Masters Thesis

Data Protection and Behavioural Analysis in Social Media

By: Ayana Datta
Supervisor(Hannover): Prof.em. Dr. Dr. h.c. Wolfgang Kilian
Supervisor(Oslo): Dr Lee.A. Bygrave

Submission Date: 15.05.2018
Words of thanks and gratitude

This entire journey of researching and writing would not have been possible without the kind guidance of Prof. em. Dr. Dr. h.c. Wolfgang Kilian of Leibniz University Hannover and Dr Lee. A. Bygrave of the University of Oslo.

A special thanks to the Library faculties of both the University of Oslo and Leibniz University Hannover for allowing me to do the research and making their resources available at all time.
Table of contents

1. Generation of Personal Data in Social Media… ..........................4
   1.1. Internet of Things… .........................................................6
   1.2. Big Data… ......................................................................8
2. Data Providers’ Usage of the Personal Data of the users… ..............10
3. Personal Data and Behavioural Data… .......................................15
4. Prediction and Push Advertisement in Social Media…………………21
5. The concept of consent in Big Data Analysis and Behavioural
   Targeting… ...........................................................................28
6. Purpose Limitation and Breach of Trust …..................................39
7. Conclusion… ...........................................................................42
Introduction

In this digitised world data may well be recognised as the currency of the cyberworld. Of those data, personal data is regarded as the sensitive of all data, thereby requiring protection. The concept of Data Protection is not something that has started in the last few years. It dates back at least 25 years in terms directives and regulations.

The EU's data protection laws have long been regarded as a gold standard all over the world. Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed. In 2016, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years. It replaces the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy. The GDPR is now recognised as law across the EU. Member States have two years to ensure that it is fully implementable in their countries by May 2018.¹

The legal history of Data Protection starts on 24/10/1995 with the adoption of The European Data Protection Directive (Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is adopted.²

The Directive was adopted when the modern day complexities and problems of internet were not known. For this very reason, when the European Data Protection Supervisor published an opinion on the European Commission 'A comprehensive approach on personal data protection in EU' on 22.06.2011, the wheels for a major change and revision of the provisions of the existing Directive started rolling. By 2012, EU Commission had already proposed a comprehensive reform of the rules of the Directive 95/46/EC to strengthen online privacy rights and digital economy within the territory of the European Union.

The same year, The Article 29 Working Party adopts an opinion on the data protection reform proposal and provides further input on the data protection reform discussions.³ The resulting discussions went for about for two years when finally European Parliament showed strong

support for the current GDPR with a huge 621 votes in plenary.\textsuperscript{4} By July, 2015, the European Data Protection Supervisor had published his final recommendations on the text of the GDPR.\textsuperscript{5}

By the beginning of May, 2018 the GDPR will be in force, thereby repealing the Data Protection Directive of 1995.

With these new changes, the value of personal data are even higher than before. My thesis here is trying to find out if Data Collection and Compilation is absolutely necessary and if it can be avoided for the processing for targeted behavior analysis and thereby creating push advertisement in social media, where most of the Data subjects spend most of their ‘online’ time.

1. Generation of Personal Data in Social Media

Personal Data can be regarded as the foundation stones when it come to the implementation of either Directive or regulation. It is regarded as one of the fundamental human rights in accordance to Art. 8 of the European Convention of Human Rights (ECHR), where it is clearly stated that:

‘Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’\textsuperscript{6}

The word, Personal Data, itself refers to any kind of data that pertains to our personal life information. According to the Data Protection Directive, Art 2(a) and the Council of Europe Convention 108, Art. 2(a) ‘Personal data’ are defined as information relating to an identified or identifiable natural person, that is, information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information.\textsuperscript{7}

The basis of using Social Media is by creating accounts on specific websites. One of the prerequisites of creating such accounts are providing personal data such as Name, Date of Birth and Gender of the account creator. These are the identification datas that pinpoint the users.


\textsuperscript{6}https://www.echr.coe.int/Documents/Convention_ENG.pdf (as seen on 21.04.2018)

Furthermore, the Check-in services in Facebook pinpoint the real time location of the users. Facebook also uses the ‘Current City’ and ‘Homecity’ under the pretext of locating the friends and acquaintances of the users in the city, but in reality it serves as a means to track our locations. The mere usage of Google Maps for our navigation, which is an everyday usage for us in this era, also renders our real time position and moreover, can follow us point-to-point through GPS and thereby generates more personal data than we intentionally share over the social media through posts and tagging on social media.

The current trend of sharing and oversharing in social media is leaking our personal data in such an unprecedented rate and well beyond our control and in a way, our personal information is being taken from us in ways never done before, sometimes with our consent, explicit or otherwise and sometimes, without our consent.

This generation of data over social media has revolutionised the world in ways unimaginable in the last few years. Government toppling movements such as Occupy and Arab Spring came into being and turned into such a huge phenomenon due to the influence of the social media. Both the movements ‘saw widespread social media activity, have been the subjects of numerous studies in different fields that have taken advantage of abundantly available social media data. (Conover, Davis et al. 2013; Costanza-Chock 2012; Gaby and Caren 2012; Papacharissi and Oliveira 2012; Starbird and Palen 2012)

Twitter and Instagram use hashtags as a means of putting the users under a common heading, irrespective of the reasons of the users using such hashtags. For example, under the hashtag #hamburghafen, Instagram shows 36,864 public posts and under #hamburgharbour 12,807 public posts (as of 07.03.2018). The tags mean the same thing, the only difference being the language to describe ‘harbour’ has created two different tags and thereby showing a clear division among the number of users who have visited or was near the Hamburg Harbour for any number of reasons. It shows in a very clear cut manner as to how many users among those who visited Hamburg Harbour spoke German and who spoke English or at the very least, a close estimate.

1.1 Internet of things

According to Patrick Nitschke the Koblenz University, Germany ‘The Internet of Things (IoT) is a network of addressable, physical objects that contain embedded sensing, communication and actuating technologies to sense and interact with their environment (Geschickter 2015). Like every novel paradigm,
the IoT sparks interest throughout all domains both in theory and practice, resulting in the development of systems pushing technology to its limits.\textsuperscript{8}

With the internet age, we have also molded and developed ourselves to have gadgets as part of our life. Not only have we adopted these gadgets, we have also become dependent on them. The dependency is not codependent or interdependent anymore, it is one of complete dependence.

The wish to get rid of everyday boring chores ends up in divulging our personal data to various devices which in turn, store our data in their private servers. Alexa and Siri are such devices to name a few. When we allow them access to not only our personal data, but vicariously to the personal data of all the people in contact with us, including family, friends, business and work contacts and acquaintances.

Siri and Alexa dwarf in comparison, when we compare it to bigger systems such as health cards and traffic monitoring systems. Health cards, as a part of the statutory medical programme in Germany, holds essential information about a patient’s health and treatments in the chip embedded in the card. While it facilitates for a better access in case of emergencies, it also makes the patient data vulnerable to any kind of misuse in case of loss.

Traffic monitoring systems, while used for monitoring potential traffic accidents and criminal attacks, are also used for various kinds of surveillance and in turn, creates a breach in the privacy of the common people by recording them in transit, even though it is clearly mentioned in the public vehicles in Germany that the data will be retained for 24 hours, but even then, it is 24 hours too much and the data is retained without any kind of consent from the data subjects. They are merely informed, but are given no choice to decline, leaving them the only option of not using the public vehicles.

However, it must also be admitted that it is a kind of trade off. Personal data for easy accessing and for living a more comfortable and a much safer and secure life. Even the travel maps we use such as Google maps for our daily transportation also saves our regular commute data. Google Maps even has the feature to remind us of our upcoming transport should we put in the time of daily commute in it. Essentially, we take it for granted that we have to part with our personal data, namely the exact times of departure and arrival for work.

According to a survey conducted by The European Commission in 2015, 78% of the surveyed subjects in Germany and 71% of the subjects surveyed in the European Union feel that providing their personal data is an inevitable part of the modern life. 58% in Germany and 67% in the European Union feel that they have to part with their personal data in order to gain access to any kind of services. However, when asked about their opinion whether they think that they have to provide their personal information online, 43% in the European Union thought they have to, whereas in stark contrast, 64% in Germany said that they have to provide their personal data. But when asked if providing their personal data is a problem for them, about 57% in the European Union and 56% in Germany strongly objected to provide their data.

\textsuperscript{8} \url{https://kola.opus.hbz-nrw.de/files/1436/nitschke_msc.pdf} (as on 14.03.2018) by Nitschke, Patrick

‘Development of an Internet of Things architecture framework based on Sensing as a Service’ submitted on March 2017
Furthermore, when asked if they are willing to provide their personal data for free services online, such as free email address etc, a staggering 52% in the European Union and 49% in Germany strongly disagreed on it.  

This shows a contradictory trend. The people or the users have the knowledge that their data are exclusively their own data, but are also not willing to provide it as a means of payment in return for the free services. Some have come to a compromise that it is inevitable to avail online services without providing their personal data, but more than half of the data users are of the consensus that they do not want to contribute to the big data of the data providers.

However, in spite of weighing all the pros and cons of data contribution and possible data misuse, subscribers to such devices are increasing every day.

1.2. Big data

Sky Croeser and Tim Highfield, in their Article ‘Mapping Movements-Social Movement Research and Big Data: Critiques and Alternatives’ mention that the term ‘Big Data” did not originate in communication or political studies, but has increasingly been applied to the analysis of large data sets in these and many other disciplines. It is now strongly associated with social media analysis, in particular (Boyd and Crawford 2012), as data sets continue to grow alongside the increasing access to, and availability of, tools for capturing, storing and processing more data. This also reflects trends around the use of social media, of course, as platforms such as Facebook, Twitter, YouTube, or Instagram saw more users register and thus more data contributed.

One of the pre-requisites of using the social media is to create an account using our personal data such as Name, date of birth, age etc. Till date, there is no social media which allows its users to use it anonymously. Facebook, the social media giant, openly admits that it collects our personal data for various purposes:

‘Things you do and information you provide.'

*We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or


the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.’ ¹¹

According to a Berlin Regional Court’s ruling in February 2018, Facebook’s default privacy settings and use of personal data are against German consumer law. According to the newspaper, ‘The Guardian’: The court found that Facebook collects and uses personal data without providing enough information to its members for them to render meaningful consent. The federation of German consumer organisations (VZBV), which brought the suit, argued that Facebook opted users in to features which it should not have. Heiko Duenkel, litigation policy officer at the VZBV, said: “Facebook hides default settings that are not privacy friendly in its privacy centre and does not provide sufficient information about it when users register. This does not meet the requirement for informed consent.” ¹²

In spite of the debate in regards to legality and authority of social media to process the personal data, it cannot be ignored that the social media are the highest source of big data. The social media giant, Facebook, currently boasts of about 2.2 billion active users, making it the biggest source of big data. Facebook merger concerns such as Whatsapp and Instagram are also not undebated in this arena.

However, social media’s big data collection had a huge influence on the research of social movement research. Research on various trends ‘show that obtaining and analyzing big data around social movements from social media are not limited to major research projects with connections to data providers, high performance computing, and extensive technical literary.’ ¹³ Social movements like ‘Occupy Oakland’ and The Jasmine Revolution have seen an overwhelming influence of social media. This trend was most noticeably seen from 2011 onwards with the major revolutions of the Middle East and Northern Africa. The major reason for this was not only internal fast communication which was made possible through social media, but also the extensive external coverage from the outside world, namely the western world due to the usage of social media and networking.

To research or to collect big data on social media, researchers rely heavily on hashtags. With the advent of twitter, hashtags have been widely used to track sudden incidents.

¹¹ https://www.facebook.com/about/privacy/ (as seen on 03.04.2018)

For Instance, Deen Freelon's (2011) exploratory analysis of 5.88 million tweets (a corpus featuring seven hashtags, including #egypt #libya #sidibouzid and #feb14) provided initial information around tweeting patterns for each of these movements, including daily activity and user location.\footnote{14}

While analysis of user location and daily activity point towards a potential breach of privacy of the users and analysis of their personal data without their consent, it can be denied that these analysis have a beneficial side too. Such analysis are not only minefields of multi faceted information but also analysis and gathering of information over various fields apart from the central subject such as linguistic and interaction.

According to Sky Croeser and Tim Highfield, the process of using big data techniques in social movement research adds to the existing complexities and requires revisiting and revising existing ethical models for social movement research.\footnote{15}

2. Data Providers’ Usage of the Personal Data of the Data Users

Data Users or Data Subjects are the consumers of social media, that is, the users of the social media. Data Providers are those who provide the services of such social media such as Facebook, Twitter, Instagram etc. Data Subjects provide or feed data to the Social Media as they use it for sharing their personal data through their posts. As one of the biggest social media platform, Facebook is often accused of data retention and data processing, in many cases, without the consent of the data users.

The accusation that Facebook retains the personal data of the data subjects long after the commercial value of such data has been long exhausted came to light after the Schrems (C-362/14, Maximilian Schrems vs Data Protection Commissioner), where the court stated in one of its judgement in respect to the case:


The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner (‘the Commissioner’) concerning the latter’s refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd (‘Facebook Ireland’) transfers the personal data of its users to the United States of America and keeps it on servers located in that country.\(^\text{16}\)

This case, although not explicitly mentioned, shows that at least data retention and its eventual automated processing, often without no consent or unclear consent of the data subjects happens and continues to be a real threat in the future too.

While automated data processing is the core of Data Protection under Convention 108 and the Data Protection Directive, there is no such limitations under the EU law. This includes personal data in a manual filing system, that is, a specially structured paper file.\(^\text{17}\) The reason to include paper file was to prevent the circumnavigation around any kind of restriction or legal regulations of data processing by printing the information out on paper and then processing it. It is also used for the indexing purpose which allows easy and quick access to information.

In defining the term ‘Processing of Personal Data’, the Data Protection Directive (95/46/EC) states in Art.3(1):

\textit{This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.}\(^\text{18}\)

Additionally, The Court of Justice of the European Union (CJEU) in the case of Bodil Lindqvist(C-101/01, Bodil Lindqvist, 6 November 2003, para 27) held that:

‘The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions or hobbies, constitutes the “processing of personal data wholly or partly by automatic means” within the meaning of Article 3(1) of Directive 95/46.’\(^\text{19}\)

Art.4 of the General Data Protection Regulation 2016/679 (GDPR), defines processing of Personal Data in various steps. However, it defines not only the processing of personal data in an effective manner, but also defines controllers and processors, who play an important part in Data Processing.

\(^{17}\text{Data Protection Directive, Art.3(1)}\)
GDPR defines processing as:

*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

According to Handbook on European Data Protection Law, the term ‘processing’ includes actions whereby the data leave the responsibility of one controller and are transferred to the responsibility of another controller.

For example, every person residing in Germany needs to register their address with the city officials. This data is in turn, handed over to the Fee Collection Service of ARD, ZDF and Deutschlandradio(ARD ZDF Deutschlandradio Beitragsservice) as it is mandatory in Germany to pay the Media fees. As soon as the data in regards to addresses change hands, that is, transferred from the city officials to the Fee Collection Service, it may be regarded as data processing.

The definition of Data Processing in GDPR is more or less same as the Data Protection Directive. However, data processing is heavily dependant on the controllers and processors. The definition of controller as well as processor are the same in both the regulation and the directive, namely:

'fielder’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

---


In other words, controller is someone that takes the decision to process the personal data of any number of data subjects. More than one controllers are regarded as joint controllers. However, a processor is not the same as controller. A 'processor' is a legally separate entity that processes personal data on behalf of a controller.²³

Both controller and processor have the legal responsibility to follow the parameters set by the Data Protection Law and therefore, only those who can be held responsible under the applicable law can therefore assume this position. In private sectors, this is usually a natural or legal person; in the public sector, it is usually an authority.²⁴

In case of private individuals, however, EU Law does not recognize them as controllers or processors, when processing of such data is purely personal or household activity.²⁵ ²⁶

However, the CJEU held in the Bodil Lindqvist(C-101/01, Bodil Lindqvist, 6 November 2003) that “the act of referring, on an internet page, to various persons and identifying them by name or by other means (...) constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of Directive 3(1) of Directive 95/46.”²⁷ (C-101/01, Bodil Lindqvist, 6 November 2003, Para 27)

Such personal data processing does not fall under purely personal or domestic activities, which are outside the scope of the Data Protection Directive, as the exception “must […] be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.”²⁸

According to the Data Protection Directive, a controller is regarded as ‘someone who alone or jointly with others determines the purposes and means of the processing of personal data.”²⁹

However, in case of any legal disputes, in reference to any illegal processing of data, the person or company, whoever was originally responsible for such processing of data, whether the

---

²⁶ Data Protection Directive, Recital 12 and Art.3(2) last indent
²⁷ C-101/01, Bodil Lindqvist, 6 November 2003, Para 27
²⁸ C-101/01, Bodil Lindqvist, 6 November 2003, Para 47
²⁹ Data Protection Directive, Art.2(d)
processing itself was legal or otherwise,\textsuperscript{30} will be held as the controller. However, in the case of a request for deleting the data, the request must be made to the ‘original’ controller, that is, the person or organisation who was originally charged with the processing of the data.

Joint controllers enjoy a unique position in the accordance to the Directive, as it stated that in case of legal disputes or other legal situations, they decide together to process data for a shared purpose.\textsuperscript{31}

The General Data Protection Regulation do not ‘explicitly state whether joint controllership requires the shared purpose to be the same for each of the controllers or whether it is sufficient if their purposes only partly overlap.\textsuperscript{32} No jurisdiction has been recognised under the European Law and there is no provision in regards to liability.

In order to combat these discrepancies, The Article 29 Working Party advocates a broader interpretation of the concept of joint controllership with the aim of allowing some flexibility in order to cater for the increasing complexity of current data-processing reality. \textsuperscript{33} In the case of Society for Worldwide Interbank Financial Telecommunication (SWIFT), which involved SWIFT sharing banking data to the U.S. Treasury Department, thereby facilitating the storage of personal data of the clients of the involved banks in Europe, in the US, The Article 29 Working Party came to the conclusion that the European banking institutions, although not explicitly ordering SWIFT to send the processed data to the U.S. Treasury, must be held equally liable for the disclosure, as the banking institutions were negligent in supervising SWIFT and therefore, cannot be realised from their responsibility fully, thereby resulting in joint controllership.\textsuperscript{34}

With so much data processing in our everyday life, the term ‘profiling’ comes into being. Although, the term is largely used in Criminal Law and Criminal procedures, it has been adopted in the Data Protection Law. The term ‘Profiling’ has been defined for the first time under the GDPR. The General Data Protection Regulation describes ‘Profiling’ as:

\begin{quote}
‘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
\end{quote}


aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.’ 35

The SWIFT case could have been a classic example of profiling as bank transactions directly reflect the economic situation of an individual. However, when it comes to social media, the breach becomes even larger and deeper. In Social media we not share only our own details but we also share the details of others, for example, our family and friends.

For example, when we tag a person with one of our pictures in a social media, for example, Facebook, the viewing circle increases widely as not only our friends will see the pictures, but the friends of the person we tagged will also see it and will not require our permission to repost it and thereby crossing the jurisdiction of sharing our information.

In Twitter, it is not so much widespread due to the 120 character constraint.

The social networking has also created the trend of commodification of personal information. 36 It means the transformation of what is normally used to be a non-commodity into a commodity; in other words – assigning economic value to something that traditionally would not be considered in economic terms. 37 This is the case with personal data, which in the “new” economy have acquired an independent economic value, and consequently became the object of quasi-property rights making the information about individuals a tradable good. 38

However, the recent whistle blowing case of Edward Snowden brought to our knowledge about the surveillance of the U.S government. According to Economist (13th September, 2014, Special Report p. 5) the U.S.Company BlueKai, an affiliate of Oracle Marketing Cloud, is reported to gather almost about 1 billion profiles with 50 different analytical uses for it.

To sum up, we are in a rough time, with phenomenal burdens lying on information privacy. The challenges are profound, they’re complex, and they’re constantly evolving, while the consequences are not always predictable. 39 As the social networking continues to be a “cool new

36 Stoddart, ‘Privacy in the era of social networking: Legal obligations of social media sites, Address held by Address by Jennifer Stoddart, Privacy Commissioner of Canada on November 22, 2010, Saskatoon, Saskatchewan


39 Stoddart, ‘The Path to Proactive Privacy’. 1st Annual Privacy and Information Security Congress 2010 organized by Reboot Communications Ltd, Address by Jennifer Stoddart, Privacy Commissioner of
tool”, we should stay connected to its emerging technologies, its social norms and market models, and – specifically - its legal and policy queries.

3. Personal Data and Behavioral Data

Behavioural Data may be regarded as any kind of data that can be obtained through the processing of personal big data, which indicate the behaviour of consumers and users, be it criminal, commercial or any other kind of behavior. According to Economist (13th September, 2014, Special Report p. 5) a data broker company in U.S. named eXelate is reportedly selling the data of men who have searched or shopped online for chocolates and flowers under the context ‘Men in trouble’.

Behavioural Science is mostly regarded as a part of the psychological and sociological studies. The Merriam-Webster dictionary defines ‘Behavioural Science’ as ‘a branch of science (such as psychology, sociology, or anthropology) that deals primarily with human action and often seeks to generalize about human behavior in society.’

Behavioral analysis, therefore, changes its scope with the perspective. Whereas in criminal law and criminal psychology, it stands as a means to profile criminals, in data protection, it stands for a completely different scope. It is not only limited to surveillance and pattern following, but it is also used to profile certain people in the social media.

In Europe, discussions about the legal requirements for behavioural targeting, a type of online marketing, often focus on the e-Privacy Directive’s consent requirement for tracking cookies and similar technologies. Dr. F. J. Zuiderveen Borgesius, Institute for Information Law (IViR), University of Amsterdam, in his article ‘Personal data processing for behavioural targeting: which legal basis?’ argues that that companies usually cannot base personal data processing for behavioural targeting on the legal basis necessity for performance of a contract or on the legal basis necessity for the controller’s legitimate interests. Therefore, companies must generally

Canada, held on November 15, 2010 at Ottawa, Ontario

41 https://www.merriam-webster.com/dictionary/behavioral science (as on 28.04.18)
obtain the data subject’s unambiguous consent for personal data processing for behavioural targeting. He also argues that Article 5(3) of the e-Privacy Directive does not provide a legal basis for the processing of personal data. That Article 5(3) of the e-Privacy Directive requires consent for storing or accessing information on a device of a user or subscriber.43

He also argues that some companies suggest that they can use an opt-out system to comply with Article 5(3) of the e-Privacy Directive. According to him, even if companies could obtain consent for cookies that way, the companies would generally be required to obtain the data subject’s unambiguous consent if they process personal data for behavioural targeting.44

In his article, he explicitly mentions: ‘When an ad is shown to a thousand people, on average less than one person clicks on it. Behavioural targeting, a type of electronic marketing, was developed to increase the click-through rate on ads. Behavioural targeting involves monitoring people’s online behaviour and using the collected information to show people individually targeted advertisements. Massive amounts of data are collected about hundreds of millions of people for behavioural targeting. In a simplified example of behavioural targeting, three parties are involved: an Internet user, a website publisher, and an advertising network. Advertising networks are companies that serve ads on thousands of websites and can recognize people when they browse the web. If somebody often visits websites about electronic gadgets, ad network might infer that the person is a technology enthusiast. The ad network might display advertisement for electronic gadgets when that person visits a website. When visiting that same website at the same time, somebody who is profiled as a travel enthusiast might see ads for hotels.45

Advertising becomes easier in Social media as Social media itself needs personal data to even begin to operate. There is no way to operate in social media, because the base of social media is personal data. Without an account consisting of at least name and date of birth, it is not possible to operate in Social Media. Arguably it can be claimed that it is for the best as to prevent any kind of crime through social media as well as taking measure against any kind of possible crime and harassment. With the rise of cyber crimes, anonymisation might backfire into an unprecedented rise of cyberbullying and other cybercrimes. Unfortunately, to prevent such crimes, the personal data is divulged to the social media sites which act as a website publisher. According a statistical analysis, Facebook earned a worldwide revenue of 28.17 billion U.S. Dollars in the year 2017 alone.46

---

The base of such advertisement is the processing of such data, which begs the question if the actions of the social media are illegal or if they are at all allowed to process our personal data as well as activity data for such advertisement purposes.

The Data Protection Directive contains two different sets of rules for lawful processing of Data: One for non-sensitive data in Article 7 and one for sensitive data in Article 8.\(^{47}\)

Article 7 of the Data Protection Directive states that:

*Member States shall provide that personal data may be processed only if:*

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).\(^{48}\)

In the matter of Lawful processing of non-sensitive data, Chapter II of Directive 95/46, entitled ‘General rules on the lawfulness of personal data’, provides that, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the Data Protection Directive\(^{49}\) and, secondly with one of the criteria for making data processing legitimate, listed in Article 7.\(^{50}\)


\(^{50}\) CJEU, Joined cases (C-456/00, C-138/01 and C-139/01) Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, 20 May 2003, para 65; CJEU, C-524/06, Huber v. Germany, 16 December 2008, para.48; CJEU, Joined cases (C-468/10 and C-469/10,
While consent is one of the basis of legal processing of non-sensitive data, contractual relationship is also a requirement for the processing of non-sensitive data. Under EU Law, under Article 7(b) of the Data Protection Directive, it has been stated that the processing of data is legal if it is deemed to be ‘necessary for the performance of a contract to which the data party is a subject.’\textsuperscript{51} It must be noted that while opening an account in social media such as Facebook, users are actually warned about the usage of their data under the ‘Terms and Conditions’, specifically under their data policy. The moment the users click on the “I agree” button, they are making a binding contract with Facebook, making the processing of the data and using such data for advertising completely legal. The only exception possible in this case is under the Council of Europe Law, that is, under Article.8(2) of the European Convention on Human Rights, where it is clearly mentioned that ‘the protection of the rights and freedoms of others’ is a reason for legitimate interference with the right to data protection.\textsuperscript{52}

Under Article. 7(d) of Data Protection Directive, the processing of personal data is lawful if it ‘is necessary in order to protect the vital interests of a data subject’\textsuperscript{53} which refers to the data ‘closely related to the survival of the data subject’ could be the basis for the legitimate use of the health data or of data about missing persons, for example.\textsuperscript{54} Even by a long stretch, the data that is shared in the social media cannot be regarded as ‘vital data’ that can be processed to ensure the survival of the data subjects. However, as the part of the contract that we make as we click on the ‘I agree’ button while creating the account, all data ever provided by us users are available for processing. However, Facebook now provides the caveat in case of personal data under the heading ‘Data with special protections’. Facebook states that:

*Data with special protections: You can choose to provide information in your Facebook profile fields or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) is subject to special protections under EU law.*\textsuperscript{55}


\textsuperscript{55} https://www.facebook.com/about/privacy/update (as seen on 06.05.2018)
While the core privacy data is protected, Facebook however, makes it very clear in its policies that it does, in fact, follows our behavioural pattern.

It clearly states that under two heads:

- **Networks and connections**: We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes……..

- **Your usage**: We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.  

The processing of personal data of the data subject in case of legitimate interests pursued by the controller or third party is deemed legitimate under Art.7(f) of the Data Protection Directive. It clearly states that the personal data may lawfully be processed if it “is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection (....)"

Facebook, in its ‘business’ page offers ‘Audience Insights’ to its advertisers. It clearly states that the page is for its advertisers for the better understanding of its target audiences. The page states that:

_Audience Insights shows you data about your target audiences so that you can create more relevant advertisements for them._

*We use native Facebook data to show you audience features such as:*

- **Age and gender**

---

56 [https://www.facebook.com/about/privacy/update](https://www.facebook.com/about/privacy/update) (as seen on 06.05.2018)

The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence. This obligation is of the classic negative kind, described by the Court as the essential object of Article 8 (Kroon and Others v. the Netherlands, § 31). The data that is shared by Facebook are therefore, can be partly regarded as a breach into the privacy of the data subjects. Although it does not pinpoint individuals through the data shared, it does tiptoe the breach line of Article 8 of ECHR.

One of the biggest defense that Facebook can offer in this case is that it processes all its data anonymously. It is for this defence that the processing of personal data such as gender, age, job qualification and job position cannot be deemed as breach of personal data privacy. Furthermore, Facebook and other social media, while governing behavioural data, takes into account factors such as Performed Action, Friend lists, Activity logs and user demographics. According to Thomas Paul, Daniel Puscher and Thorsten Strufe from TU

---

58 https://www.facebook.com/business/help/304781119678235/?ref=u2u (as seen on 09.05.2018)
59 https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (as seen on 09.05.2018)
Darmstadt and TU Dresden in their paper ‘The User Behavior in Facebook and its Development from 2009 until 2014’ mention that ‘These records contain almost all actions which have been performed on Facebook together with the timestamp and some metadata such as communication partners.’

4. Prediction and Push advertisement in Social Media

With the storage of such information, prediction and push advertisement comes into being, with prediction being basically analysing the target behavior and requirements of such audiences in accordance to the results gathered from ‘audience insights’. Facebook, in its business pages, has a detailed information for advertisers known as ‘detailed targeting’. It clearly mentions that:

Detailed targeting is a targeting option available in the "Audience" section of ad set creation that allows you to refine the group of people we show your ads to. You can do this with additional demographic information, interests and behaviors.

These detailed targeting options may be based on:

- Apps they use
- Ads they click
- Pages they engage with
- Activities people engage in on and off Facebook related to things like their device usage, purchase behaviors or intents and travel preferences
- Demographics like age, gender and location

---

60 [https://pdfs.semanticscholar.org/9cba/08f7a7af2419ee70c93f456470b6f0df8e0f.pdf](https://pdfs.semanticscholar.org/9cba/08f7a7af2419ee70c93f456470b6f0df8e0f.pdf) (as seen on 112.05.2018) The User Behavior in Facebook and its Development from 2009 until 2014, by Thomas Paul and Daniel Puscher (both of TU Darmstadt) and Thorsten Strufe (TU Dresden)
With such data readily available, it is easy for the advertisers to form a pattern among users in the social media. The Article 29 Working Party has noted that most advertising technologies use some type of client side processing of users’ browsers or terminal equipment to track their activity. This processing refers to the accessing and use of information stored on users’ computers. In behavioural advertising, companies use software to track user behaviour and to build personal profiles. They do not refer to users by name but, instead, use a single alpha-numerical code that is placed on the users’ computers. These codes are utilised to help select the advertisements people see in addition to the variety of products that are offered to them. These are known as ‘cookies,’ and they can provide a detailed profile based on user behaviour, which can be easily exploited for marketing purposes. These ‘functional cookies’ are generally exempt from the legal obligations under the Data Protection framework unless they are also used for tracking or profiling purposes. The Data Protection Directive requires MSs to adopt legislation

---

61 The mobile device they use and the speed of their network connection

62 With such data readily available, it is easy for the advertisers to form a pattern among users in the social media. The Article 29 Working Party has noted that most advertising technologies use some type of client side processing of users’ browsers or terminal equipment to track their activity. This processing refers to the accessing and use of information stored on users’ computers. In behavioural advertising, companies use software to track user behaviour and to build personal profiles. They do not refer to users by name but, instead, use a single alpha-numerical code that is placed on the users’ computers. These codes are utilised to help select the advertisements people see in addition to the variety of products that are offered to them. These are known as ‘cookies,’ and they can provide a detailed profile based on user behaviour, which can be easily exploited for marketing purposes. These ‘functional cookies’ are generally exempt from the legal obligations under the Data Protection framework unless they are also used for tracking or profiling purposes. The Data Protection Directive requires MSs to adopt legislation

---

62 Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, Adopted on 22 June 2010


66 exception provided for under Recital 66 of the E-Privacy Directive (Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF (as seen on 14.05.2018)
regulating the processing and movement of personal data.\textsuperscript{67} As noted by van der Sloot et al., it is clear from Article 2(d) that ‘[t]he applicability of the Directive is triggered when “personal data” are “processed” under the authority of the “controller” of the personal data.’\textsuperscript{68}

In order to understand the impact of the Directive on behavioural advertising, one must first consider how cookies should be classified.\textsuperscript{69} Businesses involved in behavioural targeting often maintain that privacy legislation does not apply, as specific persons cannot be traced. This is based on the assumption that users remain anonymous, as they are only identifiable through the issued tracking cookie. However, in legal terms this notion is not completely accurate.\textsuperscript{70} The Article 29 Working Party opinion on behavioural advertising observes that targeted marketing clearly falls within the scope of the Directive for two particular reasons. First, the use of cookies normally involves the processing of unique identifiers and the collection of the IP addresses, which allows the tracking of particular machines (even when dynamic IP addresses are used). Second, the information that is collected relates to the users’ characteristics, and this is used to influence their behaviour. This view is further established if one considers the capacity for profiles to be linked with directly identifiable information given by the data subjects (for example registration details).\textsuperscript{71} The Article 29 Working Party observes that ‘mergers, data losses and the increasing availability on the Internet of personal data, in combination with IP addresses,’ are other scenarios that can lead to identification.\textsuperscript{72} The debate on this matter is however, 

\begin{footnotesize}
\textsuperscript{67} Jeroen Koëter, ‘Behavioural targeting and data protection’ available at: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf (as seen on 14.05.2018)
\textsuperscript{69} Jeroen Koëter, ‘Behavioural targeting and data protection’ (n:36) available at: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf (as seen on 14.05.2018)
\textsuperscript{70} Jeroen Koëter, ‘Behavioural targeting and data protection’ (n:36) available at: http://www.cambridgeforums.com/ww.admin/materials/privacy/5Behavioral%20targeting_paper_draft%20publication_030510.pdf (as seen on 14.05.2018)
\textsuperscript{71} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{72} Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)
\end{footnotesize}
unending. In EMI & Ors v Eircom Ltd (2010)\textsuperscript{73} Charleton J in the Irish High Court concluded that IP addresses do not amount to personal data under the terms of the Data Protection Directive.\textsuperscript{74} In contrast, one year after Charleton J’s judgement, the CJEU in Scarlet v Sabam found that IP addresses are classified as personal data, as they allow users to be directly identified.\textsuperscript{75} The Article 29 Working Party have clearly stated on a number of occasions that IP addresses constitute personal data under the terms of the Directive, as they can be traced to a natural person with the cooperation of the internet provider.\textsuperscript{76} The Article 29 Working Party is also of the opinion that cookies, in themselves, (even when IP addresses are not siphoned) still constitute personal data.\textsuperscript{77} In its assessment of the concept of personal data, the Working Party found that names are not always a necessary means of identifying individuals, as there are alternative methods of distinguishing an individual from other members of a group.\textsuperscript{78}

Under the terms of the draft Regulation the definition of personal data has been altered to include ‘online identifiers’ in the list of examples that may be used to identify an individual.\textsuperscript{79} It appears that in the proposed legislative update cookies will be specifically included as personal data under the terms of the Regulation. Even in the much more liberal landscape provided for in the US, the FTC found in a consultation document on the self-regulation of behavioural advertising a tendency to classify IP addresses and cookies that are used for behavioural targeting the same as ‘regular’ directly identifying personal data.\textsuperscript{80} It appears relatively obvious that Ad Networks, who collect and process the information and place and design the cookies used to retrieve the information, are classified as data controllers. However, the role of the publisher is much more complicated. Due to

\textsuperscript{73} EMI & Ors v Eircom Ltd [2010] IEHC 108.
\textsuperscript{74} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{75} Scarlet v Sabam Case C-70/10, November 24, 2011
\textsuperscript{76} Article 29 Working Party SE (n.36)
\textsuperscript{77} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{79} Frederik Zuiderveen Borgesius, ‘Behavioural Targeting, a European Legal Perspective’, (2013 vol. 11 no. 1) IEEE Security & Privacy 82-85
\textsuperscript{80} http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf, p. 20 et seq.
the way in which websites are engineered, it is the data subject’s browser that automatically transmits the IP addresses to the ad network provider in order to facilitate the sending/reading of the cookies and to present the tailored advertising. It is important to note that, although the data transfer is caused by the browser, it is the publisher’s implementation of the website that triggers the transfer, and the data subject has no input. Thus, the Article 29 Working Party finds that publishers have certain responsibilities under the Data Protection Directive. However:

‘This responsibility does not cover all the processing activities necessary to serve behavioural advertising, for example, the processing carried out by the ad network provider consisting of building profiles which are then used to serve tailored advertising.’

Following an ad click, the users’ actions may be tracked for conversion statistics and potential retargeting. Although this may not be strictly linked to the initial ad serving, this information can also be shared (in fact, this is often a requirement under the Terms of service) with the ad networks, and used to improve on future targeted campaigns. This certainly raises the notion of ‘co-controllers’.

According to Recital 10 of the E-Privacy Directive, the Data Protection Directive applies ‘to all matters concerning protection of fundamental rights and freedoms which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals.’ Article 29 Working Party observed that the Data Protection Working Party, Online Behavioural Advertising (n:2)

---

81 Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)
82 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
83 Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)
84 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
Protection Directive has full applicability, with the exception of the provisions that are specifically addressed in the E-Privacy Directive. This mainly corresponds to the legal grounds for data processing found in Article 7 of the Data Protection Directive.\(^87\) The remaining requirements under the Data Protection Directive (including the principles regarding data quality, the data subject’s rights, confidentiality and security of the processing and international data transfers) have full applicability.\(^88\) The E-Privacy Directive provides the specific rules relating to the processing of personal data and privacy protection, in relation to the electronic communications sector.\(^89\) Of particular importance is Article 5(3), which applies when a provider is accessing or storing information on a user’s computer remotely.\(^90\) Therefore, the targeting advertising has some concrete legal obligations around it.

In the opinion of the Article 29 Working Party, it is clear from a literal interpretation of Article 5(3) that prior consent is required before the information can be placed or processed. For the consent to be informed, prior information regarding the purposes of the cookie must have been given to the user.\(^91\) It is clear that these requirements are cumulative in nature.\(^92\) When it comes to Online Behavioral Advertising, the users should be clearly informed about the purposes of the cookies and, hence, that they will allow the tracking of the users’ visits to other websites, the advertisements they have been shown and which ones they have clicked.\(^93\) It is important that the information is presented in a user-friendly manner so as not to negate its influence. This reflects the concern that the information should be easily accessible and understandable and ‘should not be ‘‘hidden’’ in a link at the


\(^88\) Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)

\(^89\) N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, ‘Online tracking: questioning the power of informed consent’ (2012 Vol. 14 No. 5) info 57-73.


\(^91\) Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)


\(^93\) Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)
bottom of a page referring to a vague and unreadable privacy policy.\footnote{N. van Eijk, N. Helberger, L. Kool, A. van der Plas and B. van der Sloot, ‘Online tracking: questioning the power of informed consent’ (2012 Vol. 14 No. 5) info 57-73.} The Article 29 Working Party suggests that ‘Statements such as "advertisers and other third parties may also use their own cookies or action tags" are clearly not sufficient.’\footnote{Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)} Recital 66 goes on to state that the method for refusing cookies should be ‘as user-friendly as possible’.\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958} The Directive does not provide specifics as to how this may be achieved and this is reflected in the varying implementations of cookie notices.\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958} In keeping with the general move towards more transparent data processing, Article 11 of the draft regulation contains a specific provision in relation to the communication of information.\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958} This movement towards transparency and the provision of clear communication is also aided through recital 32 of the proposal, which states that privacy policies are required to be as clear and transparent as possible and should not contain ‘hidden or disadvantageous clauses’.\footnote{Christopher Kuner, Cedric Burton and Anna Pateraki, ‘The Proposed EU Data Protection Regulation Two Years Later’ (2014 13 PVLR 8) Privacy & Security Law Report http://www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf (as seen on 15.05.2018) Article 29 Working Party SE (n.32)} Article 6 of the 1995 Directive outlines various conditions that must be satisfied by the data controller in relation to data quality.\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958} It is clear from the Article that processing can only take place for legitimate purposes. In its opinion on Search Engines, the Article 29 Working Party has stated that ‘some purposes, such as “improvement of the service” or “the offering of personalised advertising” are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose.’\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958} The Working Party observed that this was particularly true when the controller also mentions additional purposes for the data.\footnote{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958}
relation to behavioural advertising, it must be understood that the Working Party’s reference to ‘personalised advertising’ reflects more the data controllers’ explanation of the purposes to the data subjects rather than the specificity of the activity in itself.\textsuperscript{103} This is also indicative of the purpose limitation principle which in Article 6(1)(b) ‘prohibits the processing of personal data which is not compatible with the purposes that legitimised the initial collection.’\textsuperscript{104} Article 6 further stipulates that data should be accurate and updated if necessary. All reasonable steps must be taken to ensure that inaccurate and/or incomplete data are erased or modified while remaining conscious of the purposes for which they are being processed. This presents a clear problem in relation to Online Behavioural Advertising in that, although analytics systems can ignore particular false positives, certain inaccuracies are unavoidable.\textsuperscript{105} Furthermore, Article 6(1)(e) outlines the retention principle, which requires the deletion of data where it is no longer necessary for the purposes it was gathered. This is an indication of the data minimisation principle which, although not expressly provided for, is implied by certain requirements in the Directive.\textsuperscript{106} There have been a number of key developments in this regard in the draft regulation.\textsuperscript{107} However, in spite of these provisions being there for the last 25 years, they are being put in text and reinforced only recently.

5. The concept of consent in Big Data Analysis and Behavioral Targeting

Article 8 of the Charter specifically recognises consent as the key condition for the protection of personal data. Behavioural advertising has based itself on the ability to place

\begin{footnotes}
\textsuperscript{103} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{104} Article 29 Data Protection Working Party, Online Behavioural Advertising (n:2)

\textsuperscript{105} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958


\textsuperscript{107} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\end{footnotes}
cookies on users’ terminal equipment. If users were unhappy with this, they were required to opt-out (provided they knew how). Under the amended Article 5(3), it is clear that informed prior consent is required before any such technology is used or even installed. Azim-Khan and Millard have observed that “[t]he requirement for explicit prior consent seems to have spelt the end of the “opt-out” regime.” The change implemented by Directive 2009/136 provides a clear departure by legislating for an ‘opt-in’ requirement by default and was a ‘bold step’. However, there is still strong criticism of this position from certain sectors. Article 2(f) provides that “consent” by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC. Hence, the interpretation of consent provided for under the Data Protection Directive is applicable. Article 2(h) of the Data Protection Directive states that “the data subject's consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

---


112 Orla Lynskey, ‘Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens’ (2011 36(6)) E.L. Rev. 874-886

113 Orla Lynskey, ‘Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens’ (2011 36(6)) E.L. Rev. 874-886


---
Furthermore, Article 7(a) of the Directive states that ‘Member States shall provide that personal data may be processed only if… the data subject has unambiguously given their consent’. This appears to be an extremely strict interpretation. Recital 66 of the amended E-Privacy Directive appears, however, to allow some room for the interpretations of the national legislators and advertisers in the interpretation of what constitutes consent. The recital states that ‘[w]here it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application.’ This appears to permit the use of browser settings to indicate consent to cookies. As virtually all browsers have privacy settings that allow users to control cookie usage, the major talking point is whether data subjects’ consent may be inferred from pre-existing browser privacy settings. Despite its focus on the issue of consent and cookies, the amended E-Privacy Directive failed to effectively clarify the interpretation of implicit consent with respect to browser settings. The Article 29 Working Party, in its opinion on behavioural advertising, observed that consent via default browser settings is unlikely to meet the requirements under the data protection framework. This is for three particular reasons. First, the ‘respawning’ of flash cookies circumvents the deletion of cookies and allows the

---

120 Rafi Azim-Khan and Jonathan Millard, ‘EU Data Protection Opinion on Behavioural Ads & Cookies – Clarifying or Confusing?’ (July 27 2010 pillsbury.com) Privacy, Data Security & Information Use 1-4
121 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
http://jolt.richmond.edu/v18i1/article2.pdf
bypassing of the data subject’s choice in their browser settings.\textsuperscript{126} Second, consent via browser settings implies user acceptance to future processing, conceivably without any knowledge of the purposes or uses of the cookie.\textsuperscript{127} Third:

‘based on the definition and requirements for valid consent ex Article 2 (h) of Directive 95/46/EC, generally speaking data subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information.’\textsuperscript{128}

In a study conducted in the US by McDonald and Cranor, the authors noted that ‘[o]ne participant said behavioral advertising sounded like something her “paranoid” friend would dream up, but not something that would ever occur in real life.’\textsuperscript{129} Accordingly, for those involved in OBA, in theory it appears to be difficult to avoid the opt-in requirement.\textsuperscript{130} The ambiguity surrounding the interpretation of consent is a definite stumbling block to effective and consistent monitoring of OBA within the Union.\textsuperscript{131} In their recent article, de Lima and Legge have noted two particular criticisms of EU law in this regard. First, in relation to the ambiguous interpretation of the laws.\textsuperscript{132} Second, the failure to provide an effective balance between commercial and individual needs. The proposed Regulation has confirmed the EU’s move towards an opt-in regime which ‘is intended to strengthen consumer data protection rights by facilitating individual control over personal

\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{126} European Parliament Consumer Behaviour in a Digital Environment (2011) at
\item\textsuperscript{127} \url{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045} (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\item\textsuperscript{128} Article 29 Working Party, Online Behavioural Advertising (n:2)
\item\textsuperscript{129} Aleecia M. McDonald Lorrie Faith Cranor, ‘Beliefs and Behaviors: Internet Users’ Understanding of Behavioral Advertising’, August 16, 2010
\item\textsuperscript{130} Orla Lynskey, ‘Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens’ (2011 36(6)) E.L. Rev. 874-886
\item\textsuperscript{131} \url{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045} (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\item\textsuperscript{132} \url{http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045} (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\end{enumerate}
\end{footnotesize}
information.\textsuperscript{133} The draft adds a provision requiring all consent to be explicit. Previously, explicit consent was only required for the processing of sensitive data.\textsuperscript{134} The commentary supplementing the Regulation clarified that this modification was ‘added to avoid confusing parallelism with “unambiguous” consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.’\textsuperscript{135} The modification of the consent requirement provided for in Article 7 of the draft is supplemented by Recital 25 which provides, ‘[c]onsent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject’s wishes…. Silence or inactivity should therefore not constitute consent.’\textsuperscript{136} The effect of these provisions is to effectively eliminate the enforceability of implied consent through default settings by requiring an express indication of consent by the user.\textsuperscript{137} According to Article 7(4) and Recital 34 consent is invalid where ‘there is a clear imbalance between the data subject and the controller.’\textsuperscript{138} Article 7(3) provides that the data subject has ‘the right to withdraw his or her consent at any time.’ The burden of proof rests with the data controller in all situations.\textsuperscript{139} Finally, it should be noted that the advancement of consent cannot be viewed in isolation but, instead, is indicative of the overall move towards counterbalancing ‘the benefits of technological advancements and risks for individual data protection by complementing the legal framework with the

\textsuperscript{134} Slaughter and May, ‘The new EU Data Protection Regulation - revolution or evolution?’ Briefing April 2012 https://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf (as seen on 15.05.2018)
\textsuperscript{136} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{137} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
principle of ‘privacy by default and by design’. Article 23 of the Regulation provides that:

‘[h]aving regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.’

This provision aims at encouraging the development of user-friendly methods of incorporating privacy in the overall primary design and code in order to move towards the notion of user empowerment. This could impose a heavy burden upon existing business models that would need a complete overhaul to comply with the proposed provisions. Nevertheless, the development of this concept reflects the EU’s insistence upon explicit consent and the struggle to find an effective and simple means for its implementation.

The move towards explicit consent in the proposed Regulation would remove some of the ambiguities surrounding the interpretation of this concept. Nevertheless, it is unclear whether this development is to be welcomed. An analysis of the potential problems...
associated with explicit consent is necessary.\textsuperscript{147} The proposed Regulation’s emphasis on explicit consent indicates the assumption that the opt-in version provides a stronger protection for users. At first glance it may seem that such a robust interpretation is justified.\textsuperscript{148} However as noted by Tene:

‘individuals explicitly consent to agreements all the time without such consent being informed, voluntary, or meaningful. Individuals sign boilerplate contracts (e.g., with banks or insurance companies), execute clickwrap agreements and end-user license agreements (EULAs), and download apps granting whatever permissions are asked of them.’\textsuperscript{149} But if we are to stop and enforce a rigid system of gaining consent first and then the processing of data or activating an as noted by Tene et al.:

‘Excessive reliance on opt-ins inevitably will disrupt user interfaces and encumber individuals with repetitive prompts, which they will be eager to click through to reach their destination. This will be exacerbated by the requirement in Article 7(2) of the GDPR that consent to data processing must be unbundled from other agreements.’\textsuperscript{150}y kind of targeting behaviour, it would create another set of problem with the barring of the free flow of information. Posner has observed that these privacy harms are arguably unsubstantial vis-a-vis the economic and societal benefits which tracking offers.\textsuperscript{151} Moreover, to render consent difficult to procure may prevent entities from engaging in those activities given the associated costs. As per Solove, ‘the result might be to restrict uses of data in a formalistic manner that fails to distinguish beneficial from harmful uses.’\textsuperscript{151} as noted by Tene et al.:

‘Excessive reliance on opt-ins inevitably will disrupt user interfaces and encumber individuals with repetitive prompts, which they will be eager to click through to reach their

\textsuperscript{147}http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045  (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{148} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045  (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
\textsuperscript{149}Omer Tene and Christopher Wolf, ‘Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent’ (Summer 2013 Vol. 4 Issue 3) Information Security & Privacy News 19-28
destination. This will be exacerbated by the requirement in Article 7(2) of the GDPR that consent to data processing must be unbundled from other agreements. The result would be a poor user experience that nullifies any positive effects of opt-in consent. The more common cookie notices become, the more mundane, easily dismissed and ineffective the obligation to consent is rendered.

Accordingly, this issue appears to be somewhat of a double-edged sword that will result in dissatisfaction in some form, irrespective of the decision taken. It is apparent that explicit opt-in consent places the burden on the commercial entities. Nevertheless, it is uncertain whether these changes will, in fact, have any meaningful impact for the users. The task of adequately balancing interests is undoubtedly difficult. In assessing this issue, one has to realise that the commercial and data protection interests are clearly polarised. As outlined above, this manifests itself most notably in the debate surrounding the varied interpretation of consent. This ambiguity is reflected in many of the solutions presented and remains a clear stumbling block which has proven extremely difficult to navigate.

---

159 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
Social networks do not represent a particular “technology” or “tracking method” as the types of tracking techniques outlined above.\textsuperscript{161} Yet, online social networks constitute today an extremely popular trend encouraging people to stay continually “in contact”, “be watched” or “followed”.\textsuperscript{162} Surprisingly enough, such networks sometimes even promote the “tracking” as an asset of their website (for example, through an additional subscription fee, it could be possible for members to learn who other member looked at their personal details – like a cv – or who clicked on their profile to learn more about them).\textsuperscript{163}

Many users not only find this type of “tracking” trend normal but, all the more, they are seeking for it and are ready to pay extra to get it.\textsuperscript{164} On the other hand, there are social network members who usually consider the extra “tracking” features of social networking as “a necessary bad” that has to be tolerated, given that the privacy threats it entails are outweighed by the pleasure and other benefits resulting from users’ interaction on social networking sites.\textsuperscript{165}

This type of tracking uses users’ addiction to social networks in order to track every detail of the users’ every-day activities including those of their close family and friends.\textsuperscript{166} A number of heavily-used and well-known networks, such as Facebook\textsuperscript{167}, Twitter\textsuperscript{168}, Pinterest\textsuperscript{169} and LinkedIn\textsuperscript{170} have recourse to this on-line tracking technique.

Take the example provided by A. Roosendaal: the Facebook Like Button.\textsuperscript{171} According to Facebook, this widget allows users to share their interests and preferences

\textsuperscript{161}\url{https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf}
\textsuperscript{162}\url{https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf}
\textsuperscript{163}\url{https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf}
\textsuperscript{164}\url{https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf}
\textsuperscript{165}\url{https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf}
\textsuperscript{166}http://facebook.com/ (as seen on 15.05.2018)
\textsuperscript{167}http://twitter.com/ (as seen on 15.05.2018)
\textsuperscript{168}http://www.pinterest.com/ (as seen on 2018).
\textsuperscript{169}http://www.linkedin.com/ (as seen on 15.05.2018)
\textsuperscript{171}A. Roosendaal, We Are All connected to Facebook ::: by Facebook! in European Data Protection: In Good Health? (Springer Netherlands, 2012).
between them. However, the scope of this tool is far broader than what Facebook seems to tell. As explained by Roosendaal, when the users click on the Like button, a login field opens and require the user to log in his Facebook account. After the user has logged in, a link will be created in the feed of news in Facebook and the network of the user will be able to see the content of the link. No need to be connected to an account to be tracked. The simple fact of visiting a website on which a Like button has been placed is sufficient to track Facebook members, and even non-members. Non-members can also be traced if they have already visited the social network website once. The scope is therefore enlarged to other subjects that the subscribers, and to other websites than the social media website. In addition, the awareness around this tracking technique is not very extensive and, therefore, the volume of data processed is incredibly high, which represent a very high financial value.

It is clear that the effective balancing of the respective interests is difficult. In order to make significant progress in relation to the protection of users, privacy will need to be incorporated into the design of devices. To focus too strongly on the implementation of legal requirements is inappropriate given the inflexibility of this form of regulation. It is important to remember Lessig’s classifications and, thus, the balancing of the modalities of regulation. This refers to the notion that ‘Code is law’ and, hence, the effective balancing

172 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
173 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
174 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
175 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
176 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
177 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
178 https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
of the law, norms, architecture (code) and market.\textsuperscript{183} It is the mix of these modalities that is significant and any response needs to effectively consider the merits of each.\textsuperscript{184} Lessig proffers that code, in itself, has a regulatory dimension in that it can effectively direct the actions of the users.\textsuperscript{185} Indeed, he notes that code and law both play an important role in the information society.\textsuperscript{186} Significantly, code is preferable as it is not as easily ignored as legal rules. Use is restricted by the architecture of the system, whereas compliance with laws can be a matter of choice.\textsuperscript{187} In applying this concept to Online Behavioral Advertisement, ad networks could be restricted in their actions through the effective implementation of a code which effectively balances the modalities of regulation.\textsuperscript{188} The incorporation of privacy-enhancing defaults into the design of future technologies is perhaps the only means of ensuring the effective safeguarding of user privacy.\textsuperscript{189}

The key point from the above analysis is that the interpretation of consent will continue to

---

\textsuperscript{183} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{184} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{185} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{186} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{187} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{188} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{189} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
be a sticky issue under the EU Data Protection framework unless decisive measures are taken.\textsuperscript{190}

6. Purpose Limitation

Personal data must be collected for a purpose defined in advance.\textsuperscript{191} With regard to on-line tracking tools, the purpose for collecting data must be legitimate. The collection and storage of data must then be aligned with the defined purpose.\textsuperscript{192} In addition, the collection of data cannot override the purpose for which the on-line user has given his consent.\textsuperscript{193} Let us take as example the privacy statement published on the website of a market research organization explaining that, while it uses online tracking tools, the captured data will only be used to build up statistics on the number of visits that “hit” the website.\textsuperscript{194} If the market research company then uses the data for another purpose that is not directly linked to verifying the initial purpose, for example in order to sell those data to a number of companies interested in sending their on-line surveys to new prospects, then the “purpose limitation” rule has clearly been infringed.\textsuperscript{195}

Purpose Limitation is based on three data quality principles:

1) The data relevancy principle

2) The data accuracy principle and

3) The limited retention of Data principle.

\textsuperscript{190} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{191} Article 6 of Directive 95/46/EC
\textsuperscript{192} Article 6(1)(b) of Directive 95/46/EC
\textsuperscript{194} https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
\textsuperscript{195} https://www.springer.com/cda/content/document/cda.../9789401793841-c2.pdf
Purpose Limitation, in addition to the above principles also follow the ‘Fair Processing Principle’.

Under Data Relevancy principle, ‘only such data shall be processed as are’ adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed”.

The data accuracy principle maintains that ‘A controller holding information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to the date.”

In case of the limited retention of data principle, ‘Article 6(1) (e) of the Data Protection Directive and, likewise, Article 5 (e) of Convention 108 require Member States to ensure that personal data are “kept in a form which permits identification of Data subjects for no longer than the purposes which the data were collected for or for which they are further processed.” The data must therefore be erased when those purposes have been served.’

The fair processing principle governs primarily the relationship between the controller and the data subject, with transparency and establishing trust.

There are several fair information principles which need to be complied with in order to satisfy the obligations under the Data Protection Directive. The key requirement of the

---

197 Convention 108, Article 5(c); and Data Protection Directive, Article 6(1)
201 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
Directive is the vague obligation that personal data must be processed ‘fairly and lawfully’. Article 6 of the 1995 Directive outlines various conditions that must be satisfied by the data controller in relation to data quality. It is clear from the Article that processing can only take place for legitimate purposes. In its opinion on Search Engines, the Article 29 Working Party has stated that ‘some purposes, such as “improvement of the service” or “the offering of personalised advertising” are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose.’ The Working Party observed that this was particularly true when the controller also mentions additional purposes for the data.

In relation to behavioural advertising, it must be understood that the Working Party’s reference to ‘personalised advertising’ reflects more the data controllers’ explanation of the purposes to the data subjects rather than the specificity of the activity in itself. This is also indicative of the purpose limitation principle which in Article 6(1)(b) ‘prohibits the processing of personal data which is not compatible with the purposes that legitimised the initial collection.’ This prevents the re-use of information for purposes other than those originally specified to the data subject. In order for the repurposing of the collected personal data to take place, one is required to satisfy one of the legitimate grounds for processing under Article 7.

---

204 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958
205 Article 29 Working Party SE (n:32)
206 Article 29 Working Party SE (n:32)
208 Article 29 Working Party , Online Behaviorial Advertising (n:2)
updated if necessary. All reasonable steps must be taken to ensure that inaccurate and/or incomplete data are erased or modified while remaining conscious of the purposes for which they are being processed. This presents a clear problem in relation to Online Behavioural Advertising in that, although analytics systems can ignore particular false positives, certain inaccuracies are unavoidable. Furthermore, Article 6(1)(e) outlines the retention principle, which requires the deletion of data where it is no longer necessary for the purposes it was gathered. This is an indication of the data minimisation principle which, although not expressly provided for, is implied by certain requirements in the Directive. The principle provides that only the minimum amount of data required to adequately perform the processing should be gathered. This principle has been recognised by the Court of Justice which has found that the Directive ‘must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures.’

---


212 http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958


217 Case C-274/99 P Connolly v Commission, see also more recently in Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González
the terms of the Charter and the ECHR, and, hence, the importance of the principle of proportionality in this regard.\textsuperscript{218}

Data subjects have the rights of access, rectification, erasure and to object as enunciated under Article 12 and 14 of the Data Protection Directive; and, these rights should be respected by the data controller.\textsuperscript{219} In relation to Online Behavioral Advertising, this affords the data subject the right to access the information gathered by the ad network (i.e. their profile), to demand the modification or deletion of this profile, and to object to any further profiling.\textsuperscript{220} Certain Ad Networks provide these services and allow the data subject to modify and erase interest categories.\textsuperscript{221} Under the terms of the draft Regulation, the concepts of rectification and erasure are elevated in importance. These concepts are placed in a new section (Section 3), which provides for the right to rectification in Article 16 (elements of Article 12(b) in the current Directive), right to be forgotten and the right to erasure in Article 17 (elements of Article 12(b) in current Directive) and the right to data portability in Article 18.\textsuperscript{222} As noted by Savin, the latter of these ‘which is a new right, consists of the right to obtain a copy of the data from the controller for the further use by the data subject.’\textsuperscript{223}

\textsuperscript{218} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{219} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{220} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{221} https://support.google.com/ads/answer/2662850

\textsuperscript{222} http://www.jipitec.eu/issues/jipitec-5-3-2014/4095/#ftn.N10045 (as seen on 14.05.2018) EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour by Damian Clifford, URN: urn:nbn:de:0009-29-40958

\textsuperscript{223} Andrej Savin, EU Internet Law, (Elgar European Law Cheltenham UK 2013) 190-218.
7. Conclusion

The above discussion shows that while Targeted Behavioural Analysis might be a threat to the individual privacy, it is however, an essential part of the economic benefits and prevention of general threats, including cyber threat when it comes to Data Retention and Data Protection on Social Media.

With the enforcement of The General Data Protection Regulation, all major social media sites including Facebook and Instagram are updating their policies to follow the GDPR. The new changes allows data subjects and users more freedom of controlling their data on the social websites and thereby preventing, even in a small level, the misuse of their own data. Facebook especially, is creating and changing their policies to better protect their users’ personal data after the Cambridge analytica scandal, where more than 87 million profiles were harvested after Facebook launched an app called Graph in 2010, which allowed third party members to ask for the personal data of the users from the users, including the personal data of their friends.224

However, for the commercial purposes, purpose limitation acts as a shield for the processing of data of the users. Unless there is any major changes in the near future in both technology and legislature, the processing of data and targeting behavioral analysis including advertising is a necessary evil that we have to bear or remove ourselves from the digital world and social media completely, which in this digitalised world of today, is neither feasible nor desirable.