user to set the location tracking on and off him- or herself on a mobile phone. Another way to find out the individual's location is to use the IP address of the device. GPS coordinates and IP address can both be included in traffic data, i.e., data that does not reveal the content of a transmission but can reveal other information around it.  

100 See about mobile device fingerprinting in Arp et. al. p. 24 and device pairing in Mavroudis et. al. pp. 97 and 99.  
102 Apple privacy policy.  
103 Google privacy policy.  
104 Apple privacy policy.  
105 Internet service providers (ISPs) collect and use traffic data to be able to charge the use of their services.
Another, more recent technique to track location of users of mobile devices is so called wifi-tracking. When a device is connected to a wifi certain data packets are regularly sent between the device and a wifi base station in order to maintain the connection. This requires that the device has a unique identifier, such as a MAC address or an IMEI, to be identifiable to the wifi network. A wifi base station has a specific range where the information can be captured and transferred. The movements of a single mobile device can be tracked inside, e.g., a shopping mall by following through which base stations the wireless connection to the mobile device passes.

Cookies, fingerprinting, user accounts and location tracking with GPS, IP address or wifi technology are widely used today to collect information about private individuals and their behaviour. Combined they make it easy to collect a lot of data. Still, there are gaps left in the net of tracking technologies. When the user puts down his or her mobile device and turns on the TV or the radio, tracking through cookies ceases. When the user goes inside a shopping mall the GPS signals cannot reach him or her. Wifi-tracking, that is widely used indoors in shopping malls, does not cover those users who have turned off wifi connection on their devices. And so on. To fill all the gaps is, however, possible. The solution is ultrasound tracking technology which will be described in detail in the following section.

### 2.3 Ultrasound Tracking Technology

A human being can consciously hear sound on frequencies 20 Hz - 20 kHz. Frequencies below 20 Hz (infrasound) and above 20 kHz (ultrasound) can normally not be perceived by humans. Ultrasound is the inaudible sound on frequencies 20 kHz and higher. However, most people do not hear sounds above 17 kHz. Only younger or more sensitive persons have this ability. Sound on frequencies between 17 and 20 kHz are also called ultrasound. These lower ultrasonic frequencies can be used for inaudible communication with so called uBeacons. An uBeacon is an ultrasound

---


107 Arp et. al. p. 7.

108 Ibid.

109 Ibid. See also pp. 17-18 where the frequencies between 18 and 20 kHz are tested on humans, who are found to have difficulties to hear these frequencies.

110 Ibid. p. 7.

111 Ibid. pp. 7 and 17-18.
signal encoding a small sequence of characters and symbols, which can be used as an identifier. The commercial speakers and microphones usually don't support frequencies above 20 kHz, so the frequencies that can be used for communication with inaudible uBeacons are those of 18-20 kHz.

Ultrasound communication is communication with sound. Only a sender and a receiver are needed to make ultrasound communication possible. A sender can be any kind of device that can send ultrasound signals. The device must have a speaker. A receiver has to have a microphone able to receive ultrasound signals. The sender, e.g. a device mounted at the entrance of a store, transmits an uBeacon that includes information of, e.g., the sender's location. The receiver, e.g. a mobile phone carried by a customer who enters the store, 'hears' the uBeacon via its microphone. The uBeacon is read and de-coded on the mobile phone and sent to an external sever. In this way the controller of the server knows that the owner of the mobile phone is in a certain store and can now be more readily influenced by offers relating to that specific store. This technique based on location is used by, e.g., Lisnr and Shopkick applications. Both Lisnr and Shopkick are providing services that include providing content and messages based on exact location. Lisnr is used in e.g. festivals and concerts where the visitors can navigate and receive location triggered messages via the Lisnr application. Shopkick is an application that rewards the user when he or she walks in a Shopkick partner's store.

Besides location tracking the ultrasound technology can be used for other kind of tracking, too. As already mentioned above, the user account technique requires the user to be signed in on the account on all his or her devices for the cross-device tracking to be possible. Ultrasound does not have this limitation. Connecting different devices to one person is easy if all the devices can be made to send and receive uBeacons. The device pairing technique is used by the Google Cast application which uses ultrasound to pair the user's mobile device to his or her Google Chromecast. The user can identify him- or herself through ultrasonic device pairing. Google is using ultrasound as a way of authentication and identification, but the technique could be used

112 Mavroudis et. al. p. 97.
113 Arp et. al. p. 7 and Mavroudis et. al. p. 97. See also Arp et. al. pp. 17-18 where the authors find that 60% of devices can detect ultrasonic beacons.
114 Arp et. al. p. 3 and Mavroudis et. al. p. 96.
117 Mavroudis et. al. p. 99.
118 Ibid. pp. 95-96.

22
Devices which hear each other’s signals often enough belong most likely to the same person. It is also possible to deduce who are close to each other. Two mobile devices hearing each other often enough and still belonging to two different persons are most likely devices of two people who live, work or spend their free time together.

Use of traditional media has long been outside the reach of data collectors. Today TV and radio can be tracked, too. A TV advertisement can be marked with an uBeacon that is ‘heard’ by the TV viewer’s mobile phone. The uBeacon can carry information about the content, time or location of the broadcast. This information can be used for deducing what program and for how long the owner of the mobile phone is watching on TV. E.g., an uBeacon containing information about the time and the current TV channel is embedded in the sound tape of a TV advertisement. When the advertisement is on, the mobile phone of a TV viewer can hear the uBeacon and again read and decode it and send it to an external server of the advertiser. When the next advertisement of the same advertiser comes on, the procedure is repeated. By combining the information from these occurrences it is possible to deduce that the owner of the mobile phone had a certain TV channel on at a certain time. When this information is combined with the TV schedules it is found out what the owner of the mobile phone likes to watch on TV and when. SilverPush and Signal360 are examples of companies and applications that use uBeacons embedded into websites or TV advertisements.

The user receives advertisement on his or her mobile phone after being in front of a specific displayer for a certain amount of time. SilverPush is the most known of these two especially after the Federal Trade Commission of the U.S. (FTC) issued a warning letter to service providers who used the SilverPush code in their products without informing their users.

Using only ultrasonic frequencies is an effective means of data collection. Analysing all sound, including the audible frequencies, would give much more precise data about a person. Listening to all sound all the time is, however, computationally more demanding to analyse than single uBeacons and would quickly drain the battery of a mobile device. Besides, only an uBeacon can carry additional information about the location, time and context of the signal. UBeacons make it

120 The technique opens up for de-anonymisation and other more serious privacy threats, see Arp et. al. p. 5 and Mavroudis et. al. pp. 102-104.
121 Arp et. al. p. 5.
122 Ibid.
125 FTC letter.
126 Arp et. al. p. 21.
127 Ibid.
possible to hide messages in sound waves, which cannot be done by using audible frequencies. The technology can thus be used as a substitute for other communication networks on short distances.\textsuperscript{128} It could, according to some, even be possible to spread malware, e.g. computer viruses, with ultrasonic signals and take over control of systems secured with isolation, so called 'air gapped' systems.\textsuperscript{129} 'Air gapped' computer systems are isolated both physically and computationally so that there is no connection between the computer system and the outside world. 'Air gapping' has been used in, e.g., the headquarters of the United States Department of Defense, the Pentagon.\textsuperscript{130} The systems are seldom secured from sound, though, which creates an useful channel for attackers.\textsuperscript{131} All in all, ultrasound technology offers a wider range of possible applications than audible signals.

The technology does have some limitations, though.\textsuperscript{132} Firstly, several TV channels cut off at a frequency lower than 18 kHz and can therefore not include uBeacons. The second limitation is that only the frequency range of 18-20 kHz is realistic and technically feasible for the use of ultrasound technology. Third limitation is that the periodic attempts at decoding uBeacons strain the battery of a device and prevent other applications from using the speaker and the microphone.\textsuperscript{133} Finally, uBeacons cannot reliably transfer large volumes of data and can only be used for shorter pieces of encoded information.\textsuperscript{134} This means that even though the technology has high potential in terms of data transmission and data collection, it cannot replace existing technologies used for profiling purposes. Other tracking technologies will likely maintain their significance even when the use of ultrasound tracking technology has become more common. It is also possible to take preventive actions against ultrasound tracking. However, ultrasound can still play an important role as it is very easy to deploy. Many mobile devices have the technology needed to send and receive ultrasonic beacons build in them already. Only thing needed is that the user loads in an application that can decode the uBeacons. What is more, ultrasound tracking technology is extremely difficult to detect and compared to older tracking technologies it can be used to collect much more precise data on individuals.

\textsuperscript{128} Young p. 8.  
\textsuperscript{129} Ibid. pp. 17-18 and 20-22.  
\textsuperscript{130} Ibid. pp. 17-18.  
\textsuperscript{131} Ibid. p 18.  
\textsuperscript{132} Arp et. al. pp. 18 and 20-22.  
\textsuperscript{133} Mavroudis et. al. pp. 100-101.  
\textsuperscript{134} Ibid. p. 99.
2.4 Analysis of Chapter 2

The excessive use of profiling is making us more vulnerable to influence. Information once considered as strictly private has become public due to the rise of new technology. Precise behavioural profiles can be created with the help of precise behavioural data. To collect precise data becomes more easy by the use of ultrasound tracking technology.

Technologies most used in tracking users on the Internet are cookies and device fingerprinting. Fingerprinting, or remembering the characteristics of the user's device, does not need any activity from the user's side. It is impossible to know when fingerprinting is done. Fingerprinting only happens on one end of the communication. Just like the use of cookies, ultrasound tracking requires activity on the user's device. Both cookies and uBeacons carry small amounts of data and are sent from one device to another. The difference is that cookies are fetched back from the user's device. The information in uBeacons is collected and sent onwards; there is no two-way communication with the same data as with cookies. Cookies from different devices can be connected by device-pairing with the help of the ultrasound technology. Ultrasound improves the use of cookies.

By connecting different devices with ultrasound technology it is possible to track the same user on different devices. Tracking across the screens is already in use, not through ultrasound but through the use of user accounts. User does not need to be logged in by using the same user account on every device for the ultrasound tracking technology to work, which is a big difference compared to other technologies. Ultrasound also enables connection of devices without the user's knowledge. It makes the connection between different user accounts and media (TV, radio etc.) possible, too.

Ultrasound can be used to collect location data. Location data can be collected from various sources and through various technologies, but ultrasound tracking technology enables collection of more precise location data. The user's movements can be tracked inside a room. It is also possible to know who the user is in close proximity to by connecting his or her device to other people's devices. On the other hand, ultrasound can only be used on small distances. For location tracking technique to work, senders have to be installed on the location or other devices using the technology have to be nearby. In this regard ultrasound tracking technology is very similar to wifi-tracking, in which the user needs to walk near a wifi base station.

Consequently, ultrasound tracking technology bears some similarities to the other tracking technologies. UBeacons can be equated with cookies in some aspects. The technology does also
bear considerable similarities to device fingerprinting and wifi-tracking techniques. Whether the technologies are similar enough to be covered by the same legislation is discussed in chapter 5. The general regulation on profiling can, however, also limit the use of the technology. This latter option is discussed in chapter 4.

Ultrasound tracking technology, especially when combined with other techniques, is more intrusive than the 'traditional' tracking technologies since it can help collect much more precise data about individuals. It is the intrusiveness of the ultrasound technology that raises concerns. The technology has potential for very harmful applications and misuses. On the other hand it could make the use of some services easier, such as location based reward systems like Lisnr and Shopkick. The technology has potential to become one of the safer authentication applications, such as Google's use of ultrasound to connect the user's mobile phone to his or her Google Chromecast, and as a communication channel in situations where other mobile connections do not work. Prohibiting ultrasound technology as such would therefore be disproportionate. The serious privacy and security risks related to the ultrasound tracking technology and the profiling based on it must still be addressed. More so considering the importance of the notion of the right to privacy and the right to data protection. The right to privacy and the right to data protection will be discussed in the next chapter.
The concept of privacy is seen as something very abstract and hard to capture.\(^{135}\) Despite its abstract nature, privacy is seen as a fundamental human right of great value. The majority of Europeans feel uncomfortable with online profiling and would like to be able to refuse the collection and procession of their personal data.\(^{136}\) Profiling and tracking are seen as intrusions to privacy and to the intimate sphere of life. The right to privacy covers many things and is codified in several human rights instruments where it is called the right to private and family life. The right to the protection of personal data, or the right to data protection, is in some cases interpreted as part of the right to private and family life; yet it is a separate right in other cases.

This chapter will first describe privacy as a general concept. The two fundamental rights connected to privacy, their differences and interconnected nature, as well as how they are codified in the EU, will be described. The principle of technology neutrality as a means of achieving full penetration of the two rights is also discussed.

### 3.1 Privacy

Privacy can be described as a right to be let alone.\(^{137}\) It can also be said to be a right to personal integrity,\(^{138}\) a right to secrecy\(^{139}\) or intimacy,\(^{140}\) and as a right to control information about oneself.\(^{141}\) In fact, privacy can be described in so many ways that some scholars have fallen in despair when trying to define what privacy is.\(^{142}\) According to Solove, privacy ‘is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other’.\(^{143}\)

Defining privacy can therefore be hard and a full definition will be left out of the scope of this thesis. A general description of the concept of privacy is still laid out here.

---

135 Svantesson p. 3 f.
143 Ibid. p. 756.
Privacy is a very abstract concept. Instead of trying to define what privacy is Solove approaches privacy from the opposite direction than most and defines what it is not. Solove creates a taxonomy of problems related to lack of privacy. These privacy problems include surveillance, interrogation, insecurity, exclusion, breach of confidentiality and disclosure, blackmail, intrusion and decisional interference, among many others. Privacy as a right seeks to protect the individual against the intrusion of others to his or her person.

Yet, despite of its essential nature as an individual right, privacy can be seen as a precondition for a functioning democracy. According to Solove: 'Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others.' A society without a certain amount of freedom cannot call itself a democracy. Only free individuals can make free choices and having the freedom to hide one's thoughts, habits and other facts about oneself is an essential part of this freedom. The European Data Protection Supervisor (EDPS) sees the rights to privacy and to data protection as preconditions for creativity, innovation, freedom of expression and for democracy in general. According to the EDPS, constant surveillance discourages spontaneity, rewards conformist behaviour and makes people watch their own behaviour, which has a chilling effect on other fundamental rights and freedoms, such as freedom of expression and freedom of assembly and association. The protection of the private sphere is therefore of fundamental importance for the function of a democratic society.

3.2 The Right to Private and Family Life

The grounds for the right to private and family life, the right to privacy, are laid out in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). The right is seen in most parts of the world as one of the fundamental rights of an individual. Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union (EU Charter) are similar to Article 17 ICCPR. Both the ECHR and the EU Charter have special legal significance as primary sources of EU law according to the Lisbon Treaty.
Article 8(1) of the ECHR, to which the Article 7 of the EU Charter is identical, protects private life, family life, home and correspondence of an individual. The scope of the Article 8 right is thus wider than the right to privacy. The right to private life concerns a 'sphere within which everyone can freely pursue the development and fulfilment of his personality' and 'includes the right to develop relationships with other persons and the outside world'. Telephone tapping and other use of 'covert technological devices' falls within the scope of private life.

Article 8(2) of the ECHR reminds that the right to privacy is not an absolute right but can be interfered under some circumstances when the interference is done in accordance with a law and 'is necessary in a democratic society'. Acceptable reasons to interference with the right are national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

3.3 The Right to the Protection of Personal Data

The right to protection of personal data is codified in several international conventions. It is interpreted to be part of the right to privacy in Article 17 of the ICCPR and Article 8 of the ECHR. Regarding the EU, the primary sources that are being referred to when it comes to the right to data protection are Article 8 of the ECHR and Article 7 of the EU Charter (the right to private and family life) as well as Article 8 of the EU Charter and Article 16 of the TFEU (the right to the protection of personal data). The ECHR and the EU Charter are the ultimate instruments for the right but the TFEU is more close to the operational level of legislation, even though all three instruments are binding primary law of the EU.

The right to private and family life in Article 8 of the ECHR and Article 7 of the EU Charter includes the right to the protection of personal data. Collection of personal data by state officials without the individual's consent and inability to access one's own personal data in the state's records

154 Kilikelly Ursula, The right to respect for private and family life, A guide to the implementation of Article 8 of the European Convention on Human Rights, Human rights handbooks, No. 1, Council of Europe, Germany, 2003, p. 11.
155 Ibid.
156 Ibid. p. 12 f.
157 The Treaty of the Functioning of the European Union.
fall within the scope of Article 8 of the ECHR.\textsuperscript{158} The right to protection of personal data is thus part of the right to private and family life.\textsuperscript{159} The right to data protection in Article 8 of the EU Charter and Article 16 of the TFEU is strongly connected to the right to privacy in Article 8 of the ECHR and Article 7 of the EU Charter, but the right to data protection is given a separate status in the former instruments.

Article 8 of the EU Charter (as well as Article 16(1) of the TFEU) provide that everyone has the right to the protection of personal data concerning him or her and states that ‘such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’ and that ‘everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified’. Article 8 of the EU Charter is based on Article 8 of the ECHR and specified in the GDPR and the ePrivacy directive as well as in the draft ePrivacy Regulation.\textsuperscript{160}

3.4 The Right to Privacy and the Right to Data Protection in the EU Secondary Law

As became clear in chapter 2, profiling based on ultrasound tracking is very intrusive and carries many privacy risks. Protection against wrongful use of the technology must be found if the right to private and family life and the right to the protection of personal data are to be realised. The ECHR, the EU Charter and the TFEU lay down the fundamental rights to privacy and to data protection, but they do not have a direct effect. The rights must be concretised in the secondary law. Whether the protection is found in the EU law depends thus on the EU secondary laws, the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation. Technology neutrality, or lack of it, has an important role in the matter.

\textsuperscript{158} Kilkelly Ursula, \textit{The right to respect for private and family life, A guide to the implementation of Article 8 of the European Convention on Human Rights}, Human rights handbooks, No. 1, Council of Europe, Germany, 2003, p. 13.

\textsuperscript{159} Ibid. p. 11.

3.4.1 The GDPR, the ePrivacy Directive and the Draft ePrivacy Regulation

In the EU the right to private and family life and the right to the protection of personal data are protected in the GDPR and in the ePrivacy Directive, among other legislation. Recital 1 of the GDPR reminds, with reference to Article 8 of the EU Charter and Article 16 of the TFEU, that ‘[t]he protection of natural persons in relation to the processing of personal data is a fundamental right’. Recital 2 states that ‘[t]he principles of, and rules on the protection of natural persons with regard to the processing of their personal data should ... respect their fundamental rights and freedoms, in particular their right to the protection of personal data’. To make it even clearer, Article 1(2) of the GDPR says that the GDPR ‘protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data’. The ePrivacy Directive also seeks to ensure full respect for the rights set out in Articles 7 and 8 of the EU Charter and reminds that confidentiality of communications is guaranteed in the ECHR.\(^\text{161}\) The main purpose of the GDPR and the ePrivacy Directive is to protect the right to the protection of personal data. The same applies to the draft ePrivacy Regulation.\(^\text{162}\)

3.4.2 Technology Neutrality as a Leading Principle

Technology neutrality is a regulatory principle that was first introduced in the EU regulatory framework on telecommunications services in Directive 2002/21 on a common regulatory framework for electronic communications networks and services (the Framework Directive).\(^\text{163}\) Recital 18 of the Framework Directive defines technology neutrality as follows: ‘[t]he requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, i.e. that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, e.g. digital television as a means for increasing spectrum efficiency.’ The core idea in this Recital is that the legislator should not decide whether or not a certain technology is good.\(^\text{164}\) This is to be left for the market to

\(^{161}\) Recital 2 of the ePrivacy Directive.
\(^{162}\) See the explanatory memorandum of the draft ePrivacy Regulation under 1.1. Reasons for and objectives of the proposal.
decide. Moreover, the legislation should not discriminate certain type of technology. As formulated by Maxwell and Bourreau: 'technology neutrality means that the same regulatory principles should apply regardless of the technology used.'

The principle of technology neutrality was reinforced in the 2009 revision of the telecommunications legislation, which included the revision of the ePrivacy Directive, and most recently in the GDPR adopted in 2016. Recital 4 of the ePrivacy Directive addresses the technological development that made the 2009 reform of the ePrivacy Directive necessary: '[the ePrivacy Directive] has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used.' Technology neutrality is also mentioned in Recital 15 of the GDPR which speaks about the material scope of the GDPR: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.' The draft ePrivacy Regulation is also meant to be technologically neutral.

Technology neutrality is further emphasised in the principle of privacy by design in Article 25(1) of the GDPR which seeks to promote industry self-regulation on privacy. As said by Maxwell and Bourreau, the technology neutrality in the principle of privacy by design regulates the result to be achieved (i.e. privacy) and not the technology needed to achieve the said result. This formulation is the other side of the above described formulation of technology neutrality, namely 'that the same regulatory principles should apply regardless of the technology used.' Technology neutrality can thus be described in slightly different ways.

Regardless of the formulation, the principle of technology neutrality means a shift of focus from the means to the result. In the context of the EU privacy and data protection legislation this means that the emphasis should be on the penetration of the right to privacy and the right to data protection and not on the technology used. Should the opposite be the case, i.e. that the focus was on the
technology, the risk that the law should fall behind the technological development would increase remarkably.¹⁷²

3.5 Analysis of Chapter 3

The argument that only those who have something to hide should worry about privacy is well known. Those protecting privacy often refer to George Orwell's 1984 as an ultimate example of what would happen if the state could watch every step of its subjects. In today's world our steps are literally watched through our mobile devices. The one watching, though, is in most cases not the state but private marketing actors. Profiling through ultrasound tracking technology is a good example of a privacy intrusive technology. The technology is so recent it has not been taken into account in the GDPR and the draft ePrivacy Regulation, and certainly not in the ePrivacy Directive that was adopted before ultrasound tracking technology existed. The level of technology neutrality of the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation decides whether or not profiling through ultrasound tracking technology falls within the scope of these laws. If the technology falls outside of the material scope of these laws the right to privacy and the right to data protection are not fully realised in the EU law.

In order to evaluate whether the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation are technologically neutral in that they truly protect the right to privacy and the right to data protection in the context of profiling through ultrasound tracking, one must first consider the general regulation around profiling. It is the widened possibilities to profiling that constitute the main risk carried by the technology. The legislation on tracking technologies should also be considered. The next two chapters will discuss the special legislation on profiling and tracking technologies. The aim is to clarify which rules in the GDPR, in the ePrivacy Directive and in the draft ePrivacy Regulation apply to profiling in general and might thus affect the use of ultrasound technology, and which rules, if any, apply to the ultrasound tracking technology in particular.

¹⁷² Svantesson p. 22.
4 Regulating Profiling in the European Union: the GDPR

The General Data Protection Regulation (GDPR) is one of the latest developments in the European privacy and data protection reform. One of its main goals is to harmonise the data protection legislation in the EU which has become somewhat splintered due to the differentiating national implementation of the Data Protection Directive.\(^{173}\) On top of harmonisation, the GDPR has the aim of strengthening the right to the protection of personal data in practice by giving the control over personal data to the data subject.\(^{174}\) The GDPR is material legislation that gives effect to the fundamental rights established in the ECHR, the EU Charter and the TFEU. The main idea of the GDPR is that the data subject should have full access to all personal data concerning him or her, and should have the right to get the data corrected or rectified when necessary. Most importantly, collection of personal data should be limited to the absolute minimum and be based either on law or on an unambiguous consent of the data subject.\(^{175}\)

Recital 4 of the GDPR reminds us that the right to protection of personal data is not an absolute right. The GDPR is balancing between this right and other fundamental rights and freedoms and the functions of the right to protection of personal data in society. One important intention with the GDPR is to ‘contribute to the accomplishment of ... an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market’.\(^{176}\) Free movement of data is essential for the functioning modern society and therefore it must also be secured.

During the legislation process of the GDPR a general prohibition on profiling was proposed.\(^{177}\) In the final version, though, only profiling in the context of individual decision-making is prohibited \emph{per se}.\(^{178}\) This does not mean that profiling in general was unregulated by the GDPR, quite the opposite. Profiling is given a definition in Article 4(4) where behavioural profiling is particularly mentioned. Recital 72 states explicitly that profiling is covered by the GDPR provisions ‘governing the processing of personal data, such as the legal grounds for processing or data protection

\(^{173}\) See Recitals 9 and 10 of the GDPR.
\(^{174}\) Recital 7 of the GDPR.
\(^{175}\) Recital 32 of the GDPR.
\(^{176}\) Recital 2 of the GDPR.
\(^{177}\) Article 20 of the draft GDPR.
\(^{178}\) Article 22 of the GDPR.
principles'. Recital 70 states that there should be a right to object profiling in the context of direct marketing 'at any time and free of charge'. Profiling is mentioned in several Recitals even outside these ones. It is the meaning that the GDPR should address also profiling in general. How this is done in the substantial provisions of the GDPR is discussed in the following.

4.1 Applicability to Profiling and the Two Kinds of Profiling in the GDPR

According to Article 2(1) the GDPR applies to 'processing of personal data wholly or partly by automated means'. 'Processing' is defined in Article 4(2) as any operation or set of operations performed on personal data. Basically any activity that is done with personal data, including sole possession of such data is processing in the meaning of the GDPR. 'Personal data' is defined in Article 4(1) as any information relating to an identified or identifiable natural person (data subject). A person can be identifiable even by a combination of different factors that do not alone identify the data subject.

The territorial scope of the regulation is somewhat unique. According to Article 3(1) the GDPR applies to processing of personal data when the controller or the processor has an establishment in the EU, regardless of whether or not the processing takes place inside the EU. It is also applicable to processors and controllers outside the EU when the subject for the processing of the data is in the EU and the processing is related either to offering of goods or services in the EU or to monitoring of the data subject's behaviour as far as the behaviour takes place in the EU (Article 3(2)). The result of this is that when companies are tracking and profiling individuals inside the EU they must always comply with the GDPR.

Profiling is defined in Article 4(4) of the GDPR as following: '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.'

Apart from the definition in Article 4(4), only Article 22 of the GDPR on automated decision-making mentions profiling in particular. Article 22(1) states that '[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling,
which produces legal effects concerning him or her or similarly significantly affects him or her'. Only decision-making that is necessary for entering into or performance of a contract, is authorised by law or is based on the data subject's explicit consent is allowed according to Article 22(2). This means fewer legal grounds for processing of data than what applies to other kind of processing.\textsuperscript{179} When decision-making is based on contract or the data subject's consent, 'the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision', according to Article 22(3). Article 22(4) states explicitly that automated decisions shall not be based on special categories of data referred to in Article 9(1), unless the data subject has given his or her explicit consent to processing of the special category of data or the processing is based on Union or Member State law, and unless suitable measures are taken to safeguard the data subject's rights and freedoms and legitimate interests.

In its Guidelines on automated decision-making and profiling\textsuperscript{180} the Article 29 Working Party\textsuperscript{181} (WP 29) clarifies the applicability of the GDPR on profiling. The WP 29 makes a distinction between profiling that falls under the general regulation of the GDPR and profiling that falls under Article 22. According to the WP 29 Guidelines on profiling the GDPR 'applies to the collection of data for the creation of profiles' and to 'the application of those profiles to individuals'.\textsuperscript{182} 'Profiling' as addressed in Article 4(4) GDPR and which falls under the general regulation of the GDPR is, according to WP 29, composed of three elements: it is an automated form of processing, it is carried out on personal data and its objective is to evaluate personal aspects about a natural person.\textsuperscript{183}

Article 22 regulates automated decision-making. The WP 29 defines automated decision-making as 'the ability to make decisions by technological means without human involvement'.\textsuperscript{184} It is important to note that decision-making that is not wholly automated falls outside the scope of Article 22, but is still regulated by the general provisions of the GDPR.\textsuperscript{185} Automated decision-making can involve

\textsuperscript{179}The legal grounds for processing in general are found in Article 6(1) of the GDPR.
\textsuperscript{181}The Data Protection Working Party established by Article 29 of Directive 95/46/EC, hereafter the WP 29. The WP 29 is an independent advisory organ that provides advice and guidance on data protection matters. The WP 29 is composed of representatives of the national supervisory authorities, a representative of the European Data Protection Supervisor (EDPS) and of a representative of the European Commission.
\textsuperscript{182}WP29 Guidelines on profiling p. 6 and Recital 72 of the GDPR.
\textsuperscript{183}Ibid. p. 7.
\textsuperscript{184}Ibid. p. 6.
\textsuperscript{185}Ibid. p. 8.
profiling but it does not have to do so. Profiling can also happen without it being part of automated decision-making. Regardless of whether profiling falls under Article 22 or not, it has to be in compliance with the overall regulation in the GDPR according to the WP 29’s interpretation. The difference is that profiling in the context of automated decision-making under Article 22 is regulated more strictly than profiling for other purposes.

Profiling for commercial purposes falls under the general provisions in the GDPR. It is possible, though, that even commercial profiling can be seen as automated decision-making in Article 22 and therefore falls under the stricter rules, according to WP 29. Whether this is the case depends upon whether the result of the profiling (i.e. the targeted advertising) has a significant effect on the individual. The facts revealing such significant effect could, according to WP 29, be the intrusiveness of the profiling process, the expectations and wishes of the individuals concerned, the way the advertisement is delivered and the particular vulnerabilities of the data subjects targeted, among other characteristics of the individual case. In this context, the WP 29 names particularly profiling which results in differential pricing. It could have a significant effect on an individual in a case where the pricing effectively prevents the individual from buying certain products.

4.2 Substantive Regulations Applicable to Profiling

It is clear that profiling for commercial purposes falls under the provisions of the GDPR, even if the applicability of Article 22 is somewhat unclear and may vary from case to case. The commercial actors willing to engage in profiling must therefore comply with the regulations of the GDPR. This is particularly important since breach of the regulation results in sanctions including administrative fines rising up to 20 000 000 EUR, or 4% of the total worldwide annual turnover, whichever is higher. Problem is that due to the characteristics of many of the provisions of the GDPR it can be challenging to apply them to profiling. In this section the provisions of the GDPR which may be challenging to apply in the context of profiling, especially through ultrasound technology, will be described in general terms. The challenges will be discussed in the next section.

---

186 Ibid. p. 8.
187 Ibid. p. 8.
188 Ibid. pp. 6 and 17-25.
189 Ibid. p. 11.
190 Ibid. p. 11.
191 Ibid. p. 11.
192 Ibid. p. 11.
193 Chapter VIII and Article 83 of the GDPR.
4.2.1 Data Processing Principles and the Rights of the Data Subject

Data processing principles in Article 5(1) of the GDPR must always be considered when processing personal data, including processing in the context of any kind of profiling. These principles are lawful, fair and transparent processing in Article 5(1) (a), purpose limitation in Article 5(1) (b), data minimisation in Article 5(1) (c), accuracy in Article 5(1) (d), storage limitation in Article 5(1) (e) and integrity and confidentiality in Article 5(1) (f). On top of all this, the controller is responsible to demonstrate compliance with all these principles according to Article 5(2) of the GDPR.

The data subject is given quite extensive rights in the GDPR. These correlate the responsibilities of the data controller. The data subject has, among others, the right to information (Articles 13 and 14), the right to access to his or her data (Article 15), the right to rectification of inaccurate data (Article 16), the right to erasure of data in some cases (also known as the right to be forgotten, Article 17), the right to restriction of processing of the data (Article 18), the right to data portability (Article 20), the right to object the processing (Article 21) and the right not to be subject to automated decision-making (Article 22).

Transparency is a fundamental principle that is specially regulated in Articles 12(1), 13 and 14. The duty of the data processor correlates with the right of the data subject to have information about the processing. The data subject must be given concise, intelligible and easily accessible information about the profiling. The information must be provided at the time of the collection of the data. When the data collection is based on the data subject's consent the information must be provided before the said consent is given or the consent will not be valid. Unfair profiling, on the other hand, is e.g. targeting a consumer with excessively risky or costly financial products or otherwise offering some consumers less attractive deals than others.

The data collection must have specified, explicit and legitimate purpose or purposes and not be used for other than the beforehand given purposes. Purpose limitation is connected to the right to restriction of processing and to the principle of data minimization. The latter prohibits collection of data that is not relevant or necessary for the purposes of the processing.

Any inaccurate or unnecessary data must be erased or rectified without delay. The data subject's right to access to his or her data supports this principle. Furthermore, the data should be stored only for a limited period of time.

194 WP 29 is also writing special Guidelines on transparency.
195 See the argumentation on consent under section 4.2.3 below.
Appropriate technical and organisational measures should be taken to ensure the security of the personal data. Some guidance to what is appropriate level of security is given in Article 32 of the GDPR and in the preventive principles of privacy by design and privacy by default in Article 25, which latter are discussed in more detail below. It is also an intention that the data protection authorities will give guidance and more detailed principles on the security levels and requirements. The GDPR has a risk based approach to security, which means that processors must do objective risk assessments and take measures based on the identified risks. Account should be taken in particular to the risks presented from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data according to Article 32(2) of the GDPR. Evaluating personal aspects in order to create profiles is particularly mentioned as a more significant risk that needs closer attention. The risks established by third parties, such as foreign states, may also, according to Voigt and von dem Bussche, be a factor for the risk evaluation.

4.2.2 Privacy by Design and Privacy by Default

In addition to the principle of integrity and confidentiality of personal data in Article 5(1) (f), the GDPR also presents the principles of privacy by design and privacy by default in Article 25. The idea is that data protection would be an integrated part of the designing stage as well as the implementation stage of data processing. The measures taken should be both technical, i.e. related to hardware and software, and organisational, i.e. related to internal protocols, procedures and working routines. The data should also be appropriately protected against unintended access to the data.

Privacy by design means keeping the privacy and data protection aspects in mind from the very beginning of the product development process. Data minimisation and comprehensive pseudonymisation of the data are two of the concepts to be strived for. Privacy by default is meant to protect consumers against the widespread trend among companies to obtain as much personal

197 Article 57 of the GDPR.
198 Recital 76 GDPR. The same approach is presented in the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), see Recitals 49 and 57. The NIS Directive obliges ‘operators of essential services’ and digital services providers to take measures to meet the risks connected to network and information systems Article 14(1) and 16(1). The implementation of the NIS Directive has to be completed by 9 May 2018.
199 Recital 75 of the GDPR.
200 Voigt & von dem Bussche p. 41.
201 Ibid. p. 62.
data as possible’. The WP 29 has said in its Opinion 15/2011 that settings that put consent to data collection as a default are problematic. The opposite should be the case in order to ensure the freedom of choice on the matter. The user should have to take action in order to allow the use of his or her data. Lack of action should always mean full privacy. This is supported by the definition of consent in Article 4(11) of the GDPR and the WP 29 interpretation of it.

4.2.3 Lawful Grounds for Processing and the Definition of Consent

Article 6 of the GDPR lists the lawful grounds for processing of data. There are altogether six alternative grounds: 1) the data subject's consent in 6(1) (a), 2) performance of a contract in 6(1) (b), 3) compliance with a legal obligation in 6(1) (c), 4) protection of vital interests of the data subject or of another natural person in 6(1) (d), 5) performance of a task carried out in the public interest or in the exercise of official authority in 6(1) (e), and 6) legitimate interest of the controller or of a third party in 6(1) (f). Three of the grounds, compliance with a legal obligation, protection of vital interests and performance of a task carried out in the public interest, are left out of the current presentation since they have small significance as legal grounds for profiling for commercial purposes. Consent of the data subject in Article 6(1) (a) and processing necessary for the performance of a contract in Article 6(1) (b), on the other hand, are the ones of particular interest in the context of profiling for commercial purposes. It is to be noted that profiling that falls under Article 22 can be lawful only on three grounds, the data subject's consent, performance of a contract or authorisation of EU or Member State law (Article 22(2)). Legitimate interest of the controller or of a third party in Article 6(1) (f) must also be considered in the context of profiling that falls outside the scope of Article 22. Consent of the data subject is given the strongest emphasis in this presentation since consent of the data subject, when applied correctly, is considered to give the data subject best control over his or her data. Consent is also seen as the most complicated of the legal grounds and has been given a lot of attention in the GDPR.
Consent is recognised in the ECHR Article 8(2). It is an essential aspect of the fundamental right to the protection of personal data.\textsuperscript{207} When consent is used correctly it is a tool that gives data subjects control over their own data.\textsuperscript{208} The WP 29 has emphasised, though, that if the concept of consent is not used correctly the control becomes illusory and the processing unlawful.\textsuperscript{209} Consent as a lawful ground for processing should only be used in appropriate contexts where the requirements for a valid consent can be truly met. These requirements are 1) freely given, 2) specific, 3) informed and 4) unambiguous according to the Article 4(11) of the GDPR. According to Recital 32, a valid consent is 'given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her'. Article 7 of the GDPR provides for further conditions on consent, which are, among others, that the consent must not be obtained as a condition for entering a contract which does not require the data processing in question.

According to the WP 29 consent is freely given when the data subject has a real choice, does not feel compelled to provide consent, and will not face negative consequences of not consenting.\textsuperscript{210} In case of imbalance of power, such as when the data controller is a public authority or employer of the data subject, there is a great risk that the consent is not truly freely given.\textsuperscript{211} In such cases other legal grounds for processing should be considered instead, according to WP 29.\textsuperscript{212} Article 7(4) of the GDPR states that consent bundled with acceptance of terms and conditions or 'tying' the provision of a contract or a service to a consent to process personal data that is not necessary for the performance of that contract or service are unacceptable. In addition, consent that is a non-negotiable part of a contract is presumed not to be freely given.\textsuperscript{213} The data subject must also have the possibility to give separate consent for the data processing operations, when appropriate. According to the WP 29: '[i]f the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom.'\textsuperscript{214} Furthermore, not consenting or a withdrawal of a consent must not lead to any costs or service downgrading for the data subject.\textsuperscript{215}

\textsuperscript{207} See also WP 29 Opinion 15/2011 p. 5.
\textsuperscript{208} Ibid. p. 2.
\textsuperscript{209} Ibid. pp. 2 and 8-10.
\textsuperscript{210} WP 29 Guidelines on consent p. 6 and Opinion 15/2011 p. 12.
\textsuperscript{211} Recital 43 of the GDPR and WP 29 Guidelines on consent pp. 7-8.
\textsuperscript{212} WP 29 Guidelines on consent p. 7-8.
\textsuperscript{213} Recital 43 of the GDPR and WP 29 Guidelines on consent pp. 6 and 9.
\textsuperscript{214} WP 29 Guidelines on consent p. 11.
\textsuperscript{215} Ibid. p. 11.
For the consent to be specific it must be clearly separated from other matters. Different data processing purposes must be presented in a way that the data subject can consent to each and every one of them separately and independent of each other.\textsuperscript{216} The requirement of specification aims to give the data subject control over his or her data and is closely linked to the requirements that the consent must be freely given and informed.

Consent is informed only if the data subject has been provided with information about the processing in clear and plain language, and when the consent to data processing is clearly distinguishable from other matters.\textsuperscript{217} Presentation of the information must be chosen to best fit the group of data subjects that is the target of the data processing.\textsuperscript{218} As for what information must be given, Article 13 of the GDPR provides for some guidance.\textsuperscript{219}

Consent is unambiguous if it is obvious that the data subject has consented to the particular data processing action.\textsuperscript{220} Silence or passivity from the data subject's side does not constitute a valid consent. The WP 29 is of the opinion that physical motions, such as swiping on the screen or waiving to a camera, can be qualified as a clear affirmative action in compliance with the GDPR.\textsuperscript{221} There is a risk that data subjects get tired of the consent and information notions and stop reading the information. There are several opinions in the favour of browser settings as a way of obtaining valid consent.\textsuperscript{222}

The WP 29 has also on different occasions emphasised that consent should be given prior to the processing activity and still holds to the opinion: '[a]lthough the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording “has given” in Article 6(1)(a) support this interpretation.'\textsuperscript{223}

Article 7(3) of the GDPR states that the data subject must be able to withdraw his or her consent at any time. Withdrawal of consent must be as easy as giving the consent.\textsuperscript{224} Providing information is crucial even for the right to withdrawal. The WP 29 says in its Opinion 5/2005 about consent related to location tracking that 'it is a precondition for the exercise of [their rights] that individuals are kept

\textsuperscript{216}Ibid. p. 12.
\textsuperscript{217}Ibid. pp. 14-15.
\textsuperscript{218}Ibid.
\textsuperscript{219}See also WP 29 opinion on what information must be provided in WP 29 Guidelines on consent p. 13.
\textsuperscript{220}Ibid. pp. 16-17.
\textsuperscript{221}Ibid. p. 17.
\textsuperscript{222}Ibid. p. 17.
\textsuperscript{223}Ibid. p. 18. See also WP 29 Opinion 15/2011 pp. 30-31.
\textsuperscript{224}See also WP 29 Guidelines on consent pp. 21-22.
informed, not only when they subscribe to a service but also when they use it ... the service provider should regularly remind the individual concerned that his or her terminal equipment has been, will be or can be located.' Obtaining consent and offering the right to withdrawal or objection must be held separate; the latter are opt-out actions to be done after the data processing has already started and the former is an opt-in action to be done prior to the start of the processing.\textsuperscript{225}

Recital 44 and Article 6(1) (b) of the GDPR state that data processing 'should be lawful where it is necessary in the context of a contract or the intention to enter into a contract'. When processing is necessary for performance of a contract is not further explained in the GDPR but has been addressed by the WP 29. According to WP 29, the expression 'necessary for the performance of a contract' needs to be interpreted strictly.\textsuperscript{226} There needs to be a direct link between the processing action and the individual contract situation.\textsuperscript{227} The WP 29 gives examples of situations where processing is necessary to fulfil a contract. These are processing the address of the data subject so that goods purchased online can be delivered and, in the employment context, the processing of salary information and bank account details so that wages can be paid.\textsuperscript{228}

According to Article 6(1) (f), data processing is lawful if it 'is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' This legal ground differs from the other legal grounds in that it does not apply to the processing by public authorities in the performance of their tasks. According to Recital 47 of the GDPR: '[s]uch legitimate interest could exist e.g. where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.' Processing of personal data must thus be implicit in the context of the individual case. Preventing fraud, transmitting personal data within a group of undertakings for internal administrative purposes

\textsuperscript{225} WP Opinion 15/2011 pp. 30-33 and WP 29 Guidelines on consent pp. 17 and 21
\textsuperscript{226} WP 29 Guidelines on consent p. 9 and WP 29 Opinion 06/2014.
\textsuperscript{227} WP 29 Guidelines on consent p. 9.
\textsuperscript{228} Ibid. p. 9.
and ensuring network and information security are mentioned as situation where the data controller has a legitimate interest to process personal data.\textsuperscript{229}

According to Recital 47 of the GDPR, processing of personal data for direct marketing purposes may fall within the requirements of a legitimate interest of the data controller in Article 6(1) (f) of the GDPR. The data controller can thus rely on the direct marketing purposes as a legal ground for data processing. It must be noted that the controller's legitimate interest does not make the profiling lawful if the profiling falls within Article 22(1) of the GDPR.\textsuperscript{230} When applying Article 6(1) (f), one must consider, though, whether the legitimate interests of the data controller are overridden by the interests or fundamental rights and freedoms of the data subject. According to the WP 29, the following must be considered: the level of detail of the profile, the comprehensiveness of the profile, the impact of the profiling (the effects on the data subject), and the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.\textsuperscript{231} The future use and combinations of the profiles should also be considered according to the WP 29.\textsuperscript{232}

According to the WP 29, a processing activity for one specific purpose cannot be based on more than one legal ground.\textsuperscript{233} The data controller must define the legal ground for processing in advance; if the data processing is based on consent and the consent is later withdrawn the data controller cannot use the other legal grounds as a 'back-up'.\textsuperscript{234} It should also be noted that the data subject's consent does not free the data controller from his or her other obligations under the GDPR, especially the data processing principles in Article 5.\textsuperscript{235} Consent cannot legitimise data processing that would otherwise be prohibited, except in limited cases.\textsuperscript{236} The grounds in Articles 6(1) (a) (consent) and 6(1) (b) (performing of a contract) must thus be kept separate: '[e]ither processing is necessary to perform a contract, or (free) consent must be obtained.'\textsuperscript{237} The same should apply to the mixed use of consent and legitimate interest and of contract and legitimate interest.

\textsuperscript{229} Recitals 47, 48 and 49 of the GDPR, respectively.
\textsuperscript{230} Article 22(2) of the GDPR.
\textsuperscript{231} WP 29 Guidelines on profiling p. 21.
\textsuperscript{232} Ibid. p. 22.
\textsuperscript{233} WP 29 Guidelines on consent pp. 22-23.
\textsuperscript{234} Ibid.
\textsuperscript{235} Ibid. pp. 4-5. See also WP 29 Opinion 15/2011 pp. 7-8.
\textsuperscript{236} Ibid.
\textsuperscript{237} WP 29 Opinion 15/2011 p. 8.
4.2.4 Special Categories of Data and Data Subjects

Processing of special categories of data listed in Article 9(1) of the GDPR actualises the special conditions in the same Article. Special categories of data are e.g. data that reveal the racial or ethnic origin or political opinions of the data subject, or concern his or her health or sex life. According to Article 22(4), together with Article 9(2) (a) and (g), automated decision making based on special categories of data is prohibited unless the data subject has given his or her explicit consent for the use of such data or unless it is necessary for a substantial public interest.

When processing personal data of children one must take the special obligations in the GDPR on account. E.g., automated decision-making should not be applied to children according to Recital 71 of the GDPR. Profiling that falls outside the scope of Article 22 when applied to adults might fall under the same Article when applied to a child. According to WP 29, organisations should in general refrain from profiling children for commercial purposes.

4.3 Analysis of Chapter 4

The general provision of the GDPR applicable to profiling have been presented in this chapter. The following analysis will discuss the applicability of the GDPR to profiling through ultrasound tracking technology and the challenges that arise when the above described provisions of the GDPR are applied to profiling through ultrasound tracking technology.

4.3.1 Applicability of the GDPR to Profiling and to Ultrasound Tracking Technology

Profiling through ultrasound tracking technology is covered by the general regulations on profiling of the GDPR. In the light of the WP 29 Guidelines on profiling, there is a possibility that the technology could be subject to the stricter regulation of Article 22 of the GDPR.

The WP 29 Guidelines do not clearly reveal when profiling for commercial purposes would be considered as automated decision-making. 'The intrusiveness of the profiling process', e.g., could

238 E.g., Article 8 of the GDPR.
mean many things. Using ultrasound tracking techniques for collecting the profiling data could be such an interference to the private sphere of an individual that the profiling process would be considered to have a significant effect. The ultrasound tracking technology, as stated above, remarkably widens the possibilities to data collection, especially when the technology is combined with other data collection techniques. This view is supported by the fact that terminal equipment, such as a mobile device or a laptop, is recognised as part of the private sphere that needs protection according to Article 8 of the ECHR and Article 7 of the EU Charter.\textsuperscript{241}

The use of ultrasound tracking technology could fall in the material scope of the GDPR even as such, without connection to profiling. The GDPR applies to any processing of personal data according to Article 2(1). Use of tracking technologies and collection of user data often results in this kind of processing because the data collected is classified as personal in the meaning of Article 4(1) of the GDPR. The use of the tracking technology then falls within the scope of the GDPR and has to be in compliance with the provisions of the regulation.

The WP 29 has in its Opinions 1/2008 and 2/2010 clarified that cookies often contain information that is personal data.\textsuperscript{242} When these are used to collect data for profiling purposes they often contain an unique identifier and allow the user to be 'singled out'.\textsuperscript{243} What is more, the information collected for profiling is about a person's characteristics or behaviour and is used to influence that person's behaviour.\textsuperscript{244} The data collected constitutes therefore, in most cases, personal data in the meaning of the GDPR, even without an unique identifier.\textsuperscript{245}

The opinion of the WP 29 could also apply to the use of uBeacons and ultrasound tracking in general since the information collected with these is used similarly to the information collected through cookies. UBeacons and cookies differ only regarding to the technology used. UBeacons, too, contain an unique identifier that can be used to single out an individual user. UBeacons are therefore personal data. As long as an uBeacon can be seen as personal data its use is subject to the GDPR according to Article 2(1).

Both cookies and ultrasound technology can be used anonymously, though. When an uBeacon or a cookie is only used for triggering something on a terminal device or enabling a service, and not for

\textsuperscript{243} WP 29 Opinion 2/2010 p. 9.
\textsuperscript{244} Ibid.
\textsuperscript{245} The WP 29 Opinion 2/2010 discusses the Directive 95/46/EC but the definition of personal data is similar in the GDPR making the WP 29 argumentation here relevant even for the new legislation. See, e.g., Opinion of advocate general Kokott in Case C-434/16 Peter Nowak v Data Protection Commissioner, delivered on 20 July 2017, point 3.
knowing which device or user is in question the provisions of the GDPR do not actualise. This does not, however, mean that the technology would be wholly unregulated. Even uBeacons that are not personal data can be regulated by the ePrivacy Directive and/or the draft ePrivacy Regulation. This possibility is discussed in the next chapter.

4.3.2 The Data Processing Principles, the Rights of the Data Subject and Profiling through Ultrasound Tracking Technology

Regardless of the applicability of Article 22 any kind of profiling must be done in compliance with the data processing principles in Article 5 of the GDPR. The principles can, however, prove to be problematic to implement on profiling through ultrasound tracking technology, since many of the principles are against the idea of profiling, and especially the data collection necessary for creation of profiles, as they are to be done with the technology. Of the data processing principles, transparency in Article 5(1) (a), purpose limitation in Article 5(1) (b), data minimisation in Article 5(1) (c), and storage limitation in Article 5(1) (e) are especially challenging when applied to big data generated by and needed for profiling through ultrasound tracking.

The ultrasound tracking technology enables wide and detailed collection of personal data. Providing concise information about the collection and other processing of the data can be difficult when big amounts of data is collected, some data only to be kept for eventual uses in the future that could be unclear at the time of the data collection.246 Although the principles of purpose limitation and data minimisation do restrict the collection of data through ultrasound technology, it is still possible that the processing and its purposes are hard to explain in such a way that an ordinary user would fully understand what is being done with the data and what risks lay in the processing. Also, reading all the privacy related information provided in all the channels we use is nearly impossible. According to a study, reading all the privacy policies one encounters within a year would take 25 days.247 What is more, no-one really reads the privacy policies.248 This is particularly problematic when it comes to obtaining consent from users. If the principle of transparency is to be realised in practice at the

time of new tracking technologies, such as ultrasound, the ways of providing information must be changed from the existing practice.

Many marketing actors today are tempted to collect as much data as possible for eventual uses in the future. Better and better profiling algorithms are developed all the time and the data that is of little use today can be a fruitful source of information in the future. Both purpose limitation and data minimisation form obstacles in the way of big data collectors and developers. If the data protection principles are followed strictly there is a risk that the growth of the amount of the data will slow down. Whether this is a good thing or not depends on perspective. In the light of the right to privacy and the right to the protection of personal data the data minimisation and purpose limitation are positive things. What is more, when the amount of data available is limited the value of the data is better seen. This could change the way people see to their own and others' personal data and increase the valuation of personal information.

The principle of storage limitation could be difficult to realise when the amounts of data are huge. On the other hand, it should be possible to write algorithms that make this possible and even easy. Another problem is that individual data that is part of the big data forming the base of the profiles does not only affect the individual profile but group profiles, too. Removing the individual data could thus be problematic for the function and precision of the profiling process. The individual has also the right to take his or her data from one processor and transfer it to another (Article 20 of the GDPR). This would mean that the new processor could benefit from something that another processor has created.

One solution is to distinguish the group profile data from the individual data. Recital 26 of the GDPR states that anonymous data, including data that is made anonymous beforehand does not fall under the GDPR provisions. Anonymisation of the data remaining in the use of group profiling could therefore exclude the processing of individual data from the data protection regulation. The data processor could then keep the individual data and the group profiles would remain unaffected. This would not be enough for some, though. As part of the right to information, Hildebrandt and Gutwirth argue for a right to information about the group profiles and to how they are used to steer

250 Hildebrandt Mireille, Gutwirth Serge, Concise Conclusions: Citizens out of Control, in Hildebrandt & Gurtwirth, p. 365 ff.
our lives. According to them, the group profiles affect us all in many different ways, most of which we are unaware of. The knowledge about how profiles are used and what data they are based on is, according to their argumentation, essential if individuals are to have control over the profiles that are applied to them. The principle of storage limitation and the correlating rights of the data subject in Articles 16, 17, 18 and 20 of the GDPR should therefore be taken seriously and be used as a tool to restrict the use of profiling through ultrasound technology.

4.3.3 Privacy by Design and Privacy by Default as Safeguards against the Risks Related to Profiling through Ultrasound

The principle of integrity and confidentiality in Article 5(1) (f) and the principles of privacy by design and privacy by default in Article 25 are especially important when the privacy risks related to profiling and ultrasound tracking technology are to be addressed. Without technological solutions none of the data processing principles described above can be implemented.

Most privacy breaches can be avoided when the privacy and data protection aspects are taken seriously already at the designing stage. Privacy related risks created by technology can best be addressed by the technology itself. The privacy threats associated with the use of ultrasound tracking technology, e.g., are avoidable. Both Mavroudis et. al. and Arp et. al. list possible technological countermeasures to protect the user against the use of ultrasound technology. The first one is filtering out frequencies above 18 kHz in the transmitting device. Arp. et. al. point out that manipulating the hardware or software is not something that a regular user can do, neither is the sender of uBeacons in every case in the user's control. However, Mavroudis et. al. have developed an ultrasound-filtering browser extension. The extension filters out all ultrasound from the websites the user downloads, unless the user opts to allow the ultrasound for a specific website. In this way the user can control the ultrasound tracking done via his or her own browser and prevent unwanted de-anonymisation. The solution is in accordance with the idea of giving the control over personal data to the data subject, but only when it comes to his or her own browser(s). It is not

251 Hildebrandt Mireille, Gutwirth Serge, Concise Conclusions: Citizens out of Control, in Hildebrandt & Gurtwirth, p. 365 ff.
252 See the 'Code is Law' argumentation in Clifford, para 79-80.
254 Arp et. al. p. 22.

49
helpful against other kinds of ultrasound senders, such as TVs and senders used for location tracking.

Another possible way to know when ultrasound is being used would be user notifications on the mobile device and a status in the pull down menu to inform the user when recording takes place, similar to the notifications on the use of WiFi or Bluetooth.\textsuperscript{256} This would be a huge improvement for the current situation where the use of ultrasound often lacks transparency. It would also make the use to comply with the transparency requirements in the GDPR and the ePrivacy Directive. Arp et. al. bring up the permission model of Android 6 which differentiates between normal and dangerous permissions.\textsuperscript{257} The permissions that are classified as dangerous must be granted at runtime. One of these dangerous permissions is the permission of audio recording. As Arp et. al. point out, the user should be doubtful if an application suddenly wants to record audio signals. Mavroudis et. al. suggest separate permissions for listening to audible and inaudible sound.\textsuperscript{258} This would require the applications to explicitly declare if they will capture ultrasound and would make the ultrasound technology as an opt-in feature.

As the case of Android 6 shows, privacy by design, privacy by default, and transparency are possible to achieve in practice. They just have to be taken into account at the design stage. Of course, when developing new systems for profiling, the concepts of privacy by design and privacy by default are restrictive. Many companies today are tempted to collect as much data as possible in order to have good raw material for their future profiling uses of the data.\textsuperscript{259} The idea behind the principles of privacy by design and privacy by default is to put an end to this practice.

\section*{4.3.4 Challenges with Consent and Other Legal Grounds for Processing}

The concept of consent is central when talking about profiling through ultrasound technology, both under the general regulation of the GDPR and under Article 22. A freely given, specific, informed and unambiguous consent from the data subject can open doors for much wider data collection and profiling simultaneously as it gives the data subject a free choice in the matter. On the other hand, obtaining a consent that meets all the requirements can be difficult.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
\textbf{Table 1} & Description of Ultrasound\textsuperscript{260} \\
\hline
Sonar & Using sound waves to create images of internal structures\textsuperscript{261} \\
\hline
Imaging & Using sound waves to create images of external structures\textsuperscript{262} \\
\hline
\end{tabular}
\end{table}

Ultrasound tracking for profiling purposes as a general rule must be based on consent which is in compliance with all the requirements mentioned above. The problem is how the information will reach the user in a way that gives the user a real, informed choice on the matter. In today's hectic flow of privacy notices the information must be very simple, very visible, and very unavoidable in order to be noticed. The service providers will have to assess whether the right to track the individual is worth the nuisance and disturbances when using the service. Another problem is that most electronic services rely on advertising incomes. Only well-tailored marketing enables the services to be free of charge. If applied correctly the strict provisions of the GDPR do provide good protection to personal data of individuals. It is also clear that they will change conditions under which electronic services are provided since the provisions can put practical restrictions on the use of tailored advertisement online limiting the use of tracking and profiling.

Ultrasound tracking of individual users for commercial profiling purposes is in most cases not necessary for the providing of electronic services, despite the fact that most electronic services and applications can provide more individually tailored service if they are based on data about the user. Many service providers could argue that the user is not forced to use their services and thus the condition of consenting to tracking is valid. This view is explicitly rejected in Article 7 of the GDPR and in the opinions of the WP29.260

Processing of personal data for direct marketing purposes can fall within the requirements of a legitimate interest of the data controller in Article 6(1) (f) of the GDPR.261 Regarding profiling outside the scope of Article 22, the question is whether a marketing purpose is always enough to legalise data processing without consent of the data subject. In the light of the WP 29 Guidelines on profiling, there is a great possibility that it would not be the case.262 The data controller's legitimate interest must be balanced against the interest and the fundamental rights and freedoms of the data subject. The comprehensiveness of the profile, i.e. whether the profile only describes a small aspect of the data subject or paints a more comprehensive picture, may indicate that the profiling cannot be legitimised under Article 6(1) (f).263 Profiling through ultrasound tracking technology is, as stated many times before, very privacy intrusive. It is possible to create very comprehensive profiles based on the technology. Data processing in the form of profiling through ultrasound tracking technology can therefore not be based on the data controller's legitimate interest.

### 4.3.5 Problems with Distinctions between Different Categories of Data and Data Subjects

In the context of big data and profiling the distinction between sensitive and other data in Article 9 of the GDPR is problematic. Profiles created by using big data can be very accurate. When one has enough data it is possible to make quite precise deductions about a person's life and behaviour. Data that seems harmless at the time of the collection can in fact hold information about one's personal life, including health conditions, ethnic origin and political opinions. A good example is how Target in the U.S. learned to predict when its customers were expecting a child by analysing their shopping data. Making a difference between 'normal' and sensitive data is practically meaningless when all data is potentially sensitive data. Data collected through ultrasound tracking technology could seem harmless at the time of collection, but when data collected through longer time period is combined in a profiling process the information can become very sensitive. It can be argued that the safeguards to processing of sensitive data in Article 9 of the GDPR can be applicable to almost any data collected through ultrasound tracking technology and used for profiling.

Preventing the use of children's data can be difficult in practice when basically every child today is connected to the Internet and uses mobile devices. To make a difference between adults' data and children's data one must first define the users' ages, which is against the principle of data minimisation. In many cases distinguishing children's data from other data could be very difficult. E.g., many social media services today have age limits, but there is no way to prevent a minor to write a wrong year of birth in the registration form. Preventing children from using applications that use ultrasound tracking technology could also be very challenging. Another question is children's data that is used to make adult profiles more accurate. In the diaper advertisement example in chapter 2, the marketer must know the age of the children of the user in order to target the diaper advertisement correctly. In this example personal data of children in form of their ages is used to generate better profiles of adults. When an adult is tracked and profiled through ultrasound tracking technology there is a great risk that data about his or her children is collected too. Best way to protect children's personal data is to make companies refrain from profiling beyond the defining of the user's age and to make them have policies of not creating campaigns using children's data or

---


targeted to children. This is done in the GDPR through special provisions about children’s data, such as Article 8 on children's consent. Should a data processor fail to comply with these provisions, an administrative fine can be imposed according to Article 83(4) and (5). As soon as a marketing actor comes across data that could origin from a child the protective actions should be triggered. Another way to protect children from profiling would be restrictions on their terminal devices, in form of browser and other privacy settings done by adults.
5 Regulating Tracking Technologies in the European Union: the ePrivacy Directive and the Draft ePrivacy Regulation

The use of tracking technologies is a pre-condition for profiling. Without the big data collected through these technologies there would not be adequate data for creation of usable profiles. In principle, the regulation on profiling covers also the use of tracking technologies, but regarding some technologies special legislation is considered to be necessary. The GDPR sets general principles for processing of personal data. The confidentiality of communications and the use of traffic data, location data, and cookies are regulated in the ePrivacy Directive.\textsuperscript{266} The ePrivacy Directive is \textit{lex specialis} to the GDPR, which means that the provisions of the GDPR apply whenever the ePrivacy Directive is silent.\textsuperscript{267}

An interesting rule in the ePrivacy Directive is Article 9 on location data other than traffic data. Article 9 covers the use of wifi-tracking and can be argued to be applicable to location tracking through ultrasound technology as well. Another rule of interest in the context of ultrasound tracking technology is the so called cookie-rule in Article 5(3) of the ePrivacy Directive. Both Articles will be described in this chapter in general terms before applying them to ultrasound tracking technology.

Reform of the ePrivacy Directive is part of the same reform of the European privacy and data protection framework as the GDPR. Recital 173 of the GDPR states that the ePrivacy Directive is to be reformed to comply better with the GDPR. Proposal to a new ePrivacy Regulation (the draft ePrivacy Regulation) came in January 2017. The European Parliament decided about its proposal for amendments on the proposal in October 2017 (the Proposal of the Parliament).\textsuperscript{268} The new regulation was originally intended to come in force on the 25 May 2018 together with the GDPR, but it will likely miss this date.\textsuperscript{269} Before the new Regulation is in force the references to the repealed Data Protection Directive in the ePrivacy Directive will be construed as referring to the

\begin{footnotes}
\item[266] Article 5(1) of the ePrivacy Directive.
\item[267] Recital 10 and Article 1(2) of the ePrivacy Directive and Recital 173 of the GDPR.
\end{footnotes}
corresponding provisions in the GDPR.\textsuperscript{270} In this chapter the main focus will be on the ePrivacy Directive. The proposed amendments will be notified when they are relevant for the topic.

5.1 Applicability to Tracking Technologies

According to Article 3(1) of the ePrivacy Directive the directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the EU. According to Article 2(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. 'Electronic communication services' refers mainly to telecoms companies and the Internet. Broadcasting services are not included, provided that the subscriber or user cannot be identified.\textsuperscript{271}

Both the content of the communication and the data around it, i.e. traffic data, are protected in the ePrivacy Directive.\textsuperscript{272} Protection of the content of communications is quite easy to understand as part of the right to protection of private and family life, which includes the protection of correspondence.\textsuperscript{273} Traffic data is information about, e.g., who are communicating with each other, and when and where the communication takes place.\textsuperscript{274} This data is often collected and used by the provider of the communication access in order to charge for the use of the phone or Internet connection. The data can also be used for profiling since it can reveal a good deal of information about the communications of an individual.

The ePrivacy Directive applies to tracking technologies as far as the technologies are part of public electronic communications services. There needs to be some sort of communication in which the technologies take part. Cookies are one clear example of such technologies as well as user accounts and collection of location data generated in electronic communications services. In the draft ePrivacy Regulation even more clear regulation on the protection of terminal equipment of the user is proposed. Article 2(1) of the draft ePrivacy Regulation states that information related to the terminal equipment of end-users is within the material scope of the draft ePrivacy Regulation.\textsuperscript{275} This would mean that information would be protected solely because it relates to terminal

\textsuperscript{270} Article 94(2) of the GDPR.
\textsuperscript{271} Article 2 (d) and Recital 16 of the ePrivacy Directive.
\textsuperscript{272} Recital 21 of the ePrivacy Directive.
\textsuperscript{273} Article 1(1) and Recitals 2 and 3 of the ePrivacy Directive remind us about these rights.
\textsuperscript{274} Article 2(b) and Recital 15 of the ePrivacy Directive.
\textsuperscript{275} See also Article 8 and Recitals 20 and 25 of the draft ePrivacy Regulation.
equipment of a user. No further distinction as to what information is in question would be needed, in contrast to the GDPR which makes the distinction between personal data and other data. \(^{276}\) It would also mean that the information protected by the draft ePrivacy Regulation would not have to be part of communication, as is required by Article 3(1) of the ePrivacy Directive.

5.2 Substantive Regulations Applicable to Tracking Technologies

Recital 26 of the ePrivacy Directive reminds us that the data processed within the electronic communications networks often contain information on the private life of natural persons, which must be protected. Any use of the data that goes further than what is necessary for the purpose of billing and interconnection payments is only allowed if the user has agreed to it after given full information about the processing and its purposes. Data should also be erased or made anonymous after it is no longer needed for the provision of the service it is collected for.

The confidentiality of the communications, including both the contents and any data related to such communications, must be secured and measures be taken to prevent unauthorised access to the communications according to Recital 21 of the ePrivacy Directive. Article 5, which includes the cookie-rule, addresses these issues. In the draft ePrivacy Regulation Articles 5 and 6 more precise regulation on the confidentiality of the communications is proposed. In Recital 15 of the draft ePrivacy Regulation, surveillance and monitoring browsing habits for profiling purposes without explicit consent of the user are particularly mentioned as ways of interference that must be prevented. \(^{277}\) Article 10 of the draft ePrivacy Regulation includes obligations of ensuring security, privacy by design, and privacy by default.

The ePrivacy Directive incorporates the principles of data minimization and privacy by design. According to Recital 30: '[s]ystems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'. Any services going beyond the strict minimum are considered as 'value added services' for which consent of the user is required.

\(^{276}\) Article 2(1) together with Article 4(1) of the GDPR.
\(^{277}\) Note that Article 6 of the draft ePrivacy Regulation is one of those that divide opinions among the legislators, see the Proposal of the Parliament and the Consolidated version from December 2017.
Consent is a central term even in the ePrivacy Directive. According to the Article 2(f) of the ePrivacy Directive the definition of consent should be the same as in the Data Protection Directive, which is being replaced by the GDPR. In the draft ePrivacy Regulation consent is connected to the definition in the GDPR.\textsuperscript{278} Under both the ePrivacy Directive and the draft ePrivacy Regulation consent of the user is only considered valid if the user has been given adequate information about what he or she is consenting to and is given an opportunity to refuse the use of his or her data for the purposes in question. According to the WP 29 an opt-in consent is more suitable than an opt-out consent.\textsuperscript{279} This view reigns also in the GDPR and in the draft ePrivacy Regulation.\textsuperscript{280}

A great difference between the ePrivacy Directive and the draft ePrivacy Regulation is the regulation on sanctions related to breaches of the regulations. The ePrivacy Directive lacks such sanctions whereas the draft ePrivacy Regulation includes regulation on administrative fines, among others, planned to be as high as in the GDPR, which is up to 20 000 000 EUR or 4\% of the worldwide annual turnover according to Article 23 of the draft ePrivacy Regulation.

### 5.2.1 Wifi-Tracking and Other Location Tracking

Requirements for consent of the data subject are especially interesting in the context of wifi-tracking. According to Article 9(1) of the ePrivacy Directive: 'where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.' Location data is defined in Recital 14 of the ePrivacy Directive: 'Location data may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.' Wifi-tracking technology helps to collect information about locations and movements of mobile devices and is thus regulated in Article 9 of the ePrivacy Directive.

\textsuperscript{278} Article 9 and Recital 18 ff. in the draft ePrivacy Regulation.  
\textsuperscript{279} WP 29 Opinion 2/2010 pp. 16-17. Opt-in consent refers to a situation when the data processing is only began after, and if, the user has consented to it. Opt-out consent describes a situation where the consent of the user is presumed and the user has to act to show that he/she does not consent.  
\textsuperscript{280} WP 29 Guidelines on consent pp. 17 and 21.
Article 9(1) states that location tracking can only be performed if the data is made anonymous or if the data subject has given informed consent to the tracking. It is notable that the data subject must have a possibility to withdraw his or her consent 'at any time'. According to Article 9(2) the data subject must have the possibility to temporarily refuse the tracking. This has also been emphasised by the WP 29, according to which the user must be 'kept informed, not only when they subscribe to a service but also when they use it ... the service provider should regularly remind the individual concerned that his or her terminal equipment has been, will be or can be located.'

Article 9(3) requires also that the location tracking is limited to the 'persons acting under the authority of the provider of ... the value added service'. The tracking must also be restricted to what is necessary for the purpose of the service. Wifi-tracking is also regulated in Article 8(2) of the draft ePrivacy Regulation: 'The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except on following grounds...' According to Recital 25 of the draft ePrivacy Directive, the user should be informed about the use of wifi-tracking technology before they enter an area where the technology is in use.

5.2.2 Article 5(3) of the ePrivacy Directive and Cookies

Another rule that clearly regulates use of tracking technologies is Article 5(3) on cookies. Article 5(3) of the ePrivacy Directive forbids the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a user unless the user is informed about the processing and its purposes and is offered the right to refuse such processing. Providing information and getting the user's consent are not required when the processing is done for the sole purpose of carrying out the transmission of a communication or when it is strictly necessary in order to provide an information society service explicitly requested by the user. This rather technically written rule is meant to prevent the use of third party cookies. Article 5(3) has, however, been interpreted to cover even other technologies, such as device fingerprinting. The implementation of Article 5(3) has proven to be rather impractical, with all the pop-up-banners on websites, which is the reason for its reform being one of the most important part of the reform of the whole ePrivacy Directive.

The terminal equipment of users and the information stored therein are part of the private sphere of the users which is protected under the ECHR and other human rights instruments. Article 5(3) of the ePrivacy Directive refers to 'information' and not to 'personal data' as the GDPR does. The WP 29 has clarified in its Opinion 2/2010 that, in contrast to other privacy and data protection rules, it is the private sphere of the data subject that triggers the use of Article 5(3) and not the information being personal data. This means that Article 5(3) of the ePrivacy Directive provides for wider protection than what is generated by the GDPR.

Not all cookies require consent of the user: the ones that are technically necessary are excepted. The idea is that the use of cookies for legitimate purposes should not be burdened with unnecessary regulation. One of the main purposes of Article 5(3) of the ePrivacy Directive is to make users aware of the use of cookies and of the possibility of collection of their personal data through them. The offering of information is therefore a central requirement. It is also intention that users could have the possibility to have control over the collection of their personal data, hence the requirement to offer the chance of refusal. Under the ePrivacy Directive access to a website can be made conditional upon acceptance of a cookie, if it is used for a legitimate purpose. The consent under the GDPR does not allow access to a service be made conditional of consenting to personal data processing unless the processing is strictly necessary for the providing of the service. In the GDPR, the emphasis is shifted from the rights of the service provider to the rights of the user, which shows the legislator's will to give the user more control over the data.

The request in Recital 25 of the ePrivacy Directive of making all this to be 'as user-friendly as possible' has proven to be hard to realise. In the draft ePrivacy Regulation the information and obtaining of consent to cookies is planned to be done via browser settings on the user's device. The meaning is to get rid of the cookie-banners and to transfer the responsibility more from single website owners to the browser providers. The material scope of the rule is also widened to cover even other collection of information from the terminal equipment, 'including about its software and hardware' according to Article 8(1) of the draft ePrivacy Regulation.

284 Recital 24 of the ePrivacy Directive reminds about this.
285 See also Recital 24 and Clifford para 27.
287 Recital 25 of the ePrivacy Directive.
288 Recital 25 of the ePrivacy Directive.
289 Article 7(4) of the GDPR.
291 See the explanatory memorandum of the draft ePrivacy Regulation under 3.4 Impact assessment.
292 Ibid.
5.3 Analysis of Chapter 5

The general provisions of the ePrivacy Directive applicable to ultrasound tracking technology and the relevant changes that are suggested in the draft ePrivacy Regulation have been presented in this chapter. The following analysis will discuss the applicability of the ePrivacy Directive and the draft ePrivacy Regulation to ultrasound tracking technology. Applicability of Articles 5(3) and 9 of the ePrivacy Directive and the corresponding Articles in the draft ePrivacy Regulation are particularly discussed.

5.3.1 General Applicability of the ePrivacy Directive and the Draft ePrivacy Regulation to Ultrasound Tracking Technology

According to Articles 3(1) and 2(d) of the ePrivacy Directive only data processing that is part of electronic communication is protected. Part of the ultrasound tracking technology is transmission of information between the user's device and other devices that are all in public communications networks. Ultrasound tracking technology is thus principally within the material scope of the ePrivacy Directive. However, apart from the general provision on the material scope of the ePrivacy Directive, the ePrivacy Directive does not have any particular provision that would directly cover the technology. Of the tracking technologies that resemble ultrasound tracking technology cookies and wifi-tracking are directly addressed in the ePrivacy Directive. Whether ultrasound tracking technology is covered by the same provisions as these two technologies is discussed below.

The ultrasound technology is, in its essence, communication via the user's device and about the user's device. The threats related to the ultrasound technology lie rather in the possibility to trace and track the user via his or her device than in the possibility to spy on the communication that goes via the device. Ultrasound technology is used mainly for invading the private sphere of life of the user and not for violating the confidentiality of his or her communications. The legislation would be far easier to apply to ultrasound tracking technology if the object of the legislation was the terminal device itself and not the technology used for transmitting the information. Terminal equipment of the user is not covered by the wording of Article 3(1) of the ePrivacy Directive. Article 2(1) of the draft ePrivacy Regulation, that explicitly mentions terminal equipment of the user, would more clearly cover the use of ultrasound tracking technology.\textsuperscript{293}

\textsuperscript{293} See also Recital 20 of the draft ePrivacy Regulation.
5.3.2 Location Tracking through Ultrasound Technology

Ultrasound tracking technology is used for location based services. Examples are Lisnr and Shopkick applications which use the technology to provide messages triggered by physical location of the user's device. The location data generated by the technology is such that is described in Recital 14 of the ePrivacy Directive, namely data that refers to 'the latitude, longitude and altitude of the user's terminal equipment'. Location tracking generated via ultrasound technology is therefore covered by Article 9 of the ePrivacy Directive. When such tracking is performed, the user must be informed about it both before and under the tracking. The consent of the user for the tracking is always needed and the user must have the change to withdraw his or her consent at any time in accordance with Article 9(2) of the ePrivacy Directive.

Article 8(2) of the draft ePrivacy Regulation requires 'collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment'. The ultrasound tracking technology does not use information that is needed to enable connection between terminal equipment and another device/network equipment. Ultrasonic senders generate the location data directly. There is no need to collect information about several ultrasonic senders to know the location of the user, even though such information may give a more wholesome picture about the movements of the user. Therefore, the wording of Article 8(2) of the draft ePrivacy Regulation does not cover the use of ultrasound tracking technology. This leads to an interesting situation where Article 9 of the ePrivacy Directive is more technology neutral than Article 8(2) of the draft ePrivacy Regulation, even though the meaning has been the opposite. It is not said, though, that the draft ePrivacy Regulation would not cover ultrasound tracking technology at all. Whether Article 8(1) of the draft ePrivacy Regulation covers ultrasound tracking technology is discussed next together with the applicability of Article 5(3) of the ePrivacy Directive.

5.3.3 Article 5(3) of the ePrivacy Directive and uBeacons

Article 5(3) does not apply only to cookies but to similar technologies as well. The question arises what these similar technologies are. Could the sending and receiving of uBeacons on a mobile device be such similar technology? It is information in the private sphere that the Article 5(3) is protecting, not the right to get information about cookies and to be able to refuse them.

294 See chapter 2 for a more detailed description of Lisnr and Shopkick.
295 See Recital 25 which speaks about cookies and 'similar devices'.
The WP 29 has interpreted the cookie-rule so that it covers also the use of device fingerprinting despite the fact that device fingerprinting does not include sending and receiving information from the user's terminal equipment.\textsuperscript{296} According to WP 29: 'any processing which the third-party takes which influences the behaviour of [the] device or otherwise cause it to store or give access to information on that device, or exposed by that device is within the scope of Article 5(3).'\textsuperscript{297} The WP 29 interprets the use of words 'stored or accessed' in Article 5(3) so that the storage and access do not need to occur within the same communication. The storage and access do not even need to be done by the same party. Nor do the storage and access elements need to be included in every aspect of the technique.

When an ultrasound sender sends an uBeacon and a user's device 'hears' it the uBeacon triggers something on the user's device, i.e., 'influences the behaviour of that device'. When performing ultrasound tracking there are at least three different devices, compared to the two devices in cookie-tracking, which are communicating: the sender, the user's device and the server to which the information created in the communication between the sender and the user's device is sent. There can thus be two different actors triggering the communication of the information via the user's device: the sender that triggers the reading of the information and the server that acts as an ultimate collector of the information. In the light of the WP 29 opinion the use of ultrasound tracking would be covered by Article 5(3) of the ePrivacy Directive even though the storage and access do not occur within the same communication and not even necessarily between the same parties.

The WP 29 refers to its Opinion 04/2012 which emphasises that third-party advertising does not fall under the exemption in Article 5(3).\textsuperscript{298} If the purpose of the processing is targeted advertising the processing is lawful only if the user has consented to it. Ultrasound technology can be used for other than marketing purposes as well, such as identifying functions.\textsuperscript{299} Such use does not require the consent of the user since the providing of the service requested by the user is dependent on the data processing in question. The identifying function would not work without the data processing. However, using ultrasound tracking to collect information about the user and his or her device for profiling purposes should clearly fall outside of the exemption. The user must be provided with adequate information and given the possibility to refuse the processing at any time.

\textsuperscript{296} WP 29 Opinion 9/2014.  
\textsuperscript{297} Ibid. p. 8.  
\textsuperscript{298} Ibid. p. 9.  
\textsuperscript{299} See about how Google uses ultrasound to connect the user's mobile device to Google Chromecast in Mavroudis et. al. pp. 95-96.
In the draft ePrivacy Regulation the cookie-rule is widened to be more technology neutral.\textsuperscript{300} Recital 20 of the draft ePrivacy Regulation names explicitly device fingerprinting as one of the threats to privacy. Also other technologies are mentioned: ‘[t]echniques that surreptitiously monitor the actions of end-users, e.g. by tracking their activities online or the location of their terminal equipment [...] should be allowed only with the end-user’s consent and for specific and transparent purposes.’\textsuperscript{301} Recital 25 of the draft ePrivacy Regulation emphasises the information obligations in the context of wifi-tracking. It should be noted that the protection of terminal equipment is emphasised even more in the Proposal of the Parliament.\textsuperscript{301} By using ultrasound technology the user of a mobile device can be monitored without the user's knowledge of the monitoring. Tracking performed with uBeacons is a more intrusive technique than the sole use of, e.g., third party cookies or device fingerprinting. It follows from the wording of Recital 20 of the draft ePrivacy Regulation that tracking methods like ultrasound technology should only be allowed with the user's informed consent. In the light of Recital 20 of the draft ePrivacy Regulation, the ultrasound based tracking would be more directly covered by the draft ePrivacy Regulation than by the ePrivacy Directive. However, the wording of Article 8 of the draft ePrivacy Regulation does not address the ultrasound technology as clearly as Recital 20 of the draft ePrivacy Regulation would suggest. It still seems that ultrasound would be covered by the scope of Article 8 of the draft ePrivacy Regulation. Ultrasound technology uses a device's 'processing and storage capabilities' when an uBeacon is sent on the device and read therein. Collection of information from the device is performed when the information triggered by the uBeacon is sent on to a server. The question is whether the word 'and' between these two actions means that the processing and collection do not have to be done within the same communication and/or by the same actor. Such interpretation is supported by the WP 29 interpretation of Article 5(3) of the ePrivacy Directive. It should be noted, though, that the WP 29 interpretation of the applicability of Article 5(3) to device fingerprinting has not have significant practical effect. This is reflected by the draft ePrivacy Regulation's emphasise on the matter. The wording of Recital 20 of the draft ePrivacy Regulation suggests that the WP 29 interpretation would apply even to Article 8(1) of the draft ePrivacy Regulation.

\textsuperscript{300} Article 8 of the draft ePrivacy Regulation. See also the explanatory memorandum of the draft ePrivacy Directive.  
\textsuperscript{301} Amendments 84-92 and the explanatory statement of the Proposal of the Parliament under Protection of information stored in and related to users’ terminal equipment.
6 Conclusions

The right to private and family life and the right to the protection of personal data are fundamental rights codified in several human rights instruments and in the EU primary law. The GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation all aim to protect these two rights and the private sphere of life of individuals. Profiling and tracking intrude into the protected private sphere.

All the applications of profiling through ultrasound technology can be used for both good and evil. On the one hand, user experience, identification, and authorisation can become better and easier. On the other hand, personal information of a user can be easily collected, even without the user's knowledge, and used in ways that cannot be foreseen by the user. Profiling and tracking via ultrasound technology invade the private sphere in a more intrusive way than what the 'traditional' tracking technologies, such as cookies, user accounts, device fingerprinting, and location tracking, do. Prohibiting ultrasound tracking technology as such would be disproportionate because it does have many legitimate applications as well. At the same time the privacy risks of the technology must be addressed and minimised. It is essential for the implementation of the right to private and family life and the right to the protection of personal data that the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation cover profiling through ultrasound tracking technology. In this chapter the function of these three laws as safeguards against the privacy risks generated by profiling through ultrasound tracking technology is discussed.

6.1 Technology Neutrality of the GDPR, the ePrivacy Directive and the Draft ePrivacy Regulation

The GDPR, the ePrivacy Directive and the draft ePrivacy Regulation all aim to be technology neutral.302 When implemented correctly, technology neutrality can mean full penetration of the right to privacy and the right to data protection. Should the three laws fail in their aim to technology neutrality, the threats carried with ultrasound tracking technology would not be addressed by them. The technology neutrality of these laws is tested in the above discussion about their applicability to

302 Recital 15 of teh GDPR, Recital 4 of the ePrivacy Directive, and the explanatory memorandum of the draft ePrivacy Regulation under 3.5 Regulatory fitness and simplification.
profiling through ultrasound tracking technology. Here the technology neutrality of the GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation is more deeply analysed.

Profiling through ultrasound tracking technology is regulated both through regulations on profiling and through regulations on the use of the ultrasound tracking technology. The GDPR regulates both, whereas the ePrivacy Directive and the draft ePrivacy Regulation only focus on the tracking technology.

The GDPR regulates two kinds of profiling. All kind of profiling of identified or identifiable natural persons is within the general provision of the GDPR. Profiling via ultrasound tracking technology is thus also affected by the general regulations of the GDPR. Special rules on profiling are found in Article 22 of the GDPR, which regulates profiling in the context of individual decision-making. The WP 29 makes in its Guidelines on profiling an interpretation that even profiling for commercial purposes can fall under Article 22 when the profiling is particularly intrusive. Whether the use of ultrasound technology in the profiling process triggers the stricter rules of Article 22 is unclear, but in the light of the WP 29 Guidelines on profiling this could be the case. Clearer directives on when profiling for commercial purposes falls under Article 22 are needed.

Ultrasound tracking technology is based on sending and receiving of uBeacons which function as unique identifiers. Such identifier can be seen as personal information in the meaning of Article 4(1) of the GDPR. The use of uBeacons falls under the regulation of the GDPR when an uBeacon can be seen as personal information. Therefore the use of ultrasound tracking technology is in most cases within the material scope of the GDPR according to Article 2(1).

The ultrasound tracking technology shares some characteristics with cookies, device fingerprinting and wifi-tracking. Cookies, device fingerprinting and uBeacons are all covered by Article 5(3) of the ePrivacy Directive. Article 5(3) of the ePrivacy Directive is triggered as soon as there is communication between the user's terminal equipment and other devices and when the terminal equipment of the user is being influenced. Article 8(1) of the draft ePrivacy Regulation is to replace Article 5(3) of the ePrivacy Directive. In the light of Recital 20 of the draft ePrivacy Regulation, it is highly probable that Article 8(1) of the draft ePrivacy Regulation covers also the use of ultrasound technology. The protection under Article 5(3) of the ePrivacy Directive and Article 8(1) of the draft ePrivacy Regulation is focused on the terminal equipment of the user and not on the personal data of the user on the terminal equipment.
Location tracking via ultrasound is very similar to wifi-tracking and other location tracking. The ePrivacy Directive ruling in Article 9 on location data other than traffic data applies to ultrasound tracking as well, simply because of the tracking being location tracking. What is notable is that Article 8(2) of the draft ePrivacy Regulation does not cover the use of ultrasound tracking technology. It is focused on the use of wifi-tracking. In this aspect Article 9 of the ePrivacy Directive is more technology neutral than Article 8(2) of the draft ePrivacy Regulation.

The regulation on profiling in the GDPR covers the use of ultrasound based profiling. The regulation focuses on the data processing as such and not on the choice of technology, which makes it convincingly technology neutral. The ePrivacy Directive regulates the processing of personal data in the context of electronic communication services and is thus more technology-specific. The provisions in Articles 5(3) and 9 are, however, written in sufficiently neutral language allowing the ruling to stretch in a way that also covers the use of uBeacons and ultrasound based location tracking, respectively. In the draft ePrivacy Regulation the focus is moved more to the protection of the terminal equipment of the user, which provides for an even more clear applicability to ultrasound tracking technology. Even though Article 8(2) of the draft ePrivacy Regulation does not cover the ultrasound based location tracking, Article 8(1) covers the use of ultrasound tracking in general. The GDPR, the ePrivacy Directive and the draft ePrivacy Regulation thus all reach the goal of technology neutrality.

6.2 Safeguards to the Right to Privacy and the Right to Data Protection

The data processing principles in Article 5 of the GDPR and the distinction between sensitive and other data in Article 9 of the GDPR are challenging to apply to profiling through ultrasound technology. Transparency in Article 5(1) (a), purpose limitation in Article 5(1) (b), data minimisation in Article 5(1) (c), and storage limitation in Article 5(1) (e) are especially challenging when applied to big data generated by and needed for profiling. Accurate profiles can only be made with comprehensive data. In many cases the data is collected first and utilisations for the data are found afterwards while analysing and investigating the data. Defining purposes of the data collection and being transparent about these purposes can therefore be very difficult. Data minimisation and storage limitation limit the possibilities of utilisation of the data. From privacy
and data protection point of view this is a good thing, but some marketing actors might think otherwise. Distinguishing sensitive personal data from other personal data can also be difficult due to the fact that most uses of the data are found after the data is collected. Any data can potentially reveal sensitive information about individuals when combined with other data. The data controllers are also required to distinct and protect children's data. Exactly how this can be done without jeopardising the data processing principles is still a question mark.

Consent of the data subject is mentioned as a legal ground for data processing both under Article 6 and Article 22 of the GDPR. It is also important in the context of Articles 5(3) and 9 of the ePrivacy Directive and Article 8 of the draft ePrivacy Regulation. Since profiling for commercial purposes seldom fills the requirements for other legal grounds (even though it is possible that the requirements are met in an individual case) it is the consent of the data subject that makes the data collection and profiling legal. Consent must be freely given, specific, informed, and unambiguous, conditions which can be hard to meet. Ensuring that the data subject is fully aware of what he or she is consenting to, and even if he or she is consenting to something at all, can be very difficult when the data subject can encounter consent requests several times a day.

The principle of integrity and confidentiality in Article 5(1) (f) and the principles of privacy by design and privacy by default in Article 25 are especially important when the privacy risks related to profiling and tracking technologies are to be addressed. These principles are also found in the draft ePrivacy Regulation Article 10. Without technological solutions none of the data processing principles can be implemented. The challenges connected to obtaining appropriate consent from the user can also be solved with good and careful design and privacy focused way of thinking.

Even though there are many challenges for the implementation of the data processing principles and the consent requirements, the principles as such do provide for good safeguards to the right to private and family life and to the right to the protection of personal data in the context of profiling through ultrasound tracking technology. The GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation set boundaries for the use of tracking and profiling and thus limit the use of the technologies. The practical implementation of the legislation must be done carefully in order to secure full penetration of the fundamental rights of the individual.
6.3 Summary

The applicability of the GDPR and the ePrivacy Directive together with the draft ePrivacy Regulation to the technology of profiling by means of ultrasound tracking technology is determined in chapters 4 and 5 of this thesis. The extent to which these legal instruments provide safeguards for the right to privacy and the right to data protection is also evaluated. According to the findings, profiling through ultrasound tracking technology is within the material scope of the GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation.

The research question 1 ("What is ultrasound tracking technology, how does it relate to profiling and in what manner does it differ from other tracking technologies?") is addressed in chapter 2, where the process of profiling is described in general terms. It is also shown how tracking technologies in general and ultrasound tracking technology in particular have a central role in the profiling process. Without the data collection made possible by these technologies there would not be sufficient data for the creation of profiles. Differences and similarities between ultrasound tracking technology and other tracking technologies are described. It is found that ultrasound tracking technology enables far wider tracking and data collection than the other tracking technologies.

Question 2 ("To what extent are profiling and tracking technologies regulated in the EU?") is addressed in chapters 3, 4 and 5, where the right to privacy and the right to data protection and their implementation in the EU secondary law are described. Two kinds of regulation on profiling in the GDPR are described: profiling under Article 22, and profiling outside the scope of Article 22. Regulation on tracking technologies in the GDPR, the ePrivacy Directive and the draft ePrivacy Regulation is discussed in detail.

Question 3 ("Is the EU regulation on profiling and tracking technologies technology neutral to the extent that ultrasound tracking is regulated by these legal instruments?") is addressed mainly in chapter 6, but also throughout the chapters 3-5. According to the findings, the three legal instruments, the GDPR, the ePrivacy Directive, and the draft ePrivacy Regulation, all live up to their aim of technology neutrality. An exemption is Article 8(2) of the draft ePrivacy Regulation which, unlike Article 9 of the ePrivacy Directive, does not stretch to cover location tracking through ultrasound technology.
Primary Law:

International Instruments:

The International Covenant on Civil and Political Rights (ICCPR).

EU Instruments:

The Treaty of the Functioning of the European Union (TFEU).
The Charter of Fundamental Rights of the European Union, 2000/C 364/01 (the EU Charter).

Secondary Law:

Regulations:


Directives:


Preparatory Papers:


Article 29 Data Protection Working Party:


**Other Recommendation Papers:**


**Non-EU Law:**

**United States:**


**Case Law:**


Judgement of the Court of Justice, 28 October 1975, Case 36/75, Rutili, REG 1975, p. 1219 ff.


Opinion of advocate general Kokott in Case C-434/16 Peter Nowak v Data Protection Commissioner, delivered on 20 July 2017.

**Literature:**


Hildebrandt Mireille, Gutwirth Serge (eds.), *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, 2008 (Hildebrandt & Gutwirth).


71


**Journals:**


Clifford Damian, *EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour*, JIPITEC 2014, issue 5, p. 194 ff. (Clifford).

Fayyad Usama, Piatetsky-Shapiro Gregory, Smyth Padhraic, *From Data Mining to Knowledge Discovery in Databases*, AI Magazine, Volume 17, Number 3, 1996, p. 37 (Fayyad et. al.).


Young Hunter, *Ultrasonic Data Transmission and Steganography*, Honors College Capstones and Theses 6, 2016 (Young).

**Articles:**


Pettit Harry, *Facebook can track who you know using the DUST on your camera: Creepy patent reveals how the site can connect people by studying smudges in photos to see if they were taken by the same lens*, Daily Mail, published 12 January 2018, http://www.dailymail.co.uk/sciencetech/article-5262297/Facebook-track-using-dust-camera-lens.html, last accessed 1 February 2018.


**Websites:**


