DATA PROTECTION IN KENYA: THE CASE OF THE RIGHT TO BE FORGOTTEN

MOTURI ELIZABETH OBEGI

ADM. No. 072477

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LL.B) OF STRATHMORE UNIVERSITY

STRATHMORE LAW SCHOOL

JANUARY 2016

CONTENTS

DEDICATION

To God for giving me the strength and patience to do this dissertation and my mother for pushing me to be the best that I can be.

ACKNOWLEDGMENTS

I would like to acknowledge my supervisor Mr. Douglas Gichuki for his guidance, insight and advice and my classmates for their support.

DECLARATION

I declare that this work has not been submitted or approved for the award of a degree by this or any other university.

Signature: _____ Date: 24th March, 2016

Moturi Elizabeth Obegi

Adm. No. 072477

University Supervisor:

This dissertation has been submitted with my approval

Signature: _____ Date: 24/03/16

Mr. Douglas Gichuki

Strathmore Law School

ABSTRACT

The right to be forgotten is a data protection right that enables an individual to have personal data concerning themselves removed from the internet. Data Protection laws in Kenya are insufficient. The Data Protection Bill which was first drafted in 2008 is yet to be enacted in 2016. The internet has today become an important tool for many Kenyans that is used everyday yet there are insufficient laws to protect the data that they leave on the internet. In this paper I seek to determine whether Kenya should adopt the right to be forgotten. I examine the data protection laws in other countries to examine what a data protection right should entail. Then I look at the proposed right to be forgotten legislation and why the right to be forgotten is an important right. Finally I examine the situation in Kenya and find that there is a need for better Data Protection laws; even the right to be forgotten upon examination of the Data Protection Bill is insufficient. Not only do they not provide for the right to be forgotten or the right to erasure, it also fails to establish a regulatory authority to ensure compliance with the legislation. For these reasons I recommend that the Data Protection Bill should be amended to include the right to be forgotten and a proper regulatory authority should be set up under the Act. I also recommend that Data Protection should be a concern for the law makers who should amend the Bill and pass it.

LIST OF ABBREVIATIONS

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
EU	European Union
EUCJ	European Union Court of Justice
FSA	Financial Services Authority
ICCPR	International Covenant on Civil and Political Rights
IMP	Internet Message Processor
NHIF	National Health Insurance Fund
NSSF	National Social Security Fund
UDHR	Universal Declaration of Human Rights
UGC	User Generated Content
UK	United Kingdom

LIST OF STATUTES

1. *African Charter on Human and People's Rights,* 21 October 1986.
2. *African Union Convention on Cyber Security and Personal Data Protection,* 27 June 2014, *EX.CL/846(XXV).*
3. *Charter of Fundamental Rights of The European Union*, 2012/C 326/02.
4. *Constitution of Kenya*, (2010).
5. *Data Protection Directive*, 95/46/EC.
6. *Data Protection Act* CAP 29 of 1998 (UK).
7. *International Covenant on Civil and Political Rights*, 23 March 1976, 999 UNTS 171
8. Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (2012).
9. *The Universal Declaration of Human Rights*, 10 December 1948.

LIST OF CASES

1. *Bodil Lindqvist,* EUCJ Judgement of 6 November 2003.
2. *Durant v Financial Services Authority* [2003] EWCA Civ 1746.
3. *R v Brown* [1996] All ER, 555-556.
4. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* EUCJ Judgement of 13 May 2014.

I. CHAPTER1 INTRODUCTION

A. Background

The Right to be forgotten was established in Europe in a case that was brought by a Spanish man, Mario Costeja González, against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc. The Spaniard had requested the removal of a link to a digitized 1998 article in *La Vanguardia* newspaper about an auction for his foreclosed home, for a debt that he had subsequently paid. He went to court seeking that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared and that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results. The court held that individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them.[1] The right to be forgotten is a data protection right designed to enable a person to delete personal data on the internet when they no longer want the data retained and where there is no good reason for the data to be retained.[2]

The European Union has since then developed the draft Data Protection Regulation which explicitly provides for the right to be forgotten in article 17.[3]

The right to be forgotten goes hand in hand with the right to privacy as stated in the Constitution of Kenya. Article 31(c) gives Kenyans the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. The right to be forgotten protects this right but on the internet. .[4]

B. Statement of problem

The internet has become a part of many Kenyans lives. A study done over a period of 3 months by Portland communications, found that Nairobi is the most active city in East

---

[1] *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, EUCJ Case Ruling of 13 May 2014

[2] Murray A, *Information Technology Law: The Law and Society*, Oxford University Press, Oxford, 2013, 517.

[3] Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (2012).

[4] Article 31(c), *Constitution of Kenya*, 2010.

Africa and the sixth most active on the continent, with 123,078 geo-located tweets.[5] Kenyans are constantly sharing their lives online and giving up information about themselves and about others on the internet. In Kenya at the moment there is insufficient protection for Kenyans on the internet. There is a draft Data Protection Bill[6] which seeks to protect personal data from collection and processing. .

Given the ever growing use of the internet in Kenya, the laws in Kenya are insufficient to protect their personal data. Therefore in my paper I will be examining whether Kenya should adopt the right to be forgotten.

C. Research questions

i. What does a data protection legal framework contain?
ii. What is the right to be forgotten?
iii. Should the right to be forgotten be recognised in Kenya?

D. Limitations of study

The research will be based on the Geographical Region of Kenya however the research will involve looking at the situation in other countries that recognise the right to be forgotten because Kenya does not.

E. Literature review

The European Union has developed the draft Data Protection Regulation which explicitly provides for the right to be forgotten in article 17.[7] European Commissioner Viviane Reding[8] mentions the right as an element of the review of the Data Protection Directive (95/46/EC), which envisions strengthening the "right to be forgotten", i.e. the right of individuals to have their data fully removed when they are no longer needed for the purposes for which they were collected or when he or she withdraws consent.[9]

---

[5] : http://www.portland-communications.com/publications/how-africa-tweets-2014/#sthash.bGvnQNpU.dpuf on 13 February, 2015.
[6] Data Protection Bill, 2013
[7] Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (2012).
[8] Reding V, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, 5 *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF on 12 February, 2015.
[9] Reding V, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, 5 *available at*

We live in a world where information is constantly being collected which leads to a situation where there is a lot of information out there collected with or without our knowledge. This influx of information has been given the name 'Big Data'. Koops BJ opines that 'Big Data', consists of an accumulation of two types of data: digital footprints, i.e., data created by users themselves, and data shadows, i.e., data generated about users by others. [10]

In an article titled 'The right to be forgotten in the internet era' the writers stated that the Internet has been steadily evolving from a practically entirely 'free' network into a primarily commercial environment. In this new setting, personal data has become the major currency. The unbridled desires to accumulate this currency and the limitless data collection capacities of modern technology have caused a significant power shift between data users and data subjects. On the Internet, the latter are virtually powerless against the former.[11] This causes a conflict between the data users and the data subjects.

There are two ways to implement the right to be forgotten: a dominant perspective stressing that personal data should be deleted in due time, and two minority "clean-slate" visions: a social perspective that outdated negative information should not be used against people, and an individual self-development perspective that people should feel unrestrained in expressing themselves in the here and now, without fear of future consequences.[12]

On the other hand Rossen J[13] is of the opinion that the right to be forgotten in fact represents the biggest threat to free speech on the Internet in the coming decade because it could transform Google, for example, into a censorian- chief for the European Union, rather than a neutral platform. And because this is a role Google won't want to play, it may instead produce blank pages whenever a European user types in the name of someone who has objected to a nasty blog post or status update.[14]

---

http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF on 12 February, 2015.

[10] Koops BJ, 'Forgetting Footprints, Shunning Shadows, 8.

[11] Graux H, Ausloos J and Valcke P, 'The right to be forgotten in the internet era', *ICRI Working Paper* (2012), 7

[12] Koops BJ, 'Forgetting Footprints, Shunning Shadows, 6.

[13] Rossen J, 'The Right to be forgotten', *Stanford Law Review Online,* (2012)

[14] Rossen J, 'The Right to be forgotten', 92.

F. Hypothesis

The right to be forgotten is important right which should be granted to Kenyans in order to properly protect Kenyans right to privacy on the internet.

G. Chapter Breakdown

In the second chapter I will look at the right to privacy as the basis for data protection laws.

In Chapter 3 I will give a short overview of the internet, web 2.0 and big data in order to illustrate the data problem.

I will then look at data protection laws and the authorities involved in Chapter 4 of this paper.

In Chapter 5 I will examine the scope and application of the right to be forgotten.

Chapter 6 will then look at the atmosphere in Kenya and determine whether the right to be forgotten can be and should be adopted in Kenya. Chapter 7 will be my concluding chapter where I will summarise my findings and give recommendations.

II. CHAPTER 2: THE RIGHT TO PRIVACY

> *"My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual... Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat."*[15]
>
> Lord Hoffman

The data protection rights stem from the need to protect individual's right to privacy on the internet. The right to privacy is therefore the backbone of data protection rights of which the right to be forgotten is a part of. In this chapter I will highlight the theories regarding the meaning of the right to privacy and highlight the international and domestic instruments that contain the right to privacy. Finally I will attempt to describe why the right to privacy is important.

A. Conceptual framework

The right to privacy is the right an individual person has to control the extent to which personal information is disseminated to others.[16] Samuel D. Warren[17] and Louis D. Brandeis[18] referred to the right to privacy as the right "to be let alone."[19] The right to be let alone was itself part of an even more general right, the right to enjoy life, which was in turn part of the individual's fundamental right to life itself.[20]

John Locke opined that there are laws of nature one of them being the right to life. In his Second Treatise of Government[21] he wrote:

> *"The state of nature has a law of nature to govern it, which obliges every one: and reason, which is that law, teaches all mankind, who will but consult it, that being*

---

[15] *R v Brown* [1996] All ER, 555-556.
[16] Lloyd IJ, *Information Technology Law*, Oxford University Press, Oxford, 2008, 7.
[17] Warren SD and Brandeis LD, 'The Right to Privacy' *Harvard Law Review*, (1890).
[18] Warren SD and Brandeis LD, 'The Right to Privacy' *Harvard Law Review*, (1890).
[19] Warren SD and Brandeis LD, 'The Right to Privacy' , 195.
[20] Glancy JD, 'The Invention of the Right to Privacy', *Arizona Law Review* ,(1979), 3.
[21] Locke J, *The Second treatise of Government*, Hacket Publishing Company, Indanopolis, 1980.

all equal and independent, no one ought to harm another in his life, health, liberty, or possessions."[22]

The right to privacy finds its origins in individualism where the individual has a right of self-determination which means they have the right to decide which parts of their personal lives to share and which parts to keep to themselves.[23] John Stuart Mill stated in his essay on Liberty that... *"the only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign."*[24]

A number of theorists conceptualize privacy as "limited access" to the self.[25] This conception recognizes the individual's desire for concealment and for being apart from others. E.L. Godkin observed that "nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion."[26]

There is also the concept of privacy as secrecy.[27] When talking about privacy as secrecy, Judge Richard Posner defines it as an individual's "right to conceal discreditable facts about himself." Posner sees privacy as a form of self-interested economic behaviour, concealing true but harmful facts about oneself for one's own gain.[28]

There is the predominant conception of privacy which is the control over personal information.[29] According to Alan Westin: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[30]

---

[22] Locke J, *The Second treatise of Government*, Hacket Publishing Company, Indianapolis, 1980, Chapter .II. Of Property, Sect. 6.
[23] Glancy JD, 'The Invention of the Right to Privacy', 21.
[24] Mill JS, Essay on Liberty, available at http://www.constitution.org/jsm/liberty.htm on 04th March, 2015.
[25] Solove DJ, 'Conceptualizing Privacy', California Law Review, (2002), 1102.
[26] Solove DJ, 'Conceptualizing Privacy', 1103.
[27] Solove DJ, 'Conceptualizing Privacy', 1105.
[28] Solove DJ, 'Conceptualizing Privacy', 1106.
[29] Solove DJ, 'Conceptualizing Privacy', 1109.
[30] Solove DJ, 'Conceptualizing Privacy', 1110.

Building on Warren's and Brandeis's notion of privacy, Paul Freund came up with the terms "personhood" to refer attributes of a person that are irreducible in his selfhood. From this he viewed privacy as a form of protecting personhood. [31]

Another theory of privacy understands it as a form of intimacy. This theory recognizes that privacy is not just essential to individual self-creation, but also to human relationships. One virtue of privacy as intimacy is that it "expand[s] moral personhood beyond simple rational autonomy."[32]

B. The right to privacy as a statutory right

The right to privacy was first recognised internationally under The Universal Declaration of Human Rights (UDHR).[33] Article 12 states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.[34]The UDHR also provides that everyone has the right to the protection of the law against such interference or attacks.[35]

The right to privacy is also found in the International Covenant on Civil and Political Rights (ICCPR). [36] It states at article 17(1) that 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. It goes on to state at 17(2) that everyone has the right to the protection of the law against such interference or attacks.[37]

In Africa, the right is contained in Article 4 of the African Charter on Human and People's Rights. It states that every human being shall be entitled to respect for his life and the integrity of his person.[38]

In Kenya the right to privacy is firmly placed in the Constitution. Article 31(c) states that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed.[39]

---

[31] Solove DJ, 'Conceptualizing Privacy', 1116.
[32] Solove DJ, 'Conceptualizing Privacy', 1121.
[33] *The Universal Declaration of Human Rights.*
[34] Article 12(1), *The Universal Declaration of Human Rights*, 10 December 1948.
[35] Article 12(2)*The Universal Declaration of Human Rights.*
[36] *International Covenant on Civil and Political Rights*, 23 March 1976, 999 UNTS 171.
[37] Article 17, *International Covenant on Civil and Political Rights.*
[38] Article 4, *African Charter on Human and People's Rights,* 21 October 1986.
[39] Article 31(1), *Constitution of Kenya*, (2010).

In Europe the European Union has gone a step further. In addition to the right to privacy[40] in the Charter of Fundamental Rights of The European Union, at article 8 it includes the right to protection of personal data concerning him or her.

C. Why is the right to privacy important?

The need for privacy is a socially created need. [41] Society is fraught with conflict and friction therefore, individuals, institutions, and governments can all engage in activities that have problematic effects on the lives of others. Privacy acts as relief from a range of all kinds of social friction enabling people to engage in worthwhile activities in ways that they would otherwise find difficult or impossible.[42]

The right to privacy is not an individual right but a social right created to protect the individual for the sake of society. [43] This is due to the fact that it emerges from a set of social norms therefore it is an internal dimension of society. [44]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[45]

The sources of receiving and generating personal data have increased. Information that is usually private such as health information is now on the internet. Information can also be generated on the internet about an individual based on their searches. For example it can be deduced if someone purchases a book on Amazon regarding Breast cancer that either that person or someone close to them has Breast cancer.[46]

The right to privacy is an important right for the individual and society. This is why it is found in the Universal Declaration of Human Rights and the other international conventions stated above. Therefore, the right to privacy should be protected on the internet.

---

[40] *Charter of Fundamental Rights of The European Union*, 2012/C 326/02, article 7.
[41] Solove DJ, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* (2006), 484- 485.
[42] Solove DJ, 'A Taxonomy of Privacy',, 484- 485.
[43] Solove DJ, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *San Diego Law Review* (2007), 763.
[44] Solove DJ, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy,763.
[45] Article 17, Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation.
[46] Crawford K, Schultz J, 'Big Data And Due Process: Toward a Framework To Redress Predictive Privacy Harms', *Public Law & Legal Theory Research Paper Series Working Paper No. 13-64* (2013), 97.

III. CHAPTER 3: THE INTERNET, WEB 2.0 AND BIG DATA

A. An introduction to the internet

On 4th October 1957, the Soviet Union launched the first man- made object into space, the satellite Sputnik I. This shocked and surprised the United States and President Eisenhower determined that the US would never be taken by surprise on a technological frontier. Therefore he created a new agency directly tied to the office of the President which would oversee cutting edge research of value to both the military and civilian establishments. This organisation was named Advanced Research Projects Agency or ARPA.[47] One of the first problems that ARPA had was how to create a network of machines which would allow researchers in different parts of the country to share results and resources easily.[48] ARPA appointed J. C. R Licklider[49], an eminent experimental psychologist and a professor at the Massachusetts Institute of Technology, to deal with that problem.[50] Licklider and his team set out to build a system of computer networks which would be known as Advanced Research Projects Agency Network or ARPANET.[51]

Leonard Kleinrock[52] who was part of the team at ARPA was convinced that the best way to connect computers on a network was to use packet switching instead of circuit switching which is used by traditional telephones.[53] Packet Switching was developed by Paul Baran, who was contracted in the 1960's by the United States government to explore a secure telecommunication system because they feared that the telephone communication system used by the military could be destroyed by a nuclear attack.[54] Baran first studied the telecommunication system at the time developed by AT&T and found that the system it had built would not withstand a nuclear attack. The network was too concentrated and had no effective redundancy. So he decided to press his idea for a different telecommunications system.[55]

---

[47] Murray A, *Information Technology Law: The Law and Society,* Oxford University Press, Oxford, 2013, 16.
[48] Murray A, *Information Technology Law: The Law and Society*, 16.
[49] Murray A, *Information Technology Law: The Law and Society*, 16.
[50] Murray A, *Information Technology Law: The Law and Society*, 15.
[51] Murray A, *Information Technology Law: The Law and Society*, 17.
[52] Murray A, *Information Technology Law: The Law and Society*, 17.
[53] Murray A, *Information Technology Law: The Law and Society*, 17.
[54] Lessig L, *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, New York, 2001, 26.
[55] Lessig L, *The Future of Ideas: The Fate of the Commons in a Connected World*, 31.

Baran's idea was to digitize a conversation translating it from waves to bits—and then chop the resulting stream into packets, these packets could flow independently across a network and create the impression of a real-time connection on the other end. As long as they flowed fast enough, and the computers at both ends were quick, the conversation encoded in this packet form would seem just like a conversation along a single virtual wire across the ocean.[56]

ARPA set out to create their network using the packet switching system.[57] ARPA then had to create a way to make the computers compatible with one another because the computers in the 1960s did not have similar operating systems like Microsoft.[58]To solve this problem they created the interface message processor or IMP which would be connected to each computer which would act as the interface between the host computer and the network.[59]

The ARPANET was then created and comprised of two layers, the packet- switching model and the IMPs to support the host computers.[60] This was the first successful network but it was one single network that was a closed network only opened to those who had an IMP.[61]

After the invention of the ARPANET other independent networks were developed for example ALOHANET developed by Professor Norm Abramson of the university of Hawaii and the SATNET developed by the US, UK and Norway.[62] These networks however used different transmissions. There was need to connect these networks in order to share information therefore Bob Kahn set out to create a network of networks to connect all the independent networks.[63] This led to the development of the TCP/IP which is the system of communication rules (protocol) used for exchanging data between computers on the Internet.[64]

Today the internet has been understood to comprise of three layers. At the bottom is a "physical" layer which comprises of the computer, or wires, that link computers on the Internet. This is the hardware across which communications travel. The second layer in the

---

[56] Lessig L, *The Future of Ideas: The Fate of the Commons in a Connected World*, 31.
[57] Murray A, *Information Technology Law: The Law and Society*, 17.
[58] Murray A, *Information Technology Law: The Law and Society*, 17.
[59] Murray A, *Information Technology Law: The Law and Society*, 17.
[60] Murray A, *Information Technology Law: The Law and Society*, 17.
[61] Murray A, *Information Technology Law: The Law and Society*, 18.
[62] Murray A, *Information Technology Law: The Law and Society*, 18-19.
[63] Murray A, *Information Technology Law: The Law and Society*, 19.
[64] Murray A, *Information Technology Law: The Law and Society*, 21.

middle is the code that makes the hardware run and includes the protocols of the internet and the software on which these protocols run. At the top is the "content layer" which is the actual information that gets transmitted across the wires. These three layers function together to define any particular communications system.[65]

The internet was designed to be free and open, there is no centralized control and no one can turn it off.[66] The Internet Protocol suite (IP) was designed to follow the end-to-end principle, The principle suggests that the protocol should be indifferent both to the physical communications medium "below" it, and the applications running "above" it.[67] The End-to-End discourages forcing any service, feature, or restriction on the customer and letting his/her applications what features it needs, and whether or not to provide those features itself.

B. Big data

'Big Data' refers to the influx of information generated on the internet. 'Big Data', consists of an accumulation of two types of data: digital footprints, i.e., data created by users themselves, and data shadows, i.e., data generated about users by others. [68]

The new technology that follows the Web 2.0 model makes it possible for users to become participants in the production of their information environment rather that relying on mass media to produce all the content for passive consumers. [69]

The term "Web 2.0" is used to convey a set of principles and practices that describe a second generation (from the traditional Web 1.0) of web services mainly concerned with user collaboration and sharing.[70]Web 2.0 applications are those that deliver software as a continually-updated service that gets better the more people use it, consuming and

---

[65] Benkler Y, 'From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access' *Yale Law Journal,* (2000), 562.
[66] Carpenter B.E, *Architectural Principles of the Internet* (1996) https://www.ietf.org/rfc/rfc1958.txt on 17 December, 2015, 3.
[67] Wu T, 'Network neutrality, broadband discrimination', *Journal of Telecommunications and High Technology Law* (2003), 146.
[68] Koops BJ, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series*, (2012), 8.
[69] Benkler Y, 'From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access' *Yale Law Journal,* (2000), 562.
[70] George C and Scerri J , '*Web 20 and User-Generated Content: legal challenges in the new frontier'*, Journal of Information, Law and Technology, (2007), 3.

remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others.[71]

Data created by the individual is what is as a result of user generated content. User Generated Content (UGC), also known as consumer-generated media (CGM), refers to any material created and uploaded to the Internet by non-media professionals. The earliest forms of UGC arrived in 1980 with Usenet, a global discussion network that allowed users to share comments and experiences of a given topic.[72]

User- generated internet includes blogs, wikis, multimedia sharing services (Flickr, YouTube, Vine), content syndication, podcasting, content tagging services, social networking and professional networking, aggregation services (bringing all feeds, news and email to a single web page, e.g. www.techmeme.com), data 'mash-ups' (putting together data from difference sources to create a new service, e.g. www.housingmaps.com), tracking and filtering content (tracks and filters content from blogs and other sharing services, e.g. www.digg.com), collaborating (collaborative reference works e.g. www.squidoo.com); Web-based desktop application/document tools (e.g. www.stikkit.com); and sourcing ideas or working from a crowd.[73] The advent of blogs was considered a tipping point for UGC. It was the moment when UGC went from a small but significant component of the Internet experience to a predominant source of entertainment, information and debate.[74] It did so by incorporating user comments in the blog material.

Wikis are one of the largest UGC resources such as Wikipedia, which is the largest encyclopaedia ever. Social media allows participation on a mass scale, thus encourages UGC.

---

[71] George C and Scerri J , *'Web 20 and User-Generated Content: legal challenges in the new frontier'*, Journal of Information, Law and Technology, (2007), 3.
[72] Interactive Advertising Bureau, *IAB Platform Status Report: User Generated Content, Social Media and Advertising – An Overview*, (April 2008), 1.
[73] George C and Scerri J , *Web 2.0 and User-Generated Content, 4.*
[74] Interactive Advertising Bureau, *IAB Platform Status Report: User Generated Content, Social Media and Advertising – An Overview*, (April 2008), 4.

Video itself has moved from private enclaves and paid subscriptions toward a vast, rich, sharable sea of high quality content.[75]

The data created by users about others is usually collected by public and private entities without the users knowledge. Private companies are notorious for this practice. Google for example stores all individual search queries, not for an indeterminate period, and they are able to profile web users in great detail. Facebook also collects huge amounts of data about people's preferences through cookies, not only of Facebook users themselves but also of non-members who simply visit a page that contains Facebook's "Like this" button, even without clicking the button."[76]

Data collection is also done for the purposes of public- policy in the interest of security justice and other public policy concerns. The EU has eighteen major initiatives and large-scale database systems involving millions of people and data-processing operations. In the US alone, there are 2000 police databases.[77]Kenya has also began collecting data about their citizens which I will examine in Chapter 5 of this dissertation.

Google also does something they refer to as crawling. 'Crawling' is generally understood as the use of software programs that make requests for online material. These programs, also referred to as 'crawlers' or 'spiders', are configured to look for information on the Internet, 'according to a set of criteria which tell it where to go and when'. Once the relevant web pages have been fetched (i.e. a copy has been collected), their content is analyzed and parsed for purposes of indexation. Google compares its search engine index to an index found in the back of a book, in that it 'includes information about words and their locations'. It is this index which is consulted when a search engine user enters a search query.[78]

The Internet has been steadily evolving from a practically entirely 'free' network into a primarily commercial environment. In this new setting, personal data has become the major currency. The unbridled desires to accumulate this currency and the limitless data collection capacities of modern technology have caused a significant power shift between

---

[75] User-generated content is dead – as video evolves, available at http://www.forbes.com/sites/stevenrosenbaum/2014/07/14/user-generated-content-is-dead-as-video-evolves/ (accessed on 25/7/2015).

[76] Koops BJ, 'Forgetting Footprints, Shunning Shadows, 8.

[77] Koops BJ, 'Forgetting Footprints, Shunning Shadows, 7.

[78] Van Alsenoy B, Kuczerawy A and Ausloos J, 'Search engines after Google Spain: internet@liberty or privacy@peril? ' ICRI Working Paper 15 (2013) , 11.

data users and data subjects. On the Internet, the latter are virtually powerless against the former.[79]

This influx of data on the internet has lead to the development of data protection laws. In the next chapter I will examine those laws in order to determine what they entail.

[79] Graux H, Ausloos J and Valcke P, 'The right to be forgotten in the internet era', ICRI Working Paper (2012), 7.

IV. CHAPTER 4: THE SCOPE OF DATA PROTECTION

To understand the scope of data protection I will examine what kind of data is protected data processing, the data controller, and the supervision of data protection. Kenya is yet to enact a data protection law therefore I will be examining the legislation in the European Union because the European Union has taken a firm stance on data protection and the United Kingdom because like Kenya they are a common law jurisdiction.

A. Protected data

Data protection legislation has been directed towards the protection of personal data. The European Union came up with the 1995 Directive[80] on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 1(1) places an obligation on Member states to protect fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.[81]

1. Personal data

Personal data is described in article 2(a) of the Data Directive 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.'*[82]

In the United Kingdom Data Protection Act 1998 the term personal data also extends to any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[83]

The Data Protection Directive also adds a category of personal data which they refer to as special categories of data. These special categories include personal data revealing racial

[80] EU *Data Protection Directive*, 95/46/EC.
[81] Article 1(1), EU *Data Protection Directive*, 95/46/EC.
[82] Article 2(a), EU *Data Protection Directive*, 95/46/EC.
[83] Section 1(1), *Data Protection Act* CAP 29 of 1998 (UK).

or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[84]

The UK act refers to these special categories as sensitive personal data and subjects its processing to more extensive requirements.[85] In addition to the categories in the Data Protection Directive the UK Act also refers to the commission or alleged commission of an offence or any proceedings for any offence as a special category.[86]

The scope of what constitutes a special category has been interpreted by the courts in a rather broad manner. In the case of *Bodil Lindqvist*[87], the European Court of Justice was asked to give a preliminary ruling in response to a number of questions posed by the Swedish courts. Mrs Lindqvist had been convicted of breaches of the Swedish data protection law in respect of her work as a catechist in the Swedish Lutheran Church and preparation of a number of WWW pages which contained information about Mrs Lindqvist and eighteen of her parish colleagues, including brief details of the nature of their work and hobbies. It appears that much of the information was presented in what was intended to be a light-hearted manner. The item of information which caused a potential risk to an individual's data protection right was the indication that a named person had injured her foot and as a consequence was able to work only on a part-time basis. Mrs Lindqvist was prosecuted by the Swedish authorities on a number of charges, including one of processing sensitive personal data without having secured authorisation from the data protection authorities. The European Court of Justice was asked to rule on the question of whether the reference to the foot injury of Mrs Lindqvist's colleague constituted sensitive data relating to health. The court's reply was succinct and emphatic:

> *"In the light of the purpose of the Directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual".*[88]

---

[84] Article 8(1), EU *Data Protection Directive*, 95/46/EC.
[85] Lloyd IJ, *Information Technology Law*, 42.
[86] Section 2, *Data Protection Act* CAP 29 of 1998 (UK).
[87] EUCJ, Judgement of 6 November 2003.
[88] *Bodil Lindqvist case.*

2. Data relating to an identifiable person

Article 2(a) of the directive specifies that the personal data is that which relates to an identifiable person.

According to the Article 29 Working Party, data relates to an individual:

> "*if it refers to the identity, characteristics or behaviour of an individual, or if such information is used to determine or influence the way in which that person is treated or evaluated*".[89]

What does it mean for data to relate to the subject? This was discussed in the case of *Durant v Financial Services Authority*[90]. The appellant had been involved in a protracted dispute with Barclays Bank. This had resulted in unsuccessful litigation in 1993 and a continuing course of complaints to the industry regulatory body, the Financial Services Authority (FSA). The present case arose from a request from the appellant for access to a range of records under the ambit of the subject access provisions of the Data Protection Act 1998. Although some information was supplied, access to other records was provided only in partial form through the concealment or redaction of information which it was considered related to third parties. Other records were withheld on the grounds either that the information contained therein did not constitute personal data relating to the appellant, or—as will be discussed below, in the case of a number of records which were maintained in manual filing systems—that the system was not covered by the Data Protection Act.

Although there was no doubt that much, if not all, of the data in question had been generated following complaints from the appellant, the critical issue was whether it related to him.

The Court of Appeal adopted a restrictive interpretation. The court found that the right was put in place to enable the data subject to ensure that the data processing did not infringe on their rights but not to give an automatic right to access information by virtue of the fact that he might be named in a record or have some interest in the matters covered. [91]

Therefore, the mere fact that a search of a computer's contents by reference to a data subject's name revealed a number of documents did not mean that these documents

---

[89] Van Alsenoy B, Kuczerawy A and Ausloos J, 'Search engines after Google Spain, 9.
[90] [2003] EWCA Civ 1746.
[91] *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

necessarily constituted personal data relating to the subject. A more sophisticated analysis was required:

> *It seems to me that there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.*[92]

The manner in which the data is collected, used or processed must relate to an identifiable person otherwise there is no threat to privacy and no justification for the application of legislative controls.[93] An identifiable person is described as 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, psychological, mental, economic, cultural or social identity in the directive.[94]

B. Data Processing

The Directive gives a person the right to object to the processing of their personal data where the processing of that data is not justified.[95] The processing of the information may not be justified where the data controller does not have a legitimate basis (anymore) or does not fulfil requirements of the data quality.

Article 2(b) defines the 'processing of personal data' as:

> *'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by*

[92] *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at paras 27–28.
[93] Lloyd IJ, *Information Technology Law*, 46.
[94] Article 2(a), EU *Data Protection Directive*, 95/46/EC.
[95] Article 14(a), EU *Data Protection Directive*, 95/46/EC.

transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'[96]

The Directive also gives individuals the right to object to the processing of personal data relating to him/her which can be anticipated as being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.[97]

In the *Bodil Lindqvist* case[98] the court had to determine whether the mention of a person's name on a webpage constituted processing of personal data as described in the directive. The court determined that because the term covers the name of a person in conjunction with his telephone number or information about his working conditions or hobbies it constituted personal data.[99]

As to whether or not it is processing the court found that the information had been processed. The court stated that the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means.[100]

C. Data controller

The Data Protection Directive assigns the responsibility for compliance to the 'controller', who is defined by article 2(d) as;

"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[101]

In the Google Spain case[102] the court identified Google in its capacity as a search engine to be the data controller. This was due to the fact that the operator determines the purposes and means of data processing by the search engine and because the objective of the

[96] Article 2(b), EU *Data Protection Directive*, 95/46/EC.
[97] Article 14(b), EU *Data Protection Directive*, 95/46/EC.
[98] EUCJ, Judgement of 6 November 2003.
[99] EUCJ, Judgement of 6 November 2003, para. 24.
[100] EUCJ, Judgement of 6 November 2003, para. 25.
[101] Article 2(d), European Data Protection Directive.
[102] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12).

relevant provisions of the Directive is to ensure effective and complete protection of data subjects through a broad definition of the concept of 'controller'. The Court determined that Google Inc. is both the actual operator and the data controller of the Google search engine.[103]

Some argue that it is not fare to put the responsibility on search engines because they only act as intermediaries and only display what is found on other websites. Google for example, simply displays the information that has been published by the other websites. If the information was not provided by the original publisher then Google would not produce the information in a web search. It can thus be argued that the publisher of the information is the sole controller of the data.[104]

Nevertheless, search engines perform some if not all of the functions listed in article 2(b) of the directive. The Directive provides that the processing can either be automatic or otherwise involves collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[105]

The Article 29 Working Party when elaborating upon the role of search engines, it reasoned that;

> '*The principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers. The formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases'.*[106]

---

[103] Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', *Law, Society and Economy Working Papers*, (2015), 6.
[104] Van Alsenoy B, Kuczerawy A and Ausloos J, 'Search engines after Google Spain: internet@liberty or privacy@peril? ' , 14.
[105] Article 2(b), European Data Protection Directive.
[106] Van Alsenoy B, Kuczerawy A and Ausloos J, 'Search engines after Google Spain: internet@liberty or privacy@peril? ' , 15.

So what is to happen to the information found on the websites where search engines retrieve the information from or rather third-party data[107]?

The CJEU stated that an individual has a right to have a search engine remove links to web pages published by third parties from search results that are made on the basis of a search on a person's name. This right applies regardless of whether the material indexed is removed from such third party web pages themselves, and regardless of whether it was posted lawfully.[108]

D. Data protection Supervision

1. Supervisory Agencies

A supervisory authority is necessary because they are better placed to take an overview of processing activities unlike an individual who may have rights but not enough information to permit them to analyse and evaluate activities of various public and private agencies.[109]On the other hand, agencies have to straddle a wide range of roles from consumer ombudsman, through law enforcer, to acting which could lead to a conflict of interest.[110]

The Data Protection Directive takes the view that there should be an independent supervisory authority set up in each member state.[111] The supervisory authority should be afforded investigative powers, powers of intervention for example delivering opinions and power to engage in legal proceedings where there has been violation of the national data protection laws.[112]

The supervisory authority is also given the authority to hear claims lodged by any person or by an association representing that person concerning the protection of his rights and freedoms in regard to the processing of personal data. [113]

---

[107] 'Third-party data', refers to data about individuals which is drawn from (other) websites and displayed in the results pages of search engines. For example, if a newspaper article or blog post references an individual by name, this name might be included in a page description displayed on the results page.
[108] Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', 6.
[109] Lloyd IJ, *Information Technology Law*, 60.
[110] Lloyd IJ, *Information Technology Law*, 60.
[111] Article 28, *Data Protection Directive*, 95/46/EC.
[112] Article 28(3), *Data Protection Directive*, 95/46/EC.
[113] Article 28(4), *Data Protection Directive*, 95/46/EC.

The UK Data Protection Act establishes the office of the Information Commissioner.[114] Data controllers are required to notify the Information Commissioner before they begin to process personal data.[115]

2. Data subject as supervisor

The primary control is through the actions of the data subject.[116]

The Directive provides that the controller or his representative must provide a data subject from whom data relating to him/her are collected with information concerning the identity of the controller or his representative, the purpose of processing and any other such information except where he already has it.[117]

Article 12 provides for a Right of access. It states that Member States shall guarantee every data subject the right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

b) 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;

---

[114] Murray A, *Information Technology Law*, 507.
[115] Section 17, *Data Protection Act* CAP 29 of 1998 (UK).
[116] Murray A, *Information Technology Law*, 508.
[117] Article 10, *Data Protection Directive*, 95/46/EC.

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.[118]

E. The African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection was adopted at the 23rd Union Summit held in June of 2014. The Convention is meant to cover Electronic Commerce, Data Protection and Cyber Crime.

Article 8(1) of the Convention states that each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.[119]

The convention applies to any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies.[120]It however exempts the processing of data for personal use and not for the dissemination to third parties and the Temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage of data and for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted.[121]

Article 10 requires that a declaration is made to a protection authority before processing personal data.[122] This does not apply in the instance mentioned above or processing undertaken with the sole objective of maintaining a register meant exclusively for private use or processing undertaken by a non-profit making association or body, with a religious, philosophical, political or trade union aim, provided that the data are consistent with the

---

[118] Article 12, *Data Protection Directive*, 95/46/EC.
[119] *African Union Convention on Cyber Security and Personal Data Protection,* 27 June 2014, *EX.CL/846(XXV).*
[120] Article 9(1), *African Union Convention on Cyber Security and Personal Data Protection.*
[121] Article 9(2), *African Union Convention on Cyber Security and Personal Data Protection.*
[122] Article 10(2), *African Union Convention on Cyber Security and Personal Data Protection.*

objective of the said association or body structure, and relate solely to its members, and that the data are not disclosed to a third party.[123]

The convention is a significant step for Africa towards data protection but it gives a chance for governments to misuse personal data by taking advantage of the exceptions in the convention to restrictions on personal data processing in the name of "public interest" or "exercise of official authority." These terms are not defined in the convention and, as such, could be used to justify abuse of personal data by government entities.

[123] Article 10(1), *African Union Convention on Cyber Security and Personal Data Protection.*

V. CHAPTER 5: THE RIGHT TO BE FORGOTTEN

A. Google Spain and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González

On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, and against Google Spain and Google Inc. His compaliant had to do with the fact that, when an internet user entered Mr Costeja González's name in the Google search engine he would obtain links to two pages of La Vanguardia's newspaper, for a real-estate auction connected with attachment proceedings for the recovery of social security debts.[124]

In his complaint Mr. Costeja González wanted Google Spain or Google Inc to either alter or remove the personal data relating to him so that they ceased to be included in the search results and never appeared in links to La Vanguardia.[125] His grounds for the complaint were that the information was irrelevant because the proceedings against him had been fully resolved for a number of years.[126]

The AEPD found that search engines were subject to data protection legislation because they carry out data processing activities. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties.[127]

Google Spain and Google Inc. brought separate actions against that decision before the National High Court in Spain which joined the actions.[128]

The High Court sent the case to the European Court of Justice for a preliminary hearing because the case depended on the interpretation of Directive 95/46 in order to determine what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third

[124] *Google Spain and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, EUCJ Judgement of 13 May 2014, para 14.
[125] *Google Spain*, 15.
[126] *Google Spain*, 15.
[127] *Google Spain*, 17.
[128] *Google Spain*, 18.

parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. [129]

The court found that Article 2(b) and (d) of Directive 95/46/EC are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).[130]

Further, article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.[131]

B. Why Do We Need the Right to be forgotten?

Blanchette JF and Johnson DJ argue that the right to be forgotten is a social value but they also admit that there is also a reason not to forget where they state:

> *"A world in which individuals are not held accountable over time for the consequences of their actions will not produce the sense of responsibility that is just as necessary to a democratic society. Thus, achieving the appropriate degree of social forgetfulness is a complex balancing act, ever in tension between the need to hold accountable, and the need to grant a "fresh start."*[132]

---

[129] *Google Spain*, 19.
[130] *Google Spain*, 100(1).
[131] *Google Spain, 100(3).*
[132] Blanchette JF and Johnson DJ, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' *Taylor and Francis*, (2002), 36.

The Constitution stipulates that in the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others.[133]

The right to information is limited by the Constitution where it states that every person has the right to the correction or deletion of untrue or misleading information that affects the person.[134]

Is all information useful or necessary? For example is it important to hold information where it is damaging to the reputation of a person where it is no longer relevant? In the case of Les Alfacs a company that owned a campground filed a lawsuit against Google Spain because the search engine would not stop placing in its top results news about a horrific tragedy that took place on their campsite in 1978, when a truck transporting propylene exploded, leaving 243 dead. The company wanted Google to filter the search results and differentiate between those who were looking for information on the tragedy and those who merely sought information about the campground. The fact that the incident appeared in Google's search results was causing damage to the company 10 to 15 years on.[135] Despite the fact that Les Alfacs case involved a company and not an individual it is a good example of how irrelevant information can still be damaging yet it is not important.

There is a benefit to forgetting as it is essential to democracy. The idea that every act of an individual has permanence limits a person's freedom to express themselves out of fear of being affected by those acts in the future therefore, limiting the democratic citizens' development.[136]

The law has in many cases favoured the idea of forgetting past transgressions and beginning afresh. The writers Blanchette JF and Johnson DJ highlight the different areas where the law has encouraged forgetfulness as a social good. These include Bankruptcy law and Juvenile Crime reports. When it comes to Bankruptcy the value of forgetting is to allow the debtors and the creditors to move on from the debt and allow the debtor to participate in the economy. In this case forgetfulness is a social good in favour of the economy. In the instance of Juvenile crime records it is important for a juvenile to not be

---

[133] Article 33(3),Constitution of Kenya 2010 .
[134] Article 35(2),The Constitution of Kenya 2010.
[135] Azurmendi A, 'The Spanish Origins of the European "Right to be Forgotten": The Mario Costeja and Les Alfacs Cases', *Internet Monitor 2014, Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse 1*, (2014), 44.
[136] Blanchette JF and Johnson DJ, 'Data Retention and the Panoptic Society, 36.

held back by past transgressions. That is why it is argued that Juveniles should not have a permanent record of their crimes.[137]

C. The right to be forgotten in the Data Protection Regulation 2012

There is a proposed Data Protection Regulation 2012 which will replace the Data Protection Directive.

The Regulation introduces the right to be forgotten/ the right of erasure. This will allow individuals to have all personal data that businesses holds on them deleted. This will include all photos and any public links to, or copies of, personal data that can be found on the Internet for example in social networks or via search engines. Business will be required to permanently delete the individual's data unless there are legitimate grounds for retaining it.

Article 17 of the proposed regulation provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology "blocking".[138]

Individuals may "lodge a complaint" against data users through their local "supervisory authority"—the regulatory bodies charged with enforcing compliance with the Regulation—which have the power "to order the rectification, erasure or destruction" of data. Additionally, a data subject may bring a direct action against a data user in local courts, which are also empowered to enforce the provisions of the Regulation using injunctions. Finally, a data user that "intentionally or negligently" fails to respond to a data subject's attempt to exercise his or her right to be forgotten may be subject to extremely high fines."[139]

---

[137] Blanchette JF and Johnson DJ, 'Data Retention and the Panoptic Society, 37.

[138] Article 17, Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (2012).

[139] Victor J. M, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy', *Yale Law Journal* (2013) ,526.

The law does not provide any reprieve or repeal for the affected website however. A removal appears to be permanent, even though changing circumstances might make an initial removal no longer warranted.[140]

The search engine only removes the links to the web pages from its search results but it does not remove the information from the World Wide Web. A careful reading shows that the right affirmed by the Court is that of obliging the operators of Internet search engines to suppress links to web pages from the list of search results made on the basis of a person's name, not a right to have data itself deleted from the Internet.[141]

The court found that the individual's rights of privacy outweighed the economic interests of the search engine and the rights of the internet users. However, the Court also stated that suppression may be refused in specific cases, based on a balancing test that considers factors such as '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, [...] [and on] the role played by the data subject in public life'.[142]

The proprietors of the various search engine websites that hold the information are now charged with the responsibility of determining whether the information should be erased or not. Private companies are simply not in a position to make complex decisions on the balancing of different fundamental rights (freedom of expression and right to information), a task that is difficult even for courts, data protection authorities, and academics.[143]

The "right to be forgotten" however does not mean that the information disappears completely. Google stated that a result such as a news report may not appear if one searches for the name of a person mentioned in that report, while a search for other terms mentioned in that report may still display a search result linking to that report.[144]

It is also important to note that the 'right to be forgotten' is territorial. This means that the data controller will only remove the information from the country where the right has been recognised but it will still be available to people who search in other countries. The EUCJ failed to say anything concerning the case's implications for non-EU data controllers, and

---

[140] Zittrain J, 'Troubling Solution to a Real Problem') Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse, (2014), 46.
[141] Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', 7.
[142] *Google Spain, 100(4).*
[143] Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', 19.
[144] Letter to Working Party from Google dated 31st July, 2014 available at https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit, 8.

virtually nothing about its potential impact on the internet despite the fact that Google is located outside the European Union and it is accessible all over the world.[145]

According to the Directive 95/46/EC the only rights available right to access and obtain information from the data controller and the right of erasure was only limited to where the information is incomplete or inaccurate[146]. The right to be forgotten is an extension of data protection laws giving an individual more control over their personal data to have their information deleted from the internet.

[145] Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', 10.
[146] Article 12(b), *Data Protection Directive*, 95/46/EC.

VI. CHAPTER 6: SHOULD THE RIGHT TO BE FORGOTTEN BE RECOGNISED IN KENYA?

A. The current situation in Kenya

The Kenyan government has began collecting information about Kenyans in a bid to ensure security and ease access to government services. In the year 2015 Kenyans were invited to file their tax returns online.

The Jubilee government also launched the eCitizen[147] platform. In December 2012, EDAPS38 completed the creation of an Integrated Population Registration System (IPRS) for the Kenyan government. The IPRS collects data from a dozen databases held by various government agencies. It combines data from the birth and death register, citizenship register, ID card register, aliens register, passport register and the marriage and divorce register as well as elections register, tax register, drivers register, National Social Security Fund (NSSF) register, National Hospital Insurance Fund (NHIF) register and the Kenya National Bureau of Statistics (KNBS) register.[148]

In April 2014, the Kenyan government announced that it would be registering all Kenyans in a new national digital database that would include biometric details as well as information on land ownership, establishments and assets. The aim of the programme is to facilitate the identification of people holding forged or false identification documents.[149]

The use of biometric technology raises specific privacy concerns. As outlined in a briefing published by Privacy International, the very nature of biometric technologies can lead to several problems:

• The data processed is at risk of being misused and is subject to fraud;

• The system can produce misidentification and inaccuracies;

• Its nature renders it exclusionary, given that the universality of the technology itself is yet to be proven with failures to process, for example, the fingerprints of manual labourers and individuals with darker skin;

---

[147] https://www.ecitizen.go.ke/ on 31st August, 2015.
[148] Universal Periodic Review Stakeholder Report, The Right to Privacy in Kenya, 21st Session, Kenya, at 13.
[149] Universal Periodic Review Stakeholder Report, The Right to Privacy in Kenya, 21st Session, Kenya, at 13.

• The unregulated retention of biometric data raises the possibility of "function creep" (use of the data for purposes other than those for which it was collected) and insecure data storage. The mere existence of biometric data could lead to the development of new justifications for its use beyond the original purposes for which the data subject gave consent, and the general storage of data renders it vulnerable to theft.[150]

There is really nothing wrong with the government having information about us but because the information is now online it is important to know that this information is well protected and will be used for the intended purpose. The government should not be able to profile individuals based on tribe, residence, religion or anything else. The government or those who have access to the information should also not be able to sell our information to companies for advertising purposes.

Recently The Cabinet Secretary of Devolution, Ann Waiguru filed a civil suit against the Daily Post and Google. The Daily Post published an online article with the heading "Confirmed it is Anne Waiguru who wanted to sleep with Janet Mbugua's Boyfriend". She claims that the statements were defamatory and have caused her harm. She listed Google as the 1st Respondent on the grounds that she needs information from Google concerning the proprietors of the Daily Post.[151] In her petition she is seeking an order from the court directed to the Respondents to remove or cause to be removed and permanently delete all defamatory statements concerning the Petitioner in the Daily post site and permanently restraining the Respondents from allowing the google.com and google.co.ke returning search results from the said the "Daily Post" on the offending materials concerning the Petitioner. The case is yet to be decided but it is sure to raise issues concerning the right to be forgotten as the judge decides whether or not they should grant such orders.

From the above examples it is clear that Kenya is in need of data protection laws. Currently in Kenya the only laws that maybe able to protect the right to privacy as relates to personal data are:

a) Kenya Information and Communications Act

Section 83W;

---

[150] Universal Periodic Review Stakeholder Report, The Right to Privacy in Kenya, 21st Session, Kenya, at 13.

[151] *Anne Waiguru v Google Inc & 2 others* [2014] eKLR.

(1) Subject to subsection (3), any person who by any means knowingly:—

(a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, shall commit an offence.[152]

b) **Kenya Information And Communications (Consumer Protection) Regulations, 2010**

Regulation 15 (1) "Subject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data."

Data protection laws need to be wide enough to cope with the continuous growth of the internet as explained in Chapter 3. As compared with the Data Protection laws in Europe discussed in Chapter 4 of this dissertation our laws are insufficient.

In Kenya Data Protection laws are an integral part of the Right to Information as expressed in article 35 of the Constitution of Kenya. This is according to Dr Fred Matiang'i, the Cabinet Secretary for Information who says they have completed a framework for implementation of Article 35 through the: Media Bill 2013, Data Protection Bill 2013, Kenya Information and Communication Amendment Bill 2013 and the Access to Information Bill 2012.[153]

B. The Data Protection Bill 2012

The protection of freedom of information and data protection are placed under the same commission.[154]The Commission to be known as the Freedom of Information and Data Protection Commission is established in clause 4 of the Freedom of Information Bill. This implies that the two bills are likely to be passed at the same time.

---

[152]Section 83W, Kenya Information and Communication Act.
[153]http://www.icj-kenya.org/index.php/media-centre/news/566-access-to-information-bill-in-kenya-to-be-tabled-in-parliament on 18th May 2015.
[154] Clause 4(a), *Freedom Of Information Bill*, 2012.

Mr Anthony Kuria, a CIC Consultant, while speaking at the Forum on issues arising from the freedom of information bill, 2008 and data protection bill, 2009, stated that the Data Protection Bill was created in accordance with article 31 of the Constitution of Kenya which has to do with the right to privacy. He also stated that the key principle behind it is that in the automatic processing of data, the data should not be disclosed to any third parties without the permission or consent of the person to whom the information is obtained. Instead of looking at the Data protection law as a threat to the freedom of information he believes that it should be seen as the other side of the coin with regard to the right to access to information as provided in the Freedom of Information Bill.[155]

The Data Protection Bill 2013, at clause 5 asserts the right to privacy of every individual with respect to their personal data relating to their private and family life. The only limitation to the right to privacy is stated in clause 6. The right to privacy may be limited in order to safeguard overriding legitimate interests but the limitation must be carried out using the method that is least intrusive to the data subject. These legitimate interests are not listed in the Bill.

The Act at clause 4 states the principles of data protection that are to guide the application of the Act. Of particular interest are sub- clauses (c) and (h). Sub clause (c) states that the data subject should be informed of any collection of information and of the intended recipients of the information, at the time of collection and (h) gives the data subject the right of access to their personal information and a right to demand correction if such information turns out to be inaccurate. The same can be found in article 10 of European Data Protection Directive.

Further influence of article 10 of the European Directive can be found at clause 7 which states that before an agency collects personal information directly from a data subject, the agency shall take such steps as are in the circumstances reasonable to ensure that the data subject is aware of —

a) the fact that the information is being collected;

b) the purpose for which the information is being collected;

[155]Stakeholders Forum On Issues Arising From The Freedom Of Information Bill, 2008 And Data Protection Bill,2009 Organised by: The Commission For The Implementation Of The Constitution (CIC), 2011 page 13 available at: FOI Data Protection Bill Report on 26th June 2015.

c) the intended recipients of the information;

d) the name and address of the agency that is collecting the information and the agency that will hold the information and whether or not any other agency will receive the information;

e) the collection of the information is authorised or required by or under law—

   i. the particular law by or under which the collection of the information is so authorised or required;

   ii. protocols to comply with the law;

   iii. (iii) whether or not the supply of the information by that data subject is voluntary or mandatory;

f) the consequences if any, for that data subject if all or any part of the requested information is not provided;

g) the rights of access to, and correction of, personal information provided under this

Under clause 10, users are granted the right, where their personal data is destined for automated or manual processing, to information on the person processing data concerning him or her; place of origin of the data; use of the data collected; any other person to whom the data is transmitted; and rectification of incorrect data and the right to erasure of illegally processed data.

With regard to the security of the information collected, agencies holding personal information are required under clause 11 to ensure that the information is protected, by such security safeguards as are reasonable in the circumstances, against loss, damage and destruction or the access and use by an unauthorised person, modification, or negligent disclosure or use.

The Bill further requires that information be held in ways that can be easily retrieved, that users have the right to obtain access to personal information held by agencies and the right to correction of such information. It further requires under clauses 14, 15 and 16, that any information obtained be used for the intended purpose, not misused—including use for commercial purposes—without express consent of the subject or authorised under written

law respectively. Lastly, it provides that a person who interferes with the right to privacy is liable to imprisonment for a two year term or to a fine of Kshs. 100,000, or both.

VII. CHAPTER 7 CONCLUSION

A. Findings

The right to privacy is the right to keep personal information to oneself. The right is itself important to the individual as part of the society. The internet presents a unique problem because it collects information yet it is not governed like other sources of media. With the development of Web 2.0 the internet has evolved to a place where everyone and anyone with an internet connection can share anything about themselves. This is why data protection rights were developed to protect the individual rights.

Data protection laws were developed to protect people's rights on the internet. They protect personal data from processing of any kind. For Mr. Mario Costeja it was not enough to prohibit the processing of data, he wanted his information completely removed from the internet. The EUCJ held that he was within his rights to have the information deleted.

B. Recommendations

a) A proper Data Protection Authority should be set up

The EU Data Protection Directive states that there needs to be a regulatory authority to implement Data Protection laws. The same should be done in Kenya to ensure that once the Bill is passed there is an authority to ensure compliance with the law. Otherwise if the law is passed as it is it would be ineffective.

b) The data protection law should be given priority in Kenya

The first data protection bill was drafted in 2009 and as of today (08th January, 2016) the bill has not been passed. This delay is indicative of either the non prioritisation or perceived unwillingness of the government to adopt data protection legislation.[156]

[156] Kenya Human Rights Commission, The Internet Legislative and Policy Environment in Kenya, January 2014, at 36

With the growing use of the internet and the continued collection of personal data it is necessary to ensure that individual's data is protected in Kenya.

c) The data protection Bill should be altered to include the right to be forgotten

It is my recommendation that the bill should contain provisions for the right to be forgotten so as to give Kenyans a positive right as regards their personal data online. The bill gives the right to know who is processing data and the right of rectification but it does not give the right to be forgotten or the right of erasure.

d) The Data Protection Bill should be separated from the Freedom of Information Bill

The Data Protection Bill has to be passed in conjunction with the Freedom of Information Bill because they are protected by the same commission, the Commission to be known as the Freedom of Information and Data Protection Commission. This could be the reason why the law has not been passed.

Although the freedom of information and data protection are closely linked, they are not the same right. There are also instances where the right to information may be in conflict with data protection. In this instance there no guidelines to help the commission decide what to do. For this reason I believe they should not share a commission.

BIBLIOGRAPHY

C. Books

1. Lessig L, *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, New York, 2001.
2. Lloyd IJ, *Information Technology Law*, Oxford University Press, Oxford, 2008
3. Locke J, *The Second treatise of Government*, Hacket Publishing Company, Indanopolis, 1980.
4. Mill JS, Essay on Liberty, available at http://www.constitution.org/jsm/liberty.htm on 04th March, 2015.
5. Murray A, *Information Technology Law: The Law and Society,* Oxford University Press, Oxford, 2013.

D. Articles and Conference Papers

1. Azurmendi A, 'The Spanish Origins of the European "Right to be Forgotten": The Mario Costeja and Les Alfacs Cases', *Internet Monitor 2014, Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse 1*, (2014).
2. Benkler Y, 'From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access' *Yale Law Journal,* (2000).
3. Blanchette JF and Johnson DJ, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' *Taylor and Francis*, (2002).
4. Crawford K, Schultz J, 'Big Data And Due Process: Toward a Framework To Redress Predictive Privacy Harms', *Public Law & Legal Theory Research Paper Series Working Paper No. 13-64* (2013).
5. George C and Scerri J , 'Web 20 and User-Generated Content: legal challenges in the new frontier' *Journal of Information, Law and Technology*, (2007).
6. Glancy JD, 'The Invention of the Right to Privacy', *Arizona Law Review* ,(1979).
7. Graux H, Ausloos J and Valcke P, 'The right to be forgotten in the internet era', *ICRI Working Paper* (2012).
8. Koops BJ, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series*, (2012).

9. Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', *Law, Society and Economy Working Papers*, (2015).
10. Rossen J, 'The Right to be forgotten', *Stanford Law Review Online,* (2012).
11. Solove DJ, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*,(2006).
12. Solove DJ, 'Conceptualizing Privacy', *California Law Review*, (2002).
13. Solove DJ, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *San Diego Law Review,* (2007).
14. Van Alsenoy B, Kuczerawy A and Ausloos J, 'Search engines after Google Spain: internet@liberty or privacy@peril? ' *ICRI Working Paper 15* (2013).
15. Victor J. M, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy', *Yale Law Journal* (2013).
16. Warren SD and Brandeis LD, 'The Right to Privacy' *Harvard Law Review*, (1890).
17. Wu T, 'Network neutrality, broadband discrimination', *Journal of Telecommunications and High Technology Law* (2003).
18. Zittrain J, 'Troubling Solution to a Real Problem') Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse, (2014).

Reports

1. Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation.
2. Interactive Advertising Bureau, I*AB Platform Status Report: User Generated Content, Social Media and Advertising – An Overview*, (April 2008)
3. Letter to Working Party from Google dated 31st July, 2014 available at https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit.
4. Universal Periodic Review Stakeholder Report, *The Right to Privacy in Kenya*, 21st Session, Kenya.
5. Kenya Human Rights Commission, *The Internet Legislative and Policy Environment in Kenya*, January 2014.

E. Internet sources

1. Carpenter B.E, *Architectural Principles of the Internet* (1996) https://www.ietf.org/rfc/rfc1958.txt on 17 December, 2015.

2. http://www.portland-communications.com/publications/how-africa-tweets-2014/#sthash.bGvnQNpU.dpuf on 13 February, 2015

3. Reding V, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, 5 *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF on 12 February, 2015

4. User-generated content is dead – as video evolves, available at http://www.forbes.com/sites/stevenrosenbaum/2014/07/14/user-generated-content-is-dead-as-video-evolves/ (accessed on 25/7/2015).