

**TALLINN UNIVERSITY OF TECHNOLOGY**

**Faculty of Business and Governance**

**Tallinn Law School**

Ezeani Uchenna Paul

**THE RIGHT TO BE FORGOTTEN IN SOCIAL MEDIA**

Bachelor Thesis

Supervisor: Kari Kasper LL. B, LL.M

Tallinn 2017

I hereby declare that I am the sole author b  
of this Bachelor Thesis and it has  
not been presented to any other  
University of examination.

Ezeani Uchenna Paul  
“ ..... “ ..... 2017

The Bachelor Thesis meets the established requirements

Supervisor Kari Kasper “ ..... “ ..... 2017

Accepted for examination “ .... “ ..... 2017

Board of Examiners of Law Bachelor's Theses

.....

## TABLE OF CONTENTS

Acknowledgements.....	4
List of Abbreviations.....	5
Abstract.....	6
Introduction.....	7
Chapter 1 Scope of Fundamental Rights.....	12
1.0 Understanding EU Privacy Law.....	15
1.1 The Crossroad of Rights.....	16
1.2 Social Media.....	19
Chapter 2 EU General Regulation on Data Protection (GDPR).....	21
2.0 Personal data.....	22
2.1 The burden of Data Controllers.....	23
2.2 Privacy Rights.....	25
Chapter 3 Right to be forgotten.....	31
3.0 Implications of Right to be forgotten.....	34
3.1 Historical Cultural Property.....	37
3.2 Exploitation of Online Identity.....	41
3.3 Social Media and Rule of Law.....	43
Conclusion.....	47
List of Sources.....	52
Annexes.....	56

## **Acknowledgements**

I greatly appreciate the contribution of my supervisor Mr Kari Kasper, whose cooperation and counsels saw me through in accomplishing this work. My gratitude also goes to the hard working academic and non-academic members of the Department of Law, Faculty of Business and Governance, through their support and assistance my study years was rewarding and impactful. In particular Dr Archil Chochia, Ms Kaja Kattel, Mr Pawan Kumar Dutt, Dr Addi Rull and Ms Tiina Parve.

My profound appreciation goes to my parent Mr and Mrs Ezeani, and my siblings Elochukwu, Chinedu, Obiageli and Nnenna for their constant love and best wishes.

## **List of Abbreviations**

**BBC** - British Broadcasting Corporation

**CNN** - Cable News Network

**CJEU** - Court of Justice of the European Union

**ECHR** - European Convention on Human Rights

**ECtHR** - European Court of Human Rights

**EC** - European Commission

**ePD** - Electronic Privacy Directive

**EU** - European Union

**GDPR** - General Data Protection Regulation

**EU-GDPR** - European Union General Data Protection Regulation

**NSA** - National Security Agency

**UN** - United Nations

**US** - United States

**UK** - United Kingdom

**MP** - Member of Parliament

## **Abstract**

Ezeani Uchenna Paul, Department of Law, Faculty of Business and Governance,  
Tallinn University of Technology, Tallinn, Estonia.

Abstract of Bachelor's Thesis Submitted 3 May 2017:

Thesis title: The Right to Be Forgotten in Social Media

History has been the core part of humanity, from the Agricultural Age to the Industrial Revolution and now, the so-called Information Age. Information Age transition rapidly with the advent of the internet. The internet enables interconnectivity and global reach of humanity, creating new frontiers and faster means of communication. However, internet services are mostly usable when data are shared between service provider and users,

Personal data are constantly been collected and processed especially online, and social media sites remain one of the biggest collectors of such data. And to that end, a lot of question has been raised, in particular in EU concerning online safety and responsibility. Consequently a new regulation shall come into force in May 2018, the General Data Protection Regulation. Article 17 of this regulation henceforth shall be the legal basis for the right to be forgotten in EU.

## Introduction

The concept of individual liberty and freedom has been a topic in all spheres of life especially when it measure the inherent rights of all human beings. The idea of free choice and enterprise can even be traced far back to the biblical accounts of the first society as documented in Genesis<sup>1</sup>. The strength of this work arises from the Directive 95/46/EC of The European Parliament and of The Council<sup>2</sup> and the new EU General Regulation on Data Protection (EU-GDPR)<sup>3</sup>.

The GDPR came into existence as a result of the proposed reform in 2012 by the European Commission (EC), following the work of the committee saddled with the responsibility to come up with a newer framework, the GDPR was thus born, which is a more comprehensive and conceded by all Member States, and therefore have a wider application as a Regulation. The GDPR shall become applicable to all Member States of the EU from May 2018.

Thus, all EU Member States must have fully transposed the General Data Protection Regulation as mandated by the European Commission. Part of the changes in the new EU Data Protection is to strengthen citizens' rights particularly on their activities in the internet and online marketplaces. This is the backdrop of the Court of Justice of the European Union, Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner<sup>4</sup>, which rendered the Safe Harbour Scheme invalid on the basis that the personal protection of EU citizens is not guaranteed nor secure enough from misuse and abuse by other third parties. Fundamentally, "Right to be forgotten" was strengthen.

This move compounds changes in Data collection and processing of EU citizen especially among big online retailers and social media providers.

The European Union (EU) can boast of a strong 508 Million citizens which make it a viable economic and digital market influencer in the world, therefore, the European

---

1 Genesis, Bible

2 Directive 95/46/EC, Art.17

3 General Data Protection Regulation (GDPR), Art. 17

4 Maximillian Schrems v Data Protection Commissioner, Case C-362/14, <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> (11.11.2016)

Commission vision for the adequate protection of her citizens' online can be seen as visionary and bold.

The increasingly use of the internet and online generated information has been a question of contention, while it's almost inevitable for anyone to conduct business or even have access to social services and benefits without employing the use of Information Technology (IT). The junk of this information, however, are distributed amongst the big players in the so-called Information Age. For example, Google, Apple, Facebook, Yahoo, Microsoft, Twitter are some of the biggest collectors of personal information and data

Before one can access their services, you have to create an account using your personal information like names, emails, date of birth, address, phone number, photos, etc. On one hand, we cannot use such services without registering our identities with such companies, however, giving your personal data and information in order to obtain services has often resulted in "Trust" and "Integrity" issue. While a company can have our personal information, we are not sure about the how's, the when's, the what's and the where's our personal data are treated.

As a result, a growing anxiety and mistrust exist especially in the wake of Edward Snowdens revelation which demonstrated that personal information is not safe and secured as often assumed by consumers. In light of these, the European Commission in 2012, began a comprehensive and overhaul review of the current Data Protection regime in the EU, especially with an emphasis on multinational companies headquartered outside the EU.

**The author shall analyse the right to be forgotten as it relates to social media and traces the origin to European Union Human Rights. And shall also assess Article 17 of the GDPR<sup>6</sup> which is the modern regulation on the subject, and the place of cultures and historical archives online, as it concerns the right and limitation of personal data in EU.**

---

<sup>5</sup> Macaskill. E and Dance. G, The Guardian  
<https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> (16.01.2017)

<sup>6</sup> The General Data Protection Regulation(GDPR), Article 17,



For example, where do President Donald Trump tweets stands in proportionality to the cultural and historical heritage of mankind and his personal right to be forgotten online with all his tweets if he so pleased? Though his tweets as president of United States according to 1978 Act of Congress of United States on Presidential Record Act<sup>7</sup> can be argued as the official position of the country and therefore cannot be considered a personal data of Donald Trump as a natural person. Undoubtedly, right to be forgotten online is a powerful right in this context, and when collectively used can be very lethal to the idea of conservation and protection of the cultural and historical heritage of mankind.

Except if argue that online and internet imprint of humanity is not historically deserving. The author, however, would concur with the view of Carbone, C.E, that ‘cultural property’ are any shared and learned behaviour in a given member of society to the extent that it became a way of life of that society, that it can be transferred through learning from generation to generations Based on this premises, it is evident that our online identities are part and parcel of archiving of mankind.

Hypothetically, giving the statistic that 3.4 billion people worldwide are connected and using the internet<sup>9</sup>. The internet has become a global tool for dissemination of information and it is ever growing in different dimension particularly in social interaction. Social media is the new norm of communication and airing of views both publicly and privately. The impact of such massive gathering of people’s opinions linked to their personal identity exposed to the public by means of the online presence of one’s personal information is an area of consideration in the light of the right to be forgotten debate. If everyone in the EU would decide to exercise such right to be forgotten online, we are then talking about 83% of EU residents according to the report published by Eurostat about individual access to the internet.<sup>10</sup>

---

<sup>7</sup> Presidential Records Act 1978, The U.S. National Archives and Records Administration, <https://www.archives.gov/presidential-libraries/laws/1978-act.html> (06/03/2017)

<sup>8</sup> Carbone, C. E, To be or Not to be Forgotten: Balancing The Right to Know with The Right to Privacy in The Digital Age, 22nd Virginia Journal of Social Policy and the Law 2015, p525

<sup>9</sup> Manual for Measuring ICT Access and Use by Households and Individuals. International Telecommunication Union (ITU) <http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx> (06/12/2016)

<sup>10</sup> [http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital\\_economy\\_and\\_society\\_statistics\\_-\\_households\\_and\\_individuals](http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals) (06.12.2016)

The author shall analyse and trace the origin of the right to be forgotten. The research is however limited to precise operational part and the current debate in the European Union on the right to be forgotten, thus shall not dive into the US-EU legal regimes on the subject of personal data.

Chapter One shall be dedicated to the scope of the right and class of the right to be forgotten. A progressive accession shall be made from the founding universal rights as enshrined in the UN Universal Declaration of Human Rights<sup>11</sup> to the European Convention on Human Rights and Charter of Fundamental Rights of the European Union, including definitions and dominant cases on the matter. Chapter one shall also analyse the legal questions and why the right to be forgotten have grown to the point of legal ruling and steadfast regulation on the subject. The rise of social media as modern instrument for real-time communication and evolving new media for citizen's journalism and advocacy would also be discussed in Chapter One.

Chapter Two shall be extensively devoted to the EU Privacy Law, Data Protection regulation including the new GDPR<sup>12</sup>, Personal data and also the new EC Proposal for a Regulation on Privacy and Electronic Communications in online data collection of European citizens. And what it all means when it finally takes off in May 2018 and thus becomes binding in the 28 Member States. The characteristic definition of a Controller and Processor shall be proffer equally. The new GDPR as it regulates right to be forgotten and underpins its place in European society as part of the international player in cyberspace and information society.

In Chapter Three focus shall be made on the impact and implication of such right in the realm of things economically, especially for data collection and processing authority and entity. Definition of the right to be forgotten and limitation shall also be discussed in Chapter Three. Focus shall be maintained also in Chapter Three on social media as a revolution in the current debate which the CJEU rulings have established in privacy and personal data protection in case C-131/12 of Google Spain SL v. Agencia Española de Protección de Datos<sup>13</sup>

---

<sup>11</sup> UN General Assembly Universal Declaration of Human Rights 1948

<sup>12</sup> GDPR, (Regulation 2016/679)

<sup>13</sup> Google Spain SL vs Agencia Española de Protección de Datos, CJEU, C-131/12,

A parallel and historical review shall be made on the legal implications as well as the future of the concept of the right to be forgotten in the EU especially in social media, owing to the fact millions of EU citizens have constant online presence in social media platforms such as Facebook, Twitter, Instagram, Google, Yahoo, Snapchat, WhatsApp, Twitter etc.

The author made a comparative legal analysis from the vast scholarly body of works available on this subject with the view to arriving at a consensus on the right to be forgotten on social media as a developing trend, which a balanced and precise legal framework is required to address. The choice of scholarly material consulted and reviewed in this research are mostly contemporary legal and scientific journal by renowned publishers both in the EU and the US respectively. Others are journalistic facts carried by international news media like the BBC, The Guardian for example. International Conventions, Charter and Treaty document were also extensively sourced.

## **Chapter 1**

### **Scope of Fundamental Rights**

The idea of the protection and control of humanity became a very strong desire for global power after the atrocities of the Second World War, the consensus to have a sort of mechanism to put an end and control to the unnecessary suffering of innocent civilians became the cornerstone of today's model for fundamental rights as enshrined in UN Universal Declaration of Human Rights, which also later manifested in many other regional and national legal doctrines, including the Charter of Fundamental Rights of The European Union and European Convention on Human Rights.

The core of these rights is the rights includes freedom of opinion and expression, the right to life, the right to privacy, the right to freedom of thought and religion, right to participate in cultural life etc. These fundamental rights underscore the foundation of the modern world order in respect to peace and security internationally. They are the most easily referenced document regarding personal and collective freedom of human race.

According to Art 19 of the UN Universal Declaration of Human Rights “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”<sup>14</sup> Art 7 and Art 8 of the Charter of Fundamental Rights of the European Union provides for adequate protection for personal data and respect for private and family life. Art 7 in full states that“ Everyone has the right to respect for his or her private and family life, home and communications”<sup>15</sup> while Art 8 in part states the conditions upon which any such personal information can be sourced and the right of citizens whose personal data has been collected to have it “rectified”, in other words ““forgotten” “Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Everyone has the right of access to data which has been collected concerning him or

---

<sup>14</sup> UN Universal Declaration of Human Rights: Art 19

<sup>15</sup> Charter of Fundamental Rights of the European Union, Art 7

her, and the right to have it rectified<sup>16</sup>. On the internet various and numerous amount of information are available including personal data that could be collected and processed for short or long term, in any case, some of these data leaves an imprint in the cyberspace, upon which search engines technology maximize to give it users a more narrow search for any information so sought. As observed by S. Kulk, and F.Z, Borgesius “If you search for a person's name, a search engine presents you with a list of information from different sources. That set of information, as a whole, can create an image of that person. If one had to sift through all available information online without the help of a search engine, such an image would be difficult to construe”<sup>17</sup>

It follows that creating just an account on one social media platform does not imply that your identity and personal data is only visible or accessible only on that site, the advent of search engines like Google, Yahoo and Bing means that your personal details call be pull up just by search with your names or in combination with other details of your identity like geolocation, sex, photos etc.

When a successful search has been made and one’s data is retrieved and can be clearly studied by a third party which by no means was intended to have access to such detailed information about oneself, a simple example, is when an employer can discreetly search for a jobseeker(s) social media activities and presence by using the innocent personal data of the jobseeker in his/her Curriculum Vitae. With such information the employer extracted with the help of search engine, the employer can even make a decision without an interview and without the knowledge of the jobseeker. "There have also been many stories, some true and some likely urban myths, about people who have been adversely impacted in terms of employment searches, insurance benefits, education, and the like, as a result of information found online that may be inaccurate or out-of-date.

One of the worst risks with such information is that a data subject may not ever become aware of what caused the problem if a prospective employer or insurer, for example, does not disclose the contribution of online information in a decision adverse to a data

---

<sup>16</sup> Charter of Fundamental Rights of the European Union, Art 8

<sup>17</sup> Kulk, S., Borgesius, F. Z, Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain, 1 European Data Protection Law Review. 113 2015,

subject's application."<sup>18</sup> In this case, one's personal information can be used in a positive or negative manner depending on what the employer may be looking for in the future employee(s).

The social media as a legal basis for the fundamental right of citizens was never clearly foreseen, thus binding law in this field are scarcely precise, to interpret an action of an employer in this case as a violation of Article 8(1) (2)<sup>19</sup>.

Similarly, Article 7 and 8(1)(2) of the Charter of Fundamental Rights of the European Union which states that in Art 7 that "Everyone has the right to respect for his or her private and family life, home and communications" and similarly in Art 8(1)(2)"<sup>20</sup>.

Essentially, these Articles are the model for which further legal questions has been raised since the Convention and charter within the European Union framework is considered a customary norm, though it may not entirely be enforceable in international law, but are basis for the values, ideals and the spirit of the European Union political and social justice among the Member States. The wordings of the Articles has been interpreted to relate to the spirit of the Charter to restore power to persons who may wish to remove or have their personal information "rectified". Rectification of person's data gave breathe to the subsequent Directives in the EU affirming the possibility for a right to be deleted from a particular database of processing authority. Deletion of personal data from any online presence based on one's personal resolves to get such data rectified has formed the character of the right to be forgotten.

Social media is one area this right to be forgotten is greatly evolving especially since so many things can now be done on social media apart from the primary and traditional purpose of communication with friends and families. These days, more innovation has been added to social media sites like Facebook, Instagram, and Twitter, LinkedIn etc. which include business and commercial activities like buying and selling items either as a business to business or business to consumer. In some cases, it can also involve recruitment and advertisements like the case of LinkedIn and activism like in the case of Twitter and Instagram, the rise of the phenomenon of "Hashtag" (#) and "At" (@)

---

<sup>18</sup> Abril, P.S., Lipton. J.D, The Right to be Forgotten: Who Decides What the World Forgets? 103 Kentucky Law Journal 364 2014-2015

<sup>19</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, Art 8(1)(2)

<sup>20</sup> Charter of Fundamental Rights of the European Union; Art 7., Art 8(1)(2)

in marketing and promotional campaigns have given more popularity to social media presence to the extent that the economic and political potentials and advantages in reaching a wider audience and cutting across borders effectively with less effort and less expense.

There is no doubt for any of the account to be opened either on LinkedIn, Facebook, Instagram, Twitter, Google, Microsoft, Yahoo etc. which currently represent the biggest collector of personal data on social media in terms of number of users, without at least giving out our personal details either names, email, phone number, address, date of birthday, sex, academic, profession or the combination of all the above.

## **1.0 Understanding EU Privacy Law**

Directive 95/46/EC Art 2(a) defines Personal data or information as “any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity<sup>21</sup>” Personal Data are those detail that can be used to identify one, for example, names, email, phone, address, date of birth and even racial origin or nationality.

The purpose of sharing such information by a consumer is to obtain services and product provider by merchants and entities who need such personal information to tailor their services to an identifiable individual(s). In fact, this process is inevitable in the modern socio-political composition of the world especially in area of commerce and social activities, giving out our personal information in order to access services and product is not in doubt, however, what is in doubt is if such information or data would not be compromised or sold to a third party or misused outside the intended purpose.

These questions beg for answers and thus the idea of protection of information necessity. EU laws guarantee the protection of fundamental rights, as in Article 8 of the European Convention on Human Rights (ECHR)<sup>22</sup>, and that such rights are inherent

---

<sup>21</sup> Directive 95/46/EC Art 2(a)

<sup>22</sup> European Convention on Human Rights, Article 8

and should not be compromised. In view of that standardised convention of protection of rights, EU laws also consider the right to privacy a fundamental right. The need for such right to privacy to be protected in the growing digital economies of the world, it became apparent that some rules need to be set to ensure each individual's rights to personal privacy is not violated.

Personal Data travels far and wide, in a manner equalled to a click of a button, for that reason some protection of such data's must be enshrined in a legal binding documents and agreement that aims for accountability and mutual trust between the two parties involved *inter alia* the giver of the data and the collector of the data. The idea is that individual have full knowledge and right on what becomes of his or her data as shared with a service provider, and thus, also have right for redress in case of abuse or misuse. The protection guarantees that citizens can rest assured that giving out their personal data is secured and well managed. And can only be used for the intended purpose(s).

In 2018, the EU will have one of the most advanced and futuristic Data protection law in the world, the law empowered citizens within the block of 28 Member States to have adequate privacy protection and safety online<sup>23</sup>. This equally means stringent measures on the part of the data processors and controllers to ensure none of the rules is circumvented. In particular, article 17<sup>24</sup> specifically empowers data subjects with the right to be forgotten and the legal grounds request from data processors and controllers for such right to be enforced.

### **1.1 The Crossroad of Rights**

To clearly understand the thought process leading to the adoption of the General Data Protection Regulation (GDPR) in the EU, it is critical to examine two important phenomena that happened in the cyberspace with regards to the right to be forgotten which emerged from the right to private life.<sup>25</sup> First, the Google Spain SL v Mario. C. Gonzalez case (C-131/12)<sup>26</sup> and the infamous Edward Snowden revelation are two

---

<sup>23</sup> GDPR, Article 99

[http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

<sup>24</sup> *ibid* 17

<sup>25</sup> European Convention on Human Rights, Article 8

<sup>26</sup> Court of Justice of the European Union (CJEU), C-131/12,

<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>



examples.

Firstly, Google Spain SL v Mario. C. Gonzalez case involves "A Spanish citizen complained that an old case involving him featured too prominently in Google searches on his name, even though the case had been resolved several years before. The Court of Justice of the European Union (CJEU) upheld his case against Google, which has since provided a mechanism for people to register their desire to suppress..."<sup>27</sup> their personal data on the internet.

Secondly, the Snowden phenomenon, an employee of National Security Agency (NSA), which is an intelligent gathering agency of the US government, made some stunning revelation to journalists in 2013. Snowden revelation was detailed in series of leaks of classified documents. The bulk of the revelation was the secret programmes of the NSA to spy and collect personal information of citizens around the world by tapping, storing, recording, transferring their communications. The global surveillance programmes known as Prisms was secretly done with the cooperation of some European government and telecommunication companies including social media platforms.

The prism programme reverberated in the EU when it was revealed that German Chancellor Angela Merkel mobile phone also eavesdropped by the programme.<sup>28</sup> This loophole and vulnerability of EU citizen's data especially those data collected and processed outside the EU awaken the policymakers in the EU of the importance for an accountability and responsibility for any such violation. Thus the two events warranted a rethink and subsequently a redrafting of the current Data Protection Directive, in particular, the provision for the "right to be forgotten" was inserted in the new GDPR.

There is no attempt, to sum up the entire framework of right to be forgotten as currently drafted in the GDPR in this work, for there are many area of this concept that are still developing and not yet fully tested in courtrooms nor are there any consensus in public and private international legal order on the subject, as the case maybe in others area of binding international law, however, this work focuses on the current trend and what it

---

27 O'Hara. K., Shadbolt. N: The Right to be Forgotten: Its Potential Role in a Coherent Privacy Regime, *European Data Protection Law Review*, Vol:1, 178, 2015

28 Edward Snowden: Leaks that exposed US spy programme, BBC NEWS, <http://www.bbc.com/news/world-us-canada-23123964> ( 20/02/2017)

means specifically in relation to social media identity and the future of EU citizens online presence. For instance, consider Facebook as a country in a moment, it will be the most populous country in the world, for it currently have 1.79 billion monthly users globally as of 30th September 2016 and it is expected to further increase<sup>29</sup>

As the GDPR effectively entrust EU citizens with the right to be forgotten in the digital space, it is crucial to establish what these entrusted rights are and are there any limitations to them especially on social media which have become the new massive data collection platforms.

Consequently, the right to be forgotten are reoccurring factor predominantly in social media due to it user generated uniqueness and "Finally, the debate on the right to be forgotten affects a number of Internet services which rely on user-generated content. This issue is not unique to Facebook or social networking. Policy makers should take into account the “right to others to remember” and reach a balanced conclusion which respects freedom of expression."<sup>30</sup>

Facebook, for example, have taken some steps ensure user’s rights to be deleted permanently. “If you don't think you'll use Facebook again, you can request to have your account permanently deleted...”The process of “deletion” cancels the account and permanently removes all of the information on the account, and according to Facebook it typically takes about one month. However, the Electronic Frontier Foundation considered that “Facebook is trying to trick their users into allowing them to keep their data even after they've "deleted" their account”. Within this context, Max Schrems, who is a well-known figure in an on-going dispute between privacy rights and Facebook (as known Europe-v-Facebook), remarks that “We never complained that if you post something on Facebook, it’s going to be on Facebook...We complained that if you delete something, it’s still there.”<sup>31</sup>

---

<sup>29</sup>Statistics and Market Data on Social Media & User-Generated Content  
<https://www.statista.com/markets/424/topic/540/social-media-user-generated-content/> (27.04.2017)

<sup>30</sup> Lobbying Document by "Facebook" (2012), Facebook’s views on the proposed data protection regulation(summary by europe-v-facebook.org), Published by europe-v-facebook.org, p.6-7,  
[http://www.europe-v-facebook.org/FOI\\_Facebook\\_Lobbying.pdf](http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf) (01/05/2017)

<sup>31</sup> Gündoğan. C.O., Will Facebook Remember You Forever: The Right To Be Forgotten On Social Networks Within The Privacy Framework,University Of Essex, pg 42,  
[https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FTez%2FCigdem\\_OZER\\_GUN\\_DOGAN.pdf](https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FTez%2FCigdem_OZER_GUN_DOGAN.pdf) (01/05/2017)

## 1.2 Social Media

Social media have come to stay, it is a form of electronic communication through which users create online communities to share information, ideas, personal messages, videos and other content on the internet. The term has grown to narrowly represent sites like Facebook, Twitter, Instagram, Snapchat, WhatsApp etc. However, the phrase has also found a reference as Wikipedia, Blog sites and roughly many websites has been called social media site. It is therefore difficult to actually have singular definition for the phrase. Social media sites and social networking sites are not easily distinguishable by everyday internet users.

In order to arrive at a more practical definition, each word should be defined separately. Social describes an interacting with other people by sharing information with them and receiving information from them, while media describes a tool of communication, like the internet, while TV, radio, and newspapers are examples of more traditional forms of media.

Although, what is considered social media can be transformed into a completely different online service provider, as can be seen with MySpace and Orkut. “Social media platforms such as Orkut and MySpace are frequently being replaced, while others, for instance, Facebook, are constantly changing. As a result, our definitions and approaches also need to be dynamic. Platforms and their properties are less important as the cause of their contents (i.e. the reason why people post particular kinds of content on that platform) than we assume. Genres of content, such as schoolchildren’s banter, happily migrate to entirely different platforms with quite different properties. We reject the idea that the development of the internet represents a single trajectory. Some of the most important features of social media seem to be the exact opposite of prior uses of the internet. For example, the internet’s problem of anonymity has become for social media a problem of the loss of privacy.”<sup>32</sup>

To establish that the abovementioned definition falls within the scope of any site one visits, the following features are common in most if not all social media sites:

- User accounts: If it is usually the case that a visitor would be required to create

---

<sup>32</sup> Miller. D, et al, How the World Changed Social Media, University College London, UCL Press, pg xi, 2016, <http://discovery.ucl.ac.uk/1474805/1/How-the-World-Changed-Social-Media.pdf>

an account.

- Profile pages: As social media, it is often the case that profile pages exist so that other users can have an idea who they are communicating with. Like a profile photo, bio, website, feed of recent posts, recommendations, recent activity.
- Friends, followers, groups, hashtags etc. A function that allows users to have followings or being followed, and to have contacts and connections of other users.

Others are features like Notifications, News feeds, personalization, Like and comments sections, Information updating, Review and rating. Facebook and Twitter, epitomises our idea of social media.

"Often, each of your "friends" (Facebook) or "followers" (Twitter) will be connected to each other. Just like in real life, the connections between people aren't just one-on-one, but a network of connections. This online social network is useful for spreading information, pictures and videos and generally staying in touch with people you wouldn't normally get to interact with all the time. For example, you can easily set up a Facebook page with details and pictures of an event you might be planning, such as a school fete. The page allows you to easily send out invitations to other users of the social media site.

Just like other technology, for example, mobile phones, social media is a very effective tool for connecting with people. However, there are a few privacy and security issues worth keeping in mind."<sup>33</sup> These privacy and security issues are those the GDPR expected to tackle at least from the EU perspective

---

<sup>33</sup> Introduction to Social Media, Australian Communications Consumer Action Network (ACCAN), Australia's peak body representing communications consumers, 2007.  
<https://accan.org.au/files/Tip%20Sheets/Introduction%20to%20Social%20Media.pdf> (01/05/2017)

## Chapter 2

### EU General Data Protection Regulation (GDPR)

The year 2016 shall remain a very remarkable and a milestone in the European Union in the aspect of citizen's right advancement depending on the side of the coin one belongs. It was the year that saw the repealing and replacing of Directive 95/46/EC, the more comprehensive Directive that addresses the issues of personal data right and privacy right. The Directive has been in use for more than two decades. The changes in the digital world, in particular, the degree of cross-border online communications and businesses as well as in the processing of personal data informed the European Commission rethink, thus to rework the legal framework within the Single Market, as to enable adequate protection of EU citizens and residents from unwholesome collection or processing data of EU residents by any organization in the world.

This is to ensure that all data collected follows strict, but uniform procedures established by law within EU. As a result, Directive 95/46/EC needed to be replaced. The replacement is in the form of a Regulation, which is directly applicable in its entirety to all Member States. The General Data Protection Regulation also refers to as GPDR, (Regulation 2016/679) shall become applicable on May 2018.

At the heart of GDPR is to protect the fundamental rights of EU residents, which is proclaimed on Article 1(2) which states "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"<sup>34</sup> The most important features of the Regulation is the dedication of specific article solely to address the judicial precedent in the right to be forgotten. Article 17 is titled "Right to erasure" and bracketed "right to be forgotten". Article 17 establishes the legal basis based on the court judgement in the Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González<sup>35</sup>

The judgment in the case demonstrated that loopholes needed to closed with data collectors and processors, by establishing tougher responsibilities and also ensure that

---

<sup>34</sup> GDPR, Article 1(2), [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) (20/04/2017)

<sup>35</sup> Google Spain SL vs Agencia Española de Protección de Datos, CJEU, C-131/12, [http://curia.europa.eu/juris/document/document\\_print.jsf?doclang=EN&docid=152065](http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065) (12/02/2017)

EU resident's data are well protected no matter where their data are processed in the world.

Member States of the EU at national levels have begun sensitizations, workshops and campaigns to educate the populace especially corporations and business leaders as a preparatory step to welcome the changes in legislation and business environment as a result of the GDPR. For example, the Irish government have an ongoing project in that regard and a document called "the GDPR and you" have been distributed extensively in Ireland, part of the documents reads thus: "...GDPR introduces new elements and significant enhancements which will require detailed consideration by all organisations involved in processing personal data. Some elements of GDPR will be more relevant to certain organisations than others, and it is important and useful to identify and map out those areas which will have the greatest impact on your business model".<sup>36</sup>

"...It is essential that all organisations immediately start preparing for the implementation of GDPR by carrying out a "review and enhance" analysis of all current or envisaged processing in line with GDPR. This will allow time to ensure that you have adequate procedures in place to deal with the improved transparency, accountability and individuals' rights provisions, as well as optimising your approach to governance and how to manage data protection as a corporate issue. It is essential to start planning your approach to GDPR compliance as early as you can, and to ensure a cohesive approach amongst key people in your organisation"<sup>37</sup>

## **2.0 Personal Data**

From the moment one is born or in some cases conceived<sup>38</sup>, he or she has acquired some form identity either physical or biological identity, notably date of birth, place of birth, surname or own name, racial origin, nationality etc. This information is crystalline as one unique and distinct identity in the world at that earlier stage in life. Essentially, it is scientific and legal necessity to arrive at a consensus of the spirit of the

---

<sup>36</sup> The GDPR and You, General Data Protection Regulation, Preparing for 2018, Data Protection Commissioner, Irish Government,

<https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf> (01/05/2017)

<sup>37</sup> *ibid*

<sup>38</sup> Irving. D. N: When Do Human Beings Begins?"Scientific" Myths And Scientific Facts, International Journal of Sociology and Social Policy 1999, 19:3/4:22-36

draftsman when he declared the “fundamental freedoms” especially those emanating from the Universal Declaration of Human Rights, in particular, Article 3 (Everyone has the right to life, liberty and security of person)<sup>39</sup>

Certainly, there is no intention in the limited scope of this research to answer philosophical, moral or religious questions of when life begins, however, it is of interest to understand the origin of the concept of identity in the society and thus relate it accurately to the sophisticated advancement in personal identity especially to the question of what information can be considered a personal data in the digital age. Personal data are no doubt the objective subjects of the right to be forgotten, when an identity is formed and such information can be used to trace a natural person either digitally or otherwise without his or her consent, already the right to privacy<sup>40</sup> has been violated. The right to privacy and personal data processing are complementary and closely intertwined, to understand what exactly are personal data, we have to analyse the binding directive on the subject in the EU.

Currently, Directive 95/46/EC is the basis for personal data protection in the EU, for clarity, article 2(a) of the directive offers to define personal data. Personal data is therefore defined as “...any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. The GDPR comprehensively emboldened the definition further.

## **2.1 The Burden of Data Controllers**

The GDPR, specifically with regard to Article 17 of regulation have shouldered much of the burden to the Data controller(s), furthermore, it offers a definition as “a natural or legal person, public authority, agency or other bodies which, alone or jointly with others, determines the purposes and means of the processing of personal data; where

---

<sup>39</sup> The Universal Declaration of Human Rights, Article 3, <http://www.un.org/en/universal-declaration-human-rights/> (19/02/2017)

<sup>40</sup> Directive 2002/58/EC, Article 5(1), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> (19/02/2017)

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”<sup>41</sup> This is according to the GDPR. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. This is to avoid any possible abuse or misuse of personal data of residents and to help data controllers to fully understand their obligations and promote good practice.

Much of the internet interaction of citizens are still web or mobile based, though there is a growing demand in other forms of connectivity, specifically, the artificial intelligence technologies. This demonstrates that establishing who is directly a data controller or controllers may not easily be comprehended by everyday users, who perhaps want to download a particular Application from either IOS App Store or Android Google Play. Understanding who is collecting or processing his/her data is not of immediate concerns, rather the ability to be able to have the app installed with ease.

As information systems and business models become more complex, a number of organisations may be working together in an initiative that involves processing personal data.<sup>42</sup> Equally important is to ascertain the difference between a data controller and data processor. In order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the data controller that must exercise control over the processing and carry data protection responsibility for it.

In order to have a clearer picture of who or what data processors do compares to data controllers, is by understanding their responsibility before, during or after a data is collected. By practice, a data processor is expected to have minimal responsibility compares to a data controller with regards to each data of identifiable person collected. Subsequently, Article 4(8) defines a processor as “ a natural or legal person, public authority, agency or other bodies which process personal data on behalf of the

---

41 GDPR, Article 4(7). [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) (20/04/2017)

42 Information Commissioner’s Office; Data Controllers and Data Processors: What the Difference is and What the Governance Implications are: <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (20/04/2017)



controller”<sup>43</sup> This follows requirement by law to process personal data, data processors must retain data controller responsibility for the processing. It cannot negate its responsibility by handing over responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing<sup>44</sup>

This relationship between the data controller and data processor can be seen when one is signing up for a new App, take the example of Facebook, which has become a big data controller, much other organization depends on the data already collected by Facebook, to support its business concepts. Signing up for Tinder, for instance, require the importation of one’s personal data already collected by Facebook, like name, age, location, occupation etc. By this example, Facebook is, therefore, a data controller and share most of the responsibility, while Tinder is a data processor. Most times, data processor do not have any direct influence on the set of data to be collected or the condition or to modify the requirements. Ironically, as personal data are moved from one service provider to another, so too, we are losing our privacy along the way, as each platform maintain our data and subsequent monitor our activities.

## **2.2 Privacy Rights**

Privacy has long been the desire of humanity, the ability to mind one’s business and lifestyle without interference from any authority or persons. And privacy has in some way be linked to freedom, and freedom of oneself has a long history of protection in most international convention and customary international law, especially those freedoms elaborately encapsulated in The Universal Declaration of Human Rights, European Convention on Human Rights and Charter of Fundamental Rights of the European Union. Privacy is a phenomenon that date back pre-digital age, when no one thought that the world will be so interconnected technologically, when authorship and

---

<sup>43</sup> GDPR, Article 4(7), [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) (20/04/2017)

<sup>44</sup> Information Commissioner’s Office; Data Controllers and Data Processors: What the Difference is and What the Governance Implications are: <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (20/04/2017)

ownership of arts and literatures, poem or songs were mere intellectual property, though everyone understood then just as now the inherent right to privacy they had on their will, vow, trades, songs, or writings.

Interestingly, those are still the basis for the modern understanding of privacy rights even in the current technological and information age we live in now. Legislation may differ on the subject from country to country, depending on political history, cultural background, legal systems and perhaps the type of governments as the case between US and European continent.

Definition maybe the same between North America and Europe on privacy rights, however, concepts differs and expectation among citizens equally differs. Technologies and certainly the internet and cyberspace has increasingly connected people all around the world, it has become an instant and efficient method of dissemination of news, information, cultures, businesses and ideas. A wide range of people and citizens across Europe and America now have tremendous opportunities, especially with social media boom to even do more.

Generally across the two continent, people differ on what information can be considered private and how such personal data should be protected, and whether regulation is actually needed for such protection. And should an individual be entitled to control what information available of themselves on the internet and what role should authority have in the whole process.<sup>45</sup> While privacy is an imminent and evolving issue both in the US and the EU, the EU seems to be taking the lead in terms of the right of the citizens with regard to their personal information collected online. It is worth to mention that majority of the players in online cross-border information sharing, either e-commerce or social media are all American companies from the likes Facebook, Google, Instagram, Twitter, Amazon, Microsoft etc.

Striking a balance between users and policymakers across the two continent is increasingly necessary especially with EU agenda of a Single Market. Even as the

---

45 Siry. L Forget me, Forget Me Not: Reconciling Two Different Paradigms of The Right To be Forgotten: 103 Kentucky Law Journal 312, 2014-2015

concept of the right to be forgotten is yet to be understood clearly by American courtrooms as it was in Europe following the Court of Justice of the European Union (CJEU) ruling on the case C-131/12 between Google Spain SL vs Agencia Española de Protección de Datos.<sup>46</sup> The ruling emboldened the idea of the right to be forgotten and actually laying the bigger bedrock upon which regulations and legislations should be formulated, as the privacy rights are closely linked to the right to be forgotten.

Though the Convention on Human Rights and the European Union Charter of Fundamental Rights may have similar provisions, the Charter specifically have more detailed wordings on privacy rights and data protection rights<sup>47</sup> Article 7 and 8 of the European Convention on Human Rights (right to private life) and (the right to protection of personal data) respectively are the primary legal sources upon which privacy rights in the EU is generally extracted.

The European Court of Human Right( ECtHR) on the other hand has maintained a clear definition of privacy question in numerous rulings that span decisions on "relationships within families, the rights of persons to choose sexual partners, the rights of persons to be free from certain types of surveillance, the rights of persons (including celebrities) to be free from intrusion into their private sphere, as well as the right of convicted persons to re-integrate into society after serving a criminal penalty"<sup>48</sup>In *S & Marper v. United Kingdom*, 48 Eur. H.R. Rep. 50 (2008)<sup>49</sup>, ECtHR held that right to privacy necessarily includes the right to protection of personal information, thus the right to personal data protection especially against surveillance by the State. In 1981 saw a visionary move by the Council of Europe towards predicting the dynamism of the future with respect to the information society and dominance of internet as a means for personal data collection.

That vision leads to the Convention for the Protection of Individuals with Regards to

---

<sup>46</sup> Google Spain SL vs Agencia Española de Protección de Datos, CJEU, C-131/12, [http://curia.europa.eu/juris/document/document\\_print.jsf?doclang=EN&docid=152065](http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065) (12/02/2017)

<sup>47</sup> Siry. L: Forget me, Forget Me Not: Reconciling Two Different Paradigms of The Right To be Forgotten: 103 Kentucky Law Journal 315, 2014-2015

<sup>48</sup> Siry. L: Forget me, Forget Me Not: Reconciling Two Different Paradigms of The Right To be Forgotten: 103 Kentucky Law Journal 316, 2014-2015

<sup>49</sup> <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>, (12/02/2017)

Automatic Processing of Personal Data<sup>50</sup>, the convention sought to "secure....for every individual...respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."

Furthermore, the current Directive on Electronic Communication i.e Directive on privacy and electronic communications (Directive 2002/58/EC)<sup>51</sup> in the EU which first came into force in 2002 as a complementary directive to the Directive on Data Protection (Directive 95/46/EC). The term Electronic communication can be narrowly assumed to cover only those which passes through telephone, fax, email etc., however, in broad sense communication through electronic means are not limited to the aforementioned.

The internet is also a big junk of electronic communication which includes the email, Instant Messaging App and the social media. The dot-com era saw a remarkable shift in the way humanity does things on the cyberspace, notably communication and commerce<sup>52</sup>. Article 5(1) of Directive 2002/58/EC pays close concern to confidentiality of communication and "...in particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned...."<sup>53</sup> Also, Article 5(3) obligate data controllers as follows "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

This shall not prevent any technical storage or access for the sole purpose of carrying

---

<sup>50</sup> Convention for the Protection of Individuals with Regards to Automatic Processing of Personal, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> (12/02/2017)

<sup>51</sup> Directive 2002/58/EC, Art 1

<sup>52</sup>Ironman: Here's Why The Dot Com Bubble Began And Why It Popped, <http://www.businessinsider.com/heres-why-the-dot-com-bubble-began-and-why-it-popped-2010-12> (16.02.2017)

<sup>53</sup> Directive 2002/58/EC, Article 5(1)

out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user”<sup>54</sup>. Thus, the manner and purpose of which any information is gathered from users should not involve unlawful surveillance of the communication or tamper with personal data of the user without his or her consent.

However, Directive 2002/58/EC of the Electronic Communication is currently being reviewed, just like the Directive 95/46/EC of the Data Protection is expected to be replaced and transposed to the 28 Member States domestic legislation by the General Data Protection Regulation(GDPR) in May 2018. The new Proposal for a Regulation on Privacy and Electronic Communications (ePD)<sup>55</sup> recently published 10/01/2017 may replace the current directive when the European Commission adopt the proposal.

The proposed regulation is focused driven on the vision of the European Commission(EC) for a Digital Single Market, thus the study is divided into two part, one part focusing on the retrospective aspect between 2002-2016 and the other part focusing on the prospective aspect between 2016-2030<sup>56</sup> The proposal analyses Article 5(1)(2) of the ePD, Article 5(2) in particular which provide an exception for authority to legally monitor or place surveillance on electronic communication of users without recourse to Article 5(1). The proposed ePD further seek to harmonise and standardise the security and confidentiality of electronic communication across the EU, especially the necessity of legal framework to ensure the right to privacy and confidentiality of users.<sup>57</sup>

This is the backdrop of the statistical survey conducted among, public authorities, civil society organizations and citizens across the EU on the question of full protection of

---

<sup>54</sup> Directive 2002/58/EC, Article 5(3)

<sup>55</sup> Proposal for a Regulation on Privacy and Electronic Communications. [Proposal for a Regulation on Privacy and Electronic Communications](#) (18/02/2017)

<sup>56</sup>EC, Proposal for a Regulation on Privacy and Electronic Communications,<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications> (18/02/2017) p16,

<sup>57</sup> EC, Proposal for a Regulation on Privacy and Electronic Communications,<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications> (18/02/2017) p132

the right to privacy and confidentiality. Overall, 376 responses were collected regarding the question and "analysing the responses received in more detail, the data shows that citizens and civil society organisations, as well as public bodies, are enormously supporting EU rules on the right to privacy and confidentiality (90% each confirmed the necessity of the rules). Of all positive responses, 67% were provided by citizens and civil society organisations, 22% came from the industry, and 11% from public bodies"<sup>58</sup>

---

<sup>58</sup> *ibid*, p133

## Chapter 3

### Right to be forgotten

The right to be forgotten is a modest European concept, still in a very formative stage, but have resonated across the 28 Member States block of the European Union and it is reverberating far and wide including in the North America. Right to be forgotten became very pronounced in 1995 after European Data Protection Directive (Directive 95/46/EC)<sup>59</sup> officially took hold. Specifically, Article 6(d), 12(c) and 28(3) of the Directive emphasised the legal possibility for "...every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified", "...as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" and "...of ordering the blocking, erasure or destruction of data"<sup>60</sup> respectively. In essence, the right to be forgotten especially in the case of a criminal who has served his/her term.

"Rectified", "erasure", "blocking" and "destruction" are the exact wordings of the Directive which EU citizens are legally entitled to demand once their personal data are reasonably considered to have been processed "inaccurately" or "incompletely." Furthermore, Article 6(a) exceptionally caution that wherever collection of data is required for contract or transaction to be performed, such personal data needed shall be processed "fairly" and "lawfully"<sup>61</sup> and must be "collected for specified, explicit and legitimate purposes"<sup>62</sup>

The directive has seen vast interpretation with regards to changing the phase of internet activities and the fast pace of social media in the globalised world. The growing trend of viral tweets and videos are an example of how fast the social media landscape have completely changed. Superstars are made as fast as they can be destroyed within minutes on social media, one performance is enough to get one all the "likes", "views" or "comments", just as one uncut utterance, leak video or comments can send one down

---

<sup>59</sup>Directive 95/46/EC, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>

<sup>60</sup>Directive 95/46/EC, Art 6(d), 12(c),28(3), <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>(12/02/2017)

<sup>61</sup> Directive 95/46/EC, Art 6(a)

<sup>62</sup> Directive 95/46/EC, Art 6(b)

crashing. The internet and social media marriage is a union so powerful that it is difficult to predict what one can wake up to read or watch every single day on the internet.

The right to be forgotten is a relatively new concept in the EU and globally as well, in the EU the Court of Justice of the European Union decision in the case C-131/12 of Google Spain SL v. Agencia Española de Protección de Datos<sup>63</sup> became the cornerstone in the debate of personal right and freedom of speech and expression. The decision was a landmark ruling, not only because of its wide implication in the 28 Member States of the EU but also raises the question about the idea of personal rights.

From Google's perspective, “a nightmare potentially awaits, given the possibility that floods of requests are about to come its way. Publicly, the company has said it is looking closely at the implications. But privately, it is said to be furious”... “Right now, if you wanted to follow in Mr Gonzalez's footsteps, you would need to lawyer up.” “Eventually, if the EU has its way, sites like Google would need to set up an automated process to handle such requests. It would open up a bureaucratic nightmare, and one that would likely cost Google and others a huge amount of money to implement”<sup>64</sup>

Decisions on whether information should be removed from search engines depend “on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life”<sup>65</sup>

Google is increasingly being sued in different courts around the world on the premise of this EU precedent on the right to be forgotten judgement. And Google is making the case to balance the right to be forgotten with the right to information for the public interest. In France, for example, Google is “appealing to France’s highest court over a legal ruling that could force it to censor its search results worldwide.”<sup>66</sup>

---

<sup>63</sup> Court of Justice of the European Union (CJEU), C-131/12

<sup>64</sup> Lee. D., What is the 'right to be forgotten'?, BBC, <http://www.bbc.com/news/technology-27394751> (26/04/2017)

<sup>65</sup> *ibid*

<sup>66</sup> Hern. A., Google Takes Right to be forgotten Battle to France's Highest Court. The Guardian: <https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court> (30/04/2017)



Apparently, the challenges are enormous for Google and the legal cost inexcusable, however, Google have some cases overturned to its favour, example is the case filed in Japan against Google, and the Japan's Supreme Court..."dismissed a man's demand that internet search results of his arrest in a child prostitution case be removed under the so-called right to be forgotten "<sup>67</sup>

The man was arrested more than five years ago for paying a female high school student to conduct an indecent act. In the judgment, Justice Kiyoko Okabe, of the Supreme Court's Third Petty Bench said that "the deletion...can be allowed only when the value of privacy protection significantly outweighs that of information disclosure,"<sup>68</sup>.

Google, in a victory statement issued by Taj Meadows, head of policy and communication Google Asia Pacific said "We are pleased that the Supreme Court has unanimously recognized, based on existing privacy and defamation laws, that any decision to delete information from search results should prioritize the public's right to information"<sup>69</sup>

This Japanese decision came after various lower court rulings. "In 2015, the Saitama District Court ordered Google to remove the search results, acknowledging the right to be forgotten" In 2016, "...the Tokyo High Court rejected the man's demand, with the judge saying that the right to be forgotten is not a privilege stated in the law and its prerequisites or effects are not determined".<sup>70</sup>

The broadness of this fundamental human rights can be seen in 2010 Finnish Ministry of Transport and Communication announcement that everyone in Finland shall have "legal access "to the internet as a " fundamental right" and subsequently mandated all Telecommunication companies to abide by the legislation.<sup>71</sup> A poll conducted by BBC in 2010, in 26 countries among adult population found that about 79% agreed that

---

<sup>67</sup> Kyodo, Top Court Rejects 'Right to be forgotten' Demand:, Japanese Times, [http://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#article\\_history](http://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#article_history) (01/05/2017)

<sup>68</sup> ibid

<sup>69</sup> McCurry. J, Japanese Court rules Against Paedophile in 'right to be forgotten' Online Case: <https://www.theguardian.com/world/2017/feb/02/right-to-be-forgotten-online-suffers-setback-after-japan-court-ruling> (01/05/2017)

<sup>70</sup> ibid

<sup>71</sup> Finland Makes Broadband a Legal Right 2010 <http://www.bbc.co.uk/news/10461048>

“access to the internet should be a fundamental right”<sup>72</sup> As in the case of Finland, and by extension a shockwave in the entire EU Member States, and thus as a fundamental rights, it is further secured and protected by the first generation of human rights. Art 17(1) of International Convention on Civil and Political Rights, for example, provides “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”<sup>73</sup>

### **3.0 Implications of Right to be forgotten**

Article 6 of the Data Protection Directive 95/46, which states that data must be accurate and up to date or otherwise be erased or rectified and should only be kept identifiable for as long as it is necessary for the purposes for which it was collected. E-commerce giant like Alibaba recently on 11th November 2016 break all-time record of sales in a 24-hour online transaction with 18 billion United States Dollar worth of transactions on its annual event popularly known as “Singles Day.”<sup>74</sup>

And if we put the power and widespread of the internet into perspective, then consider Facebook as a country in a moment, it will be the most populous country in the world. These also means more power and discretion for individual users of online content either as a content producer or content consumer. The dependency of the world in doing things on the internet can only grow further in coming years and decades. Scholars have long held debates on the topic of the right to be forgotten on the cyberspace, while some held the view that such rights will alienate human culture and history completely.

This concept of oblivion, deletion or silencing of past life that do not exist anymore on the cyberspace is least controversial, it has been called many names: "rewriting history," “personal history revisionism," and "censorship" especially in the U.S because the issues are both social, legal, economic and technical<sup>75</sup>. Furthermore, is the unanswered question of what is actually “cultural” on the internet? What does humanity

---

<sup>72</sup> GlobalScan: Four in Five Regard Internet Access as Fundamental right: Global Poll, [http://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03\\_march/07/poll.shtml](http://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03_march/07/poll.shtml) (13.10/2016)

<sup>73</sup> International Convention on Civil and Political Rights, Art 17(1)

<sup>74</sup> Singles Day: Alibaba Breaks Record Sales Total, BBC NEWS, <http://www.bbc.com/news/37946470> 20/11/2016

<sup>75</sup> Ambrose. M.L: It's About Time: Privacy, Information Life Cycles, And the Right to be Forgotten. 16 Stanford Technology Law Review. 371, 2012-2013

aim to preserve culturally online? Would right to be forgotten means also forgetting where humanity is coming?

To understand the place of culture and its meaning in this context, Carbone, C.E. offered insights accordingly, today's cultural development is intimately linked to the digital world and its user-generated content arguably falls under the purview of "cultural property."

Though the precise contours of the term "culture" can be difficult to define, the following is a collection of definitions that demonstrate the term's applicability to the Internet and to the body of "property" that users are creating and nurturing in the digital world:

- ❖ The shared behaviour learned by members of a society, the way of life of a group of people
- ❖ A culture is the way of life of a group of people, the complex of shared concepts and patterns of learned behaviour that are handed down from one generation to the next through the means of language and imitation
- ❖ The set of learned behaviours, beliefs, attitudes and ideas that are characteristic of a particular society or population.
- ❖ Culture ... taken in its wide ethnographic sense is that complex whole that includes knowledge, belief, art, morals, law, custom and any other capabilities and habits acquired by man as a member of a society.
- ❖ The customary manner in which human groups learn to organize their behaviour in relation to their environment.
- ❖ . . . The learned and shared kinds of behaviour that make up the major instrument of human adaption... The way of life characteristic of a particular human society.<sup>76</sup>

Cultural assets of mankind are now increasingly been stored and documented online and in Big Data, these digital imprint of history and information when “erased” or “forgotten” as it were, what does it project about this current generation in regards to heritage and preservation of humanity and nature. Individual right to be forgotten, when

---

76 Carbone, C.E: To be or Not to be Forgotten: Balancing The Right to Know with The Right to Privacy in The Digital Age. 22nd Virginia Journal of Social Policy and the Law 2015, 527

combined with community activism, could mean the racial extermination of selective vices or at least some historical comic stereotypes embedded in the richness of a people. Societal dependence on the internet, online and digital environment as seen has grown in record numbers, and by extension social media has emerged as irresistible tools for almost everything in our daily lives. This is a new dependence and another obsession globally:

As Chelsea E. Carbone accurately puts it: “Today’s individuals in developed nations are hard-pressed to avoid the influence of technology. In fact, for many people, technology is inextricably linked to their lives. Whether it's tweeting an impressive update regarding their start-up, posting an amusing YouTube video on a friend's Facebook timeline, uploading their wedding album to Flickr, or updating their personal blog on Tumblr, people nurture their virtual identity hand-in-hand with their "real" one. A user can shop online for everything from a retired World War II tank on eBay to a soul mate on eHarmony. There are virtual friends, virtual sports leagues, virtual correspondence and virtual property; in short, virtual alter egos”<sup>77</sup>

This increased prominence for a right to be forgotten has caused alarm in the US and beyond for its potential impact on free speech, its technical demands, the burden it might place on private users of data and national security infrastructures.<sup>78</sup> While the EU and US may have seemingly diverging approach to privacy right legally, emanating from Convention, norm and political history. However, the concept and understanding are much the same, while the US privacy law is viewed as a contribution to Liberty, the EU privacy law, on the other hand, is seen as a contribution to Dignity.<sup>79</sup>

In furtherance to the overwhelming implication of the right to be forgotten in the European Union, Google for example has since step up to the challenge not only by updating its terms and condition for use, but equally have made it possible for evaluated process to allow such searchable information be removed from appearing on it search engine. Simon Wechsler captured it brilliantly; "As a means of hearing and deciding

---

77 Carbone, C.E. To be or Not to be Forgotten: Balancing The Right to Know with The Right to Privacy in The Digital Age. 22nd Virginia Journal of Social Policy and the Law 2015, 525

78 O'Hara, K., Shadbolt, N. The Right to be Forgotten: Its Potential Role in a Coherent Privacy Regime. European Data Protection Law Revised. 2015, 178

79 O'Hara, K., Shadbolt, N. The Right to be Forgotten: Its Potential Role in a Coherent Privacy Regime. European Data Protection Law Revised. 2015, 178

claims, Google created an online form to allow European citizens to request the removal of web pages that contain personal data relating to them. If Google grants a request, then the links are removed from searches for the requester's name. While the content is still available on the Internet, it cannot be found through a search for the subject's name. As of September 2016, Google had received approximately 1.1 million removal requests and granted around 40% of them. Google's process for evaluating these claims, how this process balances privacy interests against the interests of the public, and even the specific factors considered are all unknown to the public.”<sup>80</sup> In any case, Google reserves the right to either grant or deny such request(s) from EU citizens, getting a denial from Google further means extra-legal and technical hurdle for the citizen to cross.

The nearest option is to file legal action either with the local court or data protection agency in the Member State. "When Google denies a request, the requester can choose to appeal Google's decision to his or her national data protection agency, or to his or her nation's courts, by bringing suit against Google. If either the data protection agency or the court agrees with the data subject, then Google will be forced to remove the disputed content. Otherwise, Google's initial decision will stand, and the content will remain accessible.”<sup>81</sup>

### **3.1 Historical Cultural Property**

To fully understand the concept of historical cultural property, it is only rational to identify the underlying definition of the separate terms. What are considered historical? What are they that cultural? And what can be considered a property? Starting with historical: the Oxford English dictionary defines historical as thus ‘Of or concerning history or past events’... ‘Belonging to the past’ and ‘of the study of a subject based on an analysis of its development over a period’<sup>82</sup>. While, ‘cultural’ is defined as ‘Relating to the ideas, customs, and social behaviour of a society’...’Relating to the arts and to

---

80 Wechsler. S: The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten. *Columbia Journal of Law and Social Problems*. Vol: 49:1, 138, 2015-2016

81 Wechsler. S: The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten. *Columbia Journal of Law and Social Problems*. Vol: 49:1, 142, 2015-2016

82 Oxford Dictionaries: <https://en.oxforddictionaries.com/definition/historical> (16/03/2017)

intellectual achievements'<sup>83</sup> and finally, 'property'' is defined by same Oxford Dictionary as 'A thing or things belonging to someone; possessions collectively'...'an attribute, quality, or characteristic of something'<sup>84</sup>

Invariably, it can be deduced from the above definition that perhaps all human actions are themselves very cultural since mankind are essentially from the past, present and towards future. On that premise, whatever the new habitual lifestyle humanity adapted can be cultural as well, in short, cultural property of mankind is that imprint that is readable from the past to the future. Part of this readable imprint is the technological advancement, in particular, Information and Communication Technology.

"As Media Legal Defence Initiative legal director Peter Noorlander told CPJ: ...politicians with a history of corruption could bury old scandals... "These people will be able to kind of cleanse their history so journalists are thrown back 15, 20 years," ..."It is going to make research harder for journalists...In addition to weakening one of journalism's most powerful research tools, the ruling harms journalists by enabling the censorship of links to their work"<sup>85</sup>

Communication has come to stay as the undeniable human desires to explore and connect with one another in a method so determined by one, technologies have strengthened this need and have given it to some an extent irreversible addiction. And more ways to broaden this newfound communication means is only going deepen, as the Information Age is ever evolving and developing. The internet has remained the single biggest push in that regards, and so too, is the trail of cultural imprints humanity leaves behind in the process. Search engines to an extent are now perhaps the custodian of history online as argued by Abramson J.

"Principle that could narrow a person's "right to be forgotten" and make that right compatible with the First Amendment, which is to set expiration dates on personal data, limiting how long such data remains online. As Meg Ambrose has argued, information

---

<sup>83</sup> ibid

<sup>84</sup> ibid

<sup>85</sup> King. G, EU 'right to be forgotten' ruling will corrupt history:, <https://cpj.org/blog/2014/06/eu-right-to-be-forgotten-rul> (01/05/2017)

had a natural life cycle before the Internet, and perhaps even as recently as pre-search engine days. Information's "value depreciated over time" and tended to fade or be forgotten. Insofar as search engines interrupt that life cycle and re-present old personal information out of context, the setting of expiration dates could alleviate the harm."<sup>86</sup>

The internet has become a worldwide culture and a global village thus has become a collective heritage of mankind. To connect and communicate with anyone, anywhere and at any time is made possible with the internet, and more importantly, is the fact that in today's communication, one do not require approvals from anyone to lend a voice, effectively contents are created and distributed in freelance speed with the help of the social media. The era of news media bringing the news to an individual is almost gone, today individuals are taking the news to news media in unprecedented numbers. Breaking news no longer have to come from established news outlets, rather one tweet or podcast or Livestream can tell it all from an eyewitness perspective in real-time.

Consequently, to fully understand how this power has been transferred from an organised establishments to individuals, it is useful to point out how social media has empowered the digital culture. As Chelsea E. Carbone correctly stated, "the internet culture, therefore, evolves specifically because of the global contact it stimulates and creates a melting-pot effect that mirrors the dynamism of the physical world" In that internet culture create an aloof of unending satisfaction and the perceived anonymity user experience while communicating with someone.

This assertion may not exactly be the case especially when the starting point of any form of communication begins by creating an account in the digital environment,"...the Internet can offer a seemingly protected environment for self-discovery and reflection, it also has a permanence and vastness that catches many users off-guard. Whether it's a news article that misrepresented the user (or, perhaps worse, represented the user far more accurately than he or she had hoped), or a posted digital photo depicting the user in a compromising position, the internet's longevity can have drastic and far-reaching effects on a person's personal and professional life. In this context, one could argue a

---

<sup>86</sup> Abramson. J: Searching For Reputation: Reconciling Free Speech And The "Right To Be Forgotten, North Carolina Journal Of Law And Technology pg 72, VOL 17, ISS 1:2015

line should be drawn and protection afforded in respect to certain content or to the users themselves.”<sup>87</sup>

The longevity and vastness of internet communication make it a historical and cultural archiving of mankind, and the fact that it can remain a readable imprint or erasable memorable is now a debate over privacy rights and personal rights over protection of the common cultural heritage of mankind. And the question is: who is the custodian of digital culture and heritage? Do States have the right to force us to keep or erase anything in our private social media accounts and profiles?

A recent court judgement in South Africa forcing a former employee of a company to update his LinkedIn profile also exemplified the question, if companies should have control over what we do on social media. “This was highlighted by the high court in Pretoria yesterday in the case of a city estate agent who was ordered to correct his employment history on professional social media site LinkedIn. The court gave Willem van der Schyff five days within which to remove the details of former employer Daniel Crous Auctioneers from his LinkedIn profile, as it was misleading.

Van Der Schyff left the employment of the auctioneer three years ago, but his LinkedIn profile reflected that he worked there” as reported in Cape Times 9th of March 2017<sup>88</sup>

In respect to this particular case, it is seen that our offline identity, must necessarily reflect our online identity, but was that the idea behind internet revolution? Does that mean that individuals are now responsible for ensuring that their information is updated or the responsibility of the data processors? And in any case, it is a burden for individuals or data processors, to correct and adhere timely in constant data exchange clear reporting and monitoring system. It is simply an unrealistic legalistic argument to assume that all online data of an individual should necessarily correspond to offline

---

<sup>87</sup> Carbone, C.E. To be or Not to be Forgotten: Balancing The Right to Know with The Right to Privacy in The Digital Age. 22nd Virginia Journal of Social Policy and the Law 2015, 531

<sup>88</sup> Venter. Z, Ex-estate agent ordered to correct LinkedIn profile, Cape Times, <http://www.iol.co.za/capetimes/news/ex-estate-agent-ordered-to-correct-linkedin-profile-8120819> (10/04/2017)



data, even internet service providers offer such options as to use a pseudo identity like “username” in order to avoid revealing true offline identity.

However, it is clear that right to be forgotten or not to be forgotten is not an absolute right, it is a right that is often relational, and borne responsibilities and as well as privileges. One of such responsibilities is historical archiving of our online heritage.

### **3.2 Exploitation of Online Identity**

The information society is the new fast moving era and there are no indication that is slowing down. Digital information or data as it were are now becoming even cheaper to collect or store than to delete, and this is what online identity represent for mankind henceforth. While the internet is the medium, personal data is the currency of exchange in the digital world<sup>89</sup> Online identity used to be where anyone can be anything without having to fully provide his or her identity, for it was considered different from the offline identity of an individual.

The famous adage then was “on the internet, nobody knows you are a dog”, that era where real life of oneself is separate from online life has fast faded away. <sup>90</sup> However, the web has witnessed a lot of changes, much of which are engineered by Facebook and Google, the dominant role these social media sites is ever present in all we do today. Facebook have maintained that “authenticity” of user identity online is necessary for the growth and social change expected from a platform like Facebook.

In particular, section 4, subsection 1 of the terms and condition of Facebook states “You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission” <sup>91</sup> though some critics who advocate privacy and personal data protection differs, arguing that such move would limit the openness of the web.

---

<sup>89</sup> Giurgiu. A: Challenges of Regulating A Right to be Forgotten With Particular Reference to Facebook. Masaryk University Journal of Law and Technology, Vol 7:2, 362, 2013

<sup>90</sup> Krotoski. A :Online identity: is authenticity or anonymity more important? The Guardian, <https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity> (20/02/2017)

<sup>91</sup> Registration and Account Security, Terms, Facebook, Section 4:1, <https://www.facebook.com/terms> (20/02/2017)

Today, the need for authenticity have to override every other concern, much of our online activities are linked to social media sites, either Facebook, Google, Instagram, Twitter, LinkedIn, Yahoo, Hotmail, Periscope, Snapchat etc. The web interaction aims to provide some measure of confidence and trust in the platform as Facebook and others envisioned, that person's online are who they say they are, rather than people pretending or posing with a fake identity and acting out who they are not. This, however, makes our online identity non-anonymous, thus our real names, photos, address, email, phone and generally profile have to be who we are in real life, and Facebook and others collect this private data in order to process an online account for the users.

With an account created, some social media site like Facebook also have a partnership with similar players to allow the use of one account to sign up for other services on a different social media site, thus extending our personal data further to a third party.<sup>92</sup> These further advance the idea for the right to be forgotten to dominate argument in the EU, the constant demand and collection of citizens data online especially in most social media site, and the lack of control citizens has once such data is collected to have them immediately deleted or erased without any possibility of surfacing anywhere on the internet ever again. Though, article 6 of Directive 95/46/EC established that such possibility exists once such data is no longer “relevant.”<sup>93</sup>

Current trend globally demonstrates that online identity will remain an evolving and can get complicated in the future, there is no shortcoming of ideas and innovation in this area, most global players in the digital age are investing heavily in new and easier ways to collect and process citizen’s personal data online. Citizen’s data are now the actual assets online marketplace companies has as the source of revenue and capital. Instagram, Facebook and YouTube, for example, depends mostly on ads generated revenues, and ads are driven by the number of subscribers and user’s traffic.

---

<sup>92</sup> Krotoski, A :Online identity: is authenticity or anonymity more important? The Guardian, <https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity> (20/02/2017)

<sup>93</sup> Directive 95/46/EC, Article 6

### 3.3 Social Media and Rule of Law

In furtherance to the fact that social media sites assets are actually personal data, and the risk of privacy individuals incur the moment an account is created on the platforms. The legal power article 17 of the GDPR entrust on citizens is therefore unprecedented. Social media organizations are aware of this fact as they are increasingly under pressure.

In the UK for example, Twitter and Facebook are asked to change their Terms and Conditions and method in which Terms and Conditions are presented to users. "Social networking firms including Facebook and Twitter are being told to make it clearer to members how they collect and use their data..."and that the "terms and conditions are far too long and complex"<sup>94</sup> Andrew Miller MP and Chairman of the Common Science and Technology Select noted that "...serious concerns about the extent to which ticking the 'terms and conditions' box can be said to constitute informed consent when it comes to the varied ways data is now being used by many websites and apps."<sup>95</sup> The committee report concludes that Facebook and Twitter terms and conditions "...have been designed for use in US courtrooms and to protect organisations in the event of legal action rather than to convey information"<sup>96</sup>

On the other hand, it is only imperative that the activities of individuals on social media is balanced between right to protected privacy and abuse of privacy. No doubt that dependency on social media has overtaken traditional and verifiable ways of sourcing for authenticity or accuracy of information. For example, Pew Research Centre found that 7-in-10 Americans get their news from social media and 69% uses some form of social media<sup>97</sup> This figure represent large percentage of American population, and since social media platforms like Twitter, Facebook and Instagram have functions such as "tweet", "post", "comment", "retweet" "like", "share" etc. Therefore, it is no surprise that one tweet or post can be seen by millions in minutes.

If we consider the widespread of such information in minutes, it can be used as

---

<sup>94</sup> Cellan-Jones. R, Social media told to simplify terms and conditions, BBC, <http://www.bbc.com/news/technology-30234789> (02/05/2017)

<sup>95</sup> ibid

<sup>96</sup> ibid

<sup>97</sup> Pew Research Center; <http://www.pewinternet.org/fact-sheet/social-media/> (10/04/2017)

instrument for both good and evil. As Mark A. Cohen stated in a fine piece written for the Forbes “The breadth and impact of social media can scarcely be exaggerated. In less than a decade, it has disrupted journalism, influenced global politics, and altered commerce by providing a platform for instantaneous global communication. One big problem: social media does not distinguish between fact and fiction. This has frightening implications that have already surfaced”<sup>98</sup> Filtering facts from fictions becomes cumbersome to manage, and at what expense is filtering appropriate? Thus, social media has become the most propaganda tool in modern history,”...poses an existential threat to democratic societies and the rule of law.”<sup>99</sup> And can influence public opinions.

On this backdrop, legal instruments have evolved and still evolving to mitigate against some of the consequences of actions in social media intended to defame, mislead and misinformed the public. Among the legal implication for social media abuse is libel; this is a statement of false intended to damage or defames one's reputation. Libel, for example, is punishable under United Kingdom Defamation Act 2013<sup>100</sup> According to an article written by Keir Bakar and published in The Guardian on August 2016, it is observed that 46% of persons 18 to 24-year-old are not aware of the Defamation Act which is also applicable for social media. Unsubstantiated tweets or rumour about another individual can be libellous and punishable under Defamation Act<sup>101</sup>

Social media company such as Twitter, Facebook and Instagram which have features like retweets, share, and repost, these features can still amount to libel claim even when users are innocently and ignorantly retweeting, reposting or sharing false statements, pictures or videos.

It can then amount to an endorsement or sponsoring of falsehood which can trigger a legal action, for ignorant is not an excuse under the law. Libel and internet trolls claims are the most common breaches of law in social media, and many people are the victim

---

<sup>98</sup> Cohen. M.A, Law In The Age Of Social Media, <https://www.forbes.com/sites/markcohen1/2016/11/27/law-in-the-age-of-social-media/#2587f73d1db8> (10/04/2017)

<sup>99</sup> ibid

<sup>100</sup>Defamation Act 2013 [http://www.legislation.gov.uk/ukpga/2013/26/pdfs/ukpga\\_20130026\\_en.pdf](http://www.legislation.gov.uk/ukpga/2013/26/pdfs/ukpga_20130026_en.pdf) (10/04/2017)

<sup>101</sup>Baker. K, Social media law: An essential guide, The Guardian, <https://www.theguardian.com/law/2016/aug/12/social-media-law-an-essential-guide> (12/04/2017)

of the long arms of the law, unaware of the implications of their actions in the social media. The UK hold some of the highest libel and trolls convictions record in Europe. According to UK Ministry of Justice official figures for 2015, five persons are convicted per day.<sup>102</sup> And this figure is as a result of the growing dual purpose of social media as the source of news and communication. UK authority, however, has raised the minimum threshold for a successful prosecution. "Convictions for crimes under a law used to prosecute internet trolls have increased ten-fold in a decade with five a day, official figures reveal...1,209 people were found guilty of offences in social media"<sup>103</sup> in 2014. The figure is expected to rise as access to the internet and social media interconnectivity increase, with new technological devices for communication.

Most of the conviction are based on Section 127(1) of the UK Communications Act 2003<sup>104</sup> which is punishable by up to six-month imprisonment or fine or both. The rationale behind this prosecution figure is not far-fetched given the rise of "Fake News". This further puts strain on interpretation of the GDPR Right to be forgotten.

"Fake News" was the term popularised by US President Donald Trump on social media during the 2016 presidential election and especially during 2017 Trump first press conference as President-elect, where he repeatedly refers to CNN as "Fake News." It is also believed that "Fake News" gave Trump his election victory. President Trump use of the term "Fake News" continues much of the entire period until this moment.



**Donald J. Trump** ✓  
@realDonaldTrump

Follow

After being forced to apologize for its bad and inaccurate coverage of me after winning the election, the FAKE NEWS @nytimes is still lost!

3:39 PM - 4 Feb 2017

17,646 104,031

<sup>102</sup>Five internet trolls a day convicted in UK as figures show ten-fold increase, The Telegraph, <http://www.telegraph.co.uk/news/uknews/law-and-order/11627180/Five-internet-trolls-a-day-convicted-in-UK-as-figures-show-ten-fold-increase.html>

<sup>103</sup> ibid

<sup>104</sup> Section 127, Defamation Act 2013, [http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga\\_20030021\\_en.pdf](http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf) (13/04/2017)

New York Times was also repeatedly referred to as “Fake News” by President Trump on Twitter.

The rise of fake news and fake news outlet is remarkable, but not entirely surprising, owing to the fact that social media helps to spread news story very fast and quickly globally. And most media outlets are increasingly in a hurry to be the first outlet to broadcast a news story or a “breaking news” This has particularly put social media sites under an increased pressure to fact-check news streams on their platforms. Facebook have received the most criticism for not doing enough to check fake stories, spamming, political trolling, hoax etc. And in the bid to prove otherwise, Facebook in April 2017 shut down 30,000 fake accounts in France alone for spreading “Fake News”<sup>105</sup>

As social media sites are now cracking down heavily on users, different governments are also cracking down on social media sites to ensure that their platforms are not used to spread fake news, In Germany for example, the German cabinet recently passed a law that aims to fine social media site up to €50 million if they fail to quickly delete fake news from their sites.<sup>106</sup>

---

<sup>105</sup> Kottasová, I, Facebook Targets 30,000 Fake Accounts in France, <http://money.cnn.com/2017/04/14/media/facebook-fake-news-france-election/> (19/04/2017)

<sup>106</sup>Naughton, J, Facebook and Twitter could pay the price for hate speech, <https://www.theguardian.com/commentisfree/2017/mar/19/john-naughton-germany-fine-social-media-sites-facebook-twitter-hate-speech> (19/04/2017)

## Conclusion

The right to be forgotten stems from Article 8 of Convention for the Protection of Human Rights and Fundamental Freedoms<sup>107</sup> and Charter of Fundamental Rights of The European Union<sup>108</sup> respectively. These are the founding freedoms upon which individual rights was legalised in EU.

The right to be forgotten is one issue that has polarised the legal opinions, and the challenges it poses in actual interpretation and practice is enormous. Judges and all concerns in the matter including policymakers find this new concept problematic. And there are no easy ways around it either. The Google Spain SL v. Agencia Espailola de Proteccion de Datos<sup>109</sup> has demonstrated that even more challenges lie ahead with regard to social media.

The GDPR made a remarkable attempt to address the issue head-on, though Article 17 explicitly mentioned “right to be forgotten” as right EU residents are entitled to when it comes to processing or collecting their personal data by any means. Article 17(1)(a-f) also expresses the conditions upon which violation may occur with collecting personal data, however, it appears very difficult to interpret this Article in case of social media.

When Article 17(2) is examined closely, it states “Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data”<sup>110</sup>

There are grey areas to the wording of the article, first, what exactly does “reasonable

---

<sup>107</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8

<sup>108</sup> Charter of Fundamental Rights of The European Union, Article 8

<sup>109</sup> Google Spain SL v. Agencia Espailola de Proteccion de Datos, CJEU, C-131/12

<sup>110</sup> General Data Protection Regulation, Article 17(2), [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) (24/04/2017)

steps” mean? secondly, when a “data subject” requests to be “erased” by a “controller”, how many “controllers” is the reasonable number to be “inform” by the data controller for this provision to be fulfilled in case the of social media when user(s) have made copies? Who is to be held legally liable if, for the strangest of reasons, the said “erased” personal data resurfaced online?

GDPR shall become applicable in 2018, as it is yet to be tested in the courtrooms. This particular article that focuses on the right to be forgotten will no doubt resonate constantly as EU residents try to enforce their rights. Many of such cases shall arise from social media activities as a great number of EU residents depends on it for communication, news, business, politics. The provision articulated in article 17 requires some case law to be clearly understood, as it is currently worded, it appears to pay attention only to established online marketplaces which have controlled structures on what is uploaded or published, in this stance, only the organization can publish or upload contents to their online platforms. GDPR made no mention of social media or blogs which have become an instrument for spreading information including such personal information “right to be forgotten” sought to protect.

Thus, it becomes a problematic implementation when social media platforms such as Facebook, Instagram, YouTube, Twitter, which contents are actually generated by users, these social media players have little control over contents published or uploaded in their platforms at least in the first few minutes. Article 17 is silent in a situation where a resident who legally seek for personal data to be forgotten for reasons outlined in Article 17(1) (a-f)<sup>111</sup> from a social media site, and the site obliged the legal order and erased such data from its web. Meanwhile another user(s) have made copies or downloads of the said personal data and decided to publish same on a different social media sites or websites for a different reason(s). Does this mean that the second, third, fourth etc. sites that user(s) published the previously erased data are now in breach of this article?

From the standpoint of the right to be forgotten, GDPR offers perhaps an intentional

---

<sup>111</sup> General Data Protection Regulation, Article 17(1)(a-f), [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) (24/04/2017)



ambiguity which the case law should answer regarding what exactly do “forgotten” mean in the context of social media?. And how long is “forgotten” a forgotten, and does “forgotten” applies only to data “controllers” or the World Wide Web? If the latter is the case, then historic archiving of humanity is under threat. As culture is an intrinsic part of everyday existence that can be transferred from one generation to the next, and the internet embedded this cultural archiving. For if all information about a past event is “forgotten” on the ground of this provision, a dangerous trend may ensue among citizens seeking the same right. It is only natural for people to demand damaging or compromising information about them on the Web to be erased. It is left for the court practice to set a defined benchmark with regard to “forgotten.”

Notwithstanding, the GDPR is the boldest up-to-date piece of legislation globally that encapsulated the growing challenge of personal data protection especially on the internet, and that fundamentally entrust citizens and residents within the EU the rights to seek redress with regard to a violation, abuse or misuse of their personal data. It has also placed enormous responsibilities on data controllers and processors. These responsibilities are thorough and stringent, which gives residents some confidence and trust that whenever their data is collected, it follows absolute laid down data security measures enshrined in the GDPR.

It is now up to the Court of Justice of the European Union (CJEU) to brace herself in the futuristic legal fallout from article 17 interpretations as it applies to different scenario especially those relating to social media. It is therefore hoped that CJEU will give teeth to the GDPR in practice and enables a long-lasting precedent on right to be forgotten on social media.

Furthermore, the right to be forgotten, though conceived as an individual inherent right and therefore, should be organised or maintained by an individual based on consent or refusal, this may be considered a narrow view of social justice. "The individual memory cannot be understood as a purely private affair: such memory is not only supported by the memory of the subject but concerns social frameworks and external prostheses, such as speech, writing, signals, rituals, monuments, and shared organizations of space and time. Moreover, by describing the present from the selective reconstruction of the past, individuals define and negotiate their membership to the community, so as to make

their present coherent with the group of which they are a part. Contrary to the abstract representation of the individual as a self-isolated from the rest of the community, every reformulation of the past has to do with a social task. The new meaning of the past shall be comprehensible in light of the conceptual framework with which every community builds its own collective memories. But, more concretely, how should we grasp the connection between individual and collective memories?"<sup>112</sup>

In this vein, conceptualization, of article 17 of the GDPR in terms of practice poses similar concerns, as to what “legitimate ground” and “purpose” amount to since some data are collected even before the intended use. “Describing only the right to be forgotten’s benefits with regard to such values would make a controversial empirical claim absent an empirical warrant. When the effects of the right to be forgotten are analysed in practice, evidence shows that the right creates practical consequences that could, in reality, undermine the ideals it seeks to bolster. For example, the wording of the law itself deleting data when it is “irrelevant or no longer relevant”—leaves the definition of relevance unclear. While some interpret relevance as the point at which data is longer used for its initial purpose, this is “easier said than done... data are also increasingly being collected for yet unknown or rather vague initial purposes, following the logic of data mining that huge data sets can reveal new and unexpected knowledge” One might also find uses for data beyond its original purpose; in such a situation, the data would continue to be relevant but would not be used for its original purpose. Thus, the purpose seems to be a poor criterion for the relevance and possible removal of data.”<sup>113</sup>

Circumstantially, determining when a data is “relevant”, “legitimate” or for the intended “purpose” is problematic, though there are could be ways inferred to know this, but essentially, they too can be very inconsistent. “...measuring relevance,

---

<sup>112</sup> Pagallo. U.,Durante. M., Legal Memories and the Right to Be Forgotten, Law School, University of Turin, Protection of Information and the Right to Privacy – A New Equilibrium?, Law, Governance and Technology Series 17,pg 24, DOI 10.1007/978-3-319-05720-0\_2, <file:///C:/Users/User/Downloads/9783319057194-c1.pdf> (02/05/2017)

<sup>113</sup> Formulating and Implementing a Right to Be Forgotten in the United States: American Approaches to a Law of International Origin Science, Technology, and Society, ST118, pg12, 2015, [https://getinspired.mit.edu/sites/default/files/documents/ST118\\_Report.pdf](https://getinspired.mit.edu/sites/default/files/documents/ST118_Report.pdf) (02/05/2017)

however, are equally flawed”<sup>114</sup>. A...”possibility is to allow the users themselves to determine relevance or to set “expiration dates” for when certain information should be forgotten. After all, it is impossible to algorithmically determine data’s relevance—the feeling of embarrassment is a human one and not measurable by a machine. However, user-generated predictions remain subjective; not only can opinions change as one ages (one may find a certain piece of information embarrassing at one point in his or her life but later grow to embrace it), but data that has become irrelevant at one stage could regain relevance at a later time. To force users to constantly judge the relevance of data seems a tedious and unreliable demand. An alternative form of expiration dates—requiring a one-time prediction of the data’s expiry—is no better. The dynamic nature of personal identity would still be problematic, since, “while one’s sixteen-year-old self might...choose to post certain information...her thirty and even sixty-year-old self (with presumably entirely different notions of what is considered appropriate) will have to live with the consequences of that supposedly ‘informed’ decision”<sup>115</sup>

Fundamentally, the idea most associated with the right to be forgotten, its ability to give him or her a clean start again or the so-called “second chance” in life. This school of thought offers only one side to the argument, thus legally biased as it favours those who have bad past to hide or “forgotten”, consequently, the courts will be flooded with cases essentially seeking a damaging past of an individual to be “forgotten.”

“Advocates of the right to be forgotten often claim that the right to delete or remove the traces of the past, e.g., by subtracting them from the public dominion, allows the individuals to present themselves in a better light, consistent with the current and renewed image that such individuals aim to provide of themselves. Although this argument takes into account the connection between individual and collective memories, it may lead to a new paradox: by dissolving the tie which brings the present back to the past, the risk is to losing out on our own future”<sup>116</sup>

---

<sup>114</sup> *ibid*

<sup>115</sup> *ibid*

<sup>116</sup> Pagallo, U., Durante, M., *Legal Memories and the Right to Be Forgotten*, Law School, University of Turin, *Protection of Information and the Right to Privacy – A New Equilibrium? Law, Governance and Technology Series 17*, pg23, DOI 10.1007/978-3-319-05720-0\_2, <file:///C:/Users/User/Downloads/9783319057194-c1.pdf> (02/05/2017)

## List of Sources

### 1. Scientific Journals

- ❖ Formulating and Implementing a Right to Be Forgotten in the United States: American Approaches to a Law of International Origin Science, Technology, and Society, ST118, pg12, 2015, [https://getinspired.mit.edu/sites/default/files/documents/ST118\\_Report.pdf](https://getinspired.mit.edu/sites/default/files/documents/ST118_Report.pdf)
- ❖ Pagallo. U., Durante. M., Legal Memories and the Right to Be Forgotten, Law School, University of Turin, Protection of Information and the Right to Privacy – A New Equilibrium?, Law, Governance and Technology Series 17, pg 24, DOI 10.1007/978-3-319-05720-0\_2, <file:///C:/Users/User/Downloads/9783319057194-c1.pdf>
- ❖ Abramson, J. Searching for Reputation: Reconciling Free Speech and “Right to be Forgotten” North Carolina Journal of Law and Technology Oct 2015, Vol 17, Iss 1,
- ❖ Abramson. J: Searching For Reputation: Reconciling Free Speech And The "Right To Be Forgotten, North Carolina Journal Of Law And Technology pg 72, VOL 17, ISS 1:2015
- ❖ Abril, P.S., Lipton, J.D. The Right to be Forgotten: Who Decides What the World Forgets? 103 Kentucky Law Journal 2014-2015, 103th 363
- ❖ Ambrose M.L. It’s About Time: Privacy, Information Life cycles, and The right to be Forgotten. Stanford Technology Law Review 2013, Vol 16, 2
- ❖ Antani, R. The Resistance of Memory: Could The European Union’s Right to be Forgotten Exist in The United States? 30 Berkeley Tech. L.J. 1173 2015
- ❖ Bennett, S.C. The "Right to Be Forgotten": Reconciling EU and US Perspectives. 30 Berkeley Journal. International Law. 161 2012
- ❖ Berzins, C. Publicity and Privacy in Administrative Adjudication: A Right to be Forgotten? 39 Advocate. Quarterly. 1 2011-2012
- ❖ Carbone, C.E. To be or Not to be Forgotten: Balancing The Right to Know with The Right to Privacy in The Digital Age. 22nd Virginia Journal of Social Policy and the Law 2015, 525
- ❖ Castellano, P. S. A Test for Data Protection Rights Effectiveness: Charting the Future of the 'Right to be Forgotten' Under European Law. Columbia Journal of

- ❖ Forde, A. Implications of the Right To Be Forgotten. *Tul. J. Tech. & Intell. Prop* 2015. 18, 83
- ❖ Giurgiu, A., Challenges of Regulating a Right To Be Forgotten With Particular Reference To Facebook. *7 Masaryk University Journal Law and Technology*. 361 2013
- ❖ Gündoğan. C.O., Will Facebook Remember You Forever: The Right To Be Forgotten On Social Networks Within The Privacy Framework, *University Of Essex*, pg 42, [https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FTez%2FCigdem\\_OZER\\_GUNDOGAN.pdf](https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FTez%2FCigdem_OZER_GUNDOGAN.pdf) (01/05/2017)
- ❖ Kulk, S., Borgesius, F.Z. Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain. *European Data Protection Law Revised*. 2015, 178
- ❖ Lobbying Document by "Facebook" (2012), Facebook's views on the proposed data protection regulation (summary by europe-v-facebook.org), Published by europe-v-facebook.org, p.6-7, [http://www.europe-v-facebook.org/FOI\\_Facebook\\_Lobbying.pdf](http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf) (01/05/2017)
- ❖ McGoldrick, D., Developments in the Right to be forgotten. *Human Rights Law Review* 13:4 2013; Oxford University Press.
- ❖ Messenger, A. What Would a "Right to Be Forgotten" Mean for Media in the United States? *Comm. Law* 2012-2013, 29
- ❖ Miller, D., et al, How the World Changed Social Media, University College London, UCL Press, pg xi, 2016, <http://discovery.ucl.ac.uk/1474805/1/How-the-World-Changed-Social-Media.pdf>
- ❖ O'Hara, K., Shadbolt, N. The Right to be Forgotten: Its Potential Role in a Coherent Privacy Regime. *European Data Protection Law Revised*. 2015, 113
- ❖ Powles, J., The Case That Won't Be Forgotten. *47 Loyola University Chicago. Law Journal*, 583, 2015-2016
- ❖ Rustad, M.L and Kulevska, S. Reconceptualizing The Right To Be Forgotten To Enable TransAtlantic Data Flow. *Harvard Journal of Law & Technology* 2015, Vol 28,2
- ❖ Shoor, E.A., Narrowing The Right To Be Forgotten: Why The European Union

Needs To Amend The Proposed Data Protection Regulation. 39 Brook. J. Int'l L. 487 2014

- ❖ Siry, L. Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten. 103 Kentucky Law Journal 2014-2015, 311
- ❖ Wechsler, S., The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten. 49 Columbia Journal Law and Social Problems. 135, 2015-2016

## **2 International Conventions and Legal Acts**

- Charter Of Fundamental Rights Of The European Union, 2012/C 326/02
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 1, Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention 108], available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
- Data Controllers and Data Processors: What the Difference is and What the Governance Implications are: Information Commissioner's Office. <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (20/04/2017)
- European Convention on Human Rights, 1953
- [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC) (11/10/2016)
- [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC) (12/10/2016)
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (12/10/2016)
- International Covenant on Civil and Political Rights 1966
- Introduction to Social Media, Australian Communications Consumer Action Network (ACCAN), Australia's peak body representing communications consumers, 2007. [https://accan.org.au/files/Tip%20Sheets/Introduction%20to%](https://accan.org.au/files/Tip%20Sheets/Introduction%20to%20)

20Social%20Media.pdf(01/05/2017)

- Proposal for a Regulation on Privacy and Electronic Communications. <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications> (18/02/2017)
- Social Media Fact Sheet, Pew Research Center; <http://www.pewinternet.org/fact-sheet/social-media/> (10/04/2017)
- The General Data Protection Regulation, [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)
- The Universal Declaration of Human Rights, United Nations, 1948

### 3 Case Laws

- Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, C-131/12
- Maximilian Schrems v Data Protection Commissioner, CJEU, C-362/14

### 4 Other Sources

- BBC World Service, Finland makes Broadband a Legal Right 2010 <http://www.bbc.co.uk/news/10461048> (13/10/2016)
- EuroStat [http://ec.europa.eu/eurostat/statistics-explained/index.php/Population\\_and\\_population\\_change\\_statistics#EU-28\\_population\\_continues\\_to\\_grow](http://ec.europa.eu/eurostat/statistics-explained/index.php/Population_and_population_change_statistics#EU-28_population_continues_to_grow)
- Macaskill, E., Dance G. Produced by Cage, F., Chen. G, The Guardian, 2013 <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> (13/11/2016)
- Manual for Measuring ICT Access and Use by Households and Individuals. International Telecommunication Union (ITU). <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (13/10/2016)
- The GDPR and You, General Data Protection Regulation, Preparing for 2018, Data Protection Commissioner, Irish Government <https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf>

- Annexes



**Donald J. Trump** ✓

@realDonaldTrump

 Follow

After being forced to apologize for its bad and inaccurate coverage of me after winning the election, the FAKE NEWS @nytimes is still lost!

3:39 PM - 4 Feb 2017

  17,646  104,031

Twitter.com