Strathmore University
Law School

A COMPARATIVE STUDY OF SOCIAL MEDIA USE IN HIRING PROCESSES IN THE UNITED STATES, THE UNITED KINGDOM AND KENYA

BY

LOICE KERUBO NYARIBO

072323

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS

STRATHMORE UNIVERSITY

STRATHMORE LAW SCHOOL

MARCH, 2016

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I would like to thank God for his sufficient grace throughout the writing of this dissertation up till its completion and my supervisor Dr Isaac Rutenberg who has supported me throughout this process. I would also like to thank my family who have encouraged me all through law school and my friends who have understood the dedication required write a dissertation.

DECLARATION

I, **Loice Kerubo Nyaribo** declare that this dissertation is my original work and has not been submitted for the award of a degree in any other university.

Signed: _____ Date: 13/4/2016

Researcher: **LOICE KERUBO NYARIBO**

Supervisor:

This dissertation has been submitted for examination with my approval as a University lecturer.

Signed: _____ Date: 12/4/16

DR. ISAAC RUTENBERG

STRATHMORE LAW SCHOOL

ABSTRACT

The internet has become a worldwide phenomenon and with its spread to most parts of the world,[1] social media has been made accessible to more people. Hence, human interactions have been moved from the physical realm into the virtual world[2] for example, employers have started using social media sited to investigate job applicants due to the accessibility and popularity of social media sites.[3]

The aim of this dissertation is to find out whether there are policies in Kenya governing the use of social media in hiring decisions in employment and whether Kenya should allow or disallow the use of social media to vet prospective employees during the application process. The research done on this paper is from online content as little to no information on this subject has been documented in books. The content is also largely foreign as there is very little information on the subject in Kenya as it is still a developing area of law.

This research found that the most advanced country with respect to social media in the recruitment process is the United States while the UK courts recognise the existence of the use of social media in the recruitment process but fail to see the importance of creating laws to deal with the issue. Kenya, on the other hand, has no legislation to deal with the issue of the use of social media in the hiring process and no legal opinions have been issued on the same. From the literature reviewed in the paper, there can be no privacy in a public space hence job applicants should be wary about what they post online.

The recommendations given include the use of the Employment Act until new legislation dealing with social media in hiring is enacted, creation of new laws by parliament including laws to deal with online privacy and employers' rights during employment, the disclosure of the vetting methods for applications by employers, the inclusion of social media vetting late in the employment process and prudence by social media users.

---

[1] http://www.internetlivestats.com/internet-users/ on 2 March 2015.
[2] Wall DS, 'The Internet as a Conduit for Criminals' in Pattavina A (ed), *Information Technology and the Criminal Justice System*, Sage Publications Inc., revised 2015, 78.
[3] Madera JM and Chang W, "Using Social Network Sites to Investigate Employees in the Hospitality Industry".

LIST OF ABBREVIATIONS

ABC – American Broadcasting Corporation

ACAS – Advisory, Conciliation and Arbitration Service

ADA – Americans with Disabilities Act

COK – Constitution of Kenya

EEOC – Equal Employment Opportunity Commission

GA – General Assembly

ILO – International Labour Organisation

KOT – Kenyans on Twitter

UK – United Kingdom

UN GAOR – United Nations General Assembly Official Records

UNTS – United Nations Treaty Series

US – United States of America

LIST OF CASES

CHAPTER 1 - INTRODUCTION

1.1Background

The Internet[4] can simply be defined as an electronic communications network that connects computer networks and organisational computer facilities around the world.[5] It is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.[6] This has, over the years, greatly simplified the access to information and consequent interaction with other people.

Social media can be defined as a form of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).[7] With the growth and constant expansion of the internet, social media has grown with it hence created social networking sites which focus on building online communities of people who share interests and activities, or who are interested in exploring the interests and activities of others.[8] They are designed to connect users to each other and to visually display each individual's network of friends. Most provide a variety of ways for users to interact, such as e-mail and instant messaging services.[9] Rapid technological growth has led to the spread of the internet to most parts of the world; from less than 1% in 1995 to around 40% in 2014.[10] Consequently, more people have had access social media which has led to the social orders that bind time and space to become lifted out of local contexts of interaction and restructured across indefinite spans of time-space.[11]

---

[4] https://www.nitrd.gov/fnc/Internet_res.aspx on 25 February 2015.
[5] http://www.merriam-webster.com/dictionary/internet on 15 February 2015.
[6] http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet on 15 February 2015.
[7] http://www.merriam-webster.com/dictionary/social%20media on 8 August 2015.
[8] Kluemper DH and Rosen PA, 'Future employment selection methods: evaluating social networking web sites' 24 *Journal of Managerial Psychology* (2009), 3.
[9] Kluemper DH and Rosen PA, 'Future employment selection methods: evaluating social networking web sites', 3.
[10] http://www.internetlivestats.com/internet-users/ on 2 March 2015.
[11] Wall DS, 'The Internet as a Conduit for Criminals' in Pattavina A (ed), *Information Technology and the Criminal Justice System*, Sage Publications Inc., revised 2015, 78.

1.2 Statement of the problem

Due to human sociability, social networking sites have become extremely popular, with sites such as Facebook recording over 1 billion users and Twitter recording 316 million users as of August 2015.[12] Many of these sites have mechanisms for sharing personal information, such as pictures, favourite music and videos, blogs, other links, and displaying interests and personal demographic information (e.g., age, ethnicity, religion, sexual-orientation, marital status).[13] Due to the popularity and accessibility of these sites, employers have started using them to screen or investigate job applicants.[14]

Employers who hire graduating students are steadily discovering that social networking sites allow them to learn more than they ever could from reading an applicant's resume and cover letter[15] as the more information they are able to obtain, the better placed they are to determine the character of the individual who will carry the brand of their company. However, since everyone is accorded the right to privacy[16] in Kenya, should employers be able to access private social networking profiles so as to vet job applicants? There are currently no laws in Kenya dealing with the issue hence this level of hiring goes largely unmonitored by the government and undetected by most job applicants. This may lead to discrimination based on the vast amounts of information available on social networking sites as opposed to information required for job applications.

1.3 Statement of Objective(s)

The objectives of this study are to find out:

i. Whether there are policies in Kenya governing the use of social media in hiring decisions in employment.

ii. Whether Kenya should allow or disallow the use of social media to vet prospective employees during the application process.

iii. The limitations of the use of social media in the hiring process.

---

[12] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ on 7 August 2015.

[13] Madera JM and Chang W, "Using Social Network Sites to Investigate Employees in the Hospitality Industry" International CHRIE Conference-Refereed Track, Amherst, 27 July 2011, http://scholarworks.umass.edu/cgi/viewcontent.cgi?Articleicle=1643&context=refereed on 8 August 2015.

[14] Madera JM and Chang W, "Using Social Network Sites to Investigate Employees in the Hospitality Industry".

[15] Brandenburg C, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare' 60 *Federal Communications Law Journal* (2007), 2.

[16] Article 31, COK (2010)

1.4 Research Questions

i. Based on international jurisprudence, is the access to prospective employees' social networking websites without their express consent legal or does it amount to discrimination?

ii. Should the use of content sourced from social media sites to vet employees be recognised as a new form of discrimination?

iii. Should Kenya adopt the use of social media as a valid method of vetting employees during the hiring stage in its legislation?

1.5 Justification of the study

This study is important in the 21st Century as social media, in particular, has permeated modern culture and the daily lives of the incoming workforce.[17] These sites are relatively new and hence, have brought about numerous legal, ethical and moral questions that need to be addressed. This paper seeks to address one of the issues that has not been a prevalent one in the Kenyan society and will, therefore, be an important stepping stone in trying to identify the limits of employment practices with regard to social media.

1.6 Scope and limitations of the study

The research will be principally based on online and overseas content. This is due to the fact that there is little about this topic that has been documented in books, of which aren't easily accessible, and there is even less information on the subject in Kenya as it is still a developing area. Reference will mainly be done to the US as a source of cases and legislation. Therefore, secondary sources of information will be the main basis for this research.

1.7 Chapter Breakdown

Chapter 1: Introduction

This chapter introduces the paper by giving the background of the topic and reasons for the research.

Chapter 2: Conceptual/Theoretical Framework and methodology

---

[17] https://newsroom.fb.com/company-info/, on 18 November 2015; https://about.twitter.com/company , on 18 November 2015.

This chapter deals with the different legal theories that can be applied with regard to the use of social media in hiring decisions in employment.

Chapter 3: Study/analysis of the research questions

This chapter will contain an examination of the research questions by discussing case studies from other jurisdictions that have had similar questions to answer.

Chapter 4: Comparative analysis

This chapter will focus on comparing American, English and Kenyan legal frameworks with regard to their response to the question of use of social media in the employment process.

Chapter 5: Recommendations and conclusion

This chapter will contain recommendations on what can be improved upon or changed in Kenyan laws so as to address the issue of social media in the employment process effectively.

CHAPTER 2 - THEORETICAL FRAMEWORK

This section deals with the common law legal theory and in particular, the right to privacy. This right is enshrined in numerous international instruments including the Universal Declaration of Human Rights[18] and the International Convention on Civil and Political Rights[19] and is recognized in the constitutions[20] of various countries around the world.

This fundamental right generally states that no one should be subject to the arbitrary or unlawful interference of his privacy and should be protected by the law against such attacks. The Constitution of Kenya (COK) 2010 specifically states that the privacy of communications should not be infringed[21] and this, logically, can be said to extend to social networking sites as they are a platform for communication between friends and family. Nevertheless, in order for a person's privacy to be invaded, that person must have a reasonable expectation of privacy[22] which stems from the various privacy policies of these social networking sites. Facebook, for example, allows users to manage the privacy of their posts by letting them set it to "public", "friends" or "close friends"[23] hence leading a user to think that the information that they post will only be available to the specific circle they choose it to go to.

However, many students discover their social networking profile or other information posted on the Internet has cost them a job opportunity after it is too late.[24] This can be attributed to the fact that it's not uncommon for recruiters to sign-up for Facebook accounts using an alumni address and then check up on applications from any student who comes from their *alma mater*.[25] Some companies also hire current students who can access their peers' social networking profiles and

---

[18] Article 12, GA Res 217A (III), UN Doc A/811 (10 December 1948)
[19] Article 17, GA Res 2200A (XXI), 21 UN GAOR Supp. (No 16) at 52, UN Doc A/6316 (1966), 999 UNTS 171.
[20] Article 31, COK (2010); Article 14, Constitution of the Republic of South Africa (1997)
[21] Article 31 (d), COK (2010)
[22] Brandenburg C, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare', 8.
[23] https://en-gb.facebook.com/about/basics/what-others-see-about-you/posts/ on 19 November 2015.
[24] 'Nate Anderson: Google + Facebook + Alcohol = Trouble' *ArsTechnica*, 20 January 2006 http://arstechnica.com/uncategorized/2006/01/6016-2/ on 19 November 2015.
[25] 'Nate Anderson: Google + Facebook + Alcohol = Trouble' *ArsTechnica*, 20 January 2006 http://arstechnica.com/uncategorized/2006/01/6016-2/ on 19 November 2015.

effectively circumvent any privacy settings a potential hire may have put in place to attempt to restrict unwanted persons from accessing their profile.[26]

In ***Sanders v. American Broadcasting Corporation,***[27] it was held that: "There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law...**The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.**" In this case, an ABC investigative journalist obtained employment as a telephone psychic and used a hidden video camera to record her conversations with her new co-workers. The plaintiff sued the journalist after part of one of his conversations with her was aired on television. Despite the defendant's claim that since co-workers could overhear her conversations with the plaintiff then he could have no reasonable expectation of privacy in the communication, the court held that Sanders retained a reasonable expectation of privacy during his workplace discussions with co-workers.[28] The principle brought out by this case should also apply to the digital space as one can activate privacy settings online so as to preclude certain people from accessing their personal information hence being seen by some but shouldn't be legally forced to share this information with everyone. Therefore, in some cases, a person who reveals information about themselves to some people may have the right to keep that information private from other unintended persons for the purposes of privacy tort law.[29]

On the other hand, the right to privacy cannot be invoked whereby the information was given with the consent of the applicant. As Larry Hunter, a computer scientist, stated in 1985, "*Our revolution will not be in gathering data—don't look for TV cameras in your bedroom—but in analysing the information that is already willingly shared*"[30] – a phenomenon that holds true today. This concept is applied by

---

[26] Brandenburg C, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare', 6; 'Alan Finder: When a Risqu□ Online Persona Undermines a Chance for a Job' *The New York Times*, 11 June 2006 http://query.nytimes.com/gst/fullpage.html?res=9C0DE3D61231F932A25755C0A9609C8B63 on 19 November 2015.

[27] Co, 978 P.2d 67, 72 (Cal 1999).

[28] 978 P.2d 67, 79 (Cal 1999).

[29] ***YG vs Jewish Hospital of St. Louis***, 795 S.W.2d 488 (Mo. Ct. App. 1990).

[30] Hunter L, 'Public Image' in Johnson D and Nissenbaum H, *Computers, Ethics, and Social Values*, Englewood Cliffs: Prentice Hall, 1995, 294.

employers so as to analyse which applicants are best suited for positions in their companies. Since new employees have access to a wide range of sensitive materials and information via the rise of the information economy and flattened workplace structures, judgment or discretion are increasingly important characteristics for employees to have.[31] Therefore, employers may launch thorough investigations into the qualifications of a job applicant, using a host of psychological and other tests; they may conduct extensive background checks on a potential employee; they may screen them online to learn as much as possible about a potential new hire.[32]

In ***Nader vs General Motors Corporation,***[33] just before consumer advocate Ralph Nader published his best seller, *Unsafe at Any Speed*, General Motors allegedly tried to intimidate Nader by digging into his personal information and past. The company allegedly interviewed Nader's friends and relatives regarding Nader's interests, habits, political and religious beliefs, sexual history, and other areas under the false pretence that it was researching Nader for prospective employment purposes. The New York Court of Appeals determined that information already known to others could hardly be considered private, and Nader therefore could not expect to maintain his privacy despite the fact that he had shared personal information with select persons only.[34] Essentially, Nader was deemed to have assumed the risk that persons to whom he disclosed his information would spread that information to others.

As a matter of law, facts shared with others are no longer private.[35] Hence, if an applicant shares information they deem personal with friends online, and an employer is able to question those friends or happens upon the shared information, they will not be in breach of the right to privacy. Facts posted online and provided to some can be open to all, thus rendering the assessment of prospective employees online fair and just by employers.

---

[31] Brandenburg C, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare', 2.
[32] Sprague R, 'Orwell was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees' 42 *John Marshall Law Review* (2008), 84.
[33] 255 N.E.2d 765 (N.Y. 1970).
[34] 255 N.E.2d 770 (N.Y. 1970).
[35] 255 N.E.2d 770 (N.Y. 1970).

CHAPTER 3 - SHOULD PRIVACY IN A PUBLIC SPACE BE PROTECTED?

3.1 Privacy

I. Privacy in public: When does private content become public?

Even though the revelation of secrets can be daunting due to the possibility of being spread, it is likely that most of us have shared our most embarrassing details with other people and by common parlance, we still consider these facts to be "secrets" even after we have revealed them to a handful of people.[36] But do they remain secrets such that a plaintiff can recover in tort against someone who discovers them through improper means or publishes them in a newspaper without her consent? If so, at what point does a fact "cross-over" from being a "private matter" to a "public matter" whose widespread disclosure does not provide the plaintiff with a cause of action? Can something still be "private" if two people know about it?[37] When John Kerry and John Edwards were criticized after the presidential and vice-presidential debates in 2004 for violating Mary Cheney's "privacy" by mentioning her sexual orientation – an orientation that thousands of Americans already knew about – were the critics making a coherent claim? The press had already mentioned her sexual orientation before the debates hence her privacy wasn't violated even though conservatives seemed to think so.[38]

The principle of privacy was illustrated by the ***Sipple v. Chronicle Publishing Company***[39] case whereby the Appellant saved the US President, Gerald R. Ford, in 1975 from an assassination attempt. Sipple was considered a hero for his selfless action and was subject to significant publicity throughout the nation following the assassination attempt. The Respondent published an article, which was subsequently adopted by other newspapers e.g. the Los Angeles Times, that contained the fact that the Appellant was gay hence the latter sued for a breach of his right to privacy. The court enumerated that there are **three elements of a cause of action predicated on tortious invasion of privacy**:

---

[36] Strahilevitz JL, 'A Social Networks Theory of Privacy' 72 *The University of Chicago Law Review* (2005), 919.
[37] Strahilevitz JL, 'A Social Networks Theory of Privacy', 920.
[38] 'Nicole Caster: Despite conservative accusations, Kerry didn't "out" Mary Cheney' *Media Matters For America*, 15 October 2004 http://mediamatters.org/research/2004/10/15/despite-conservative-accusations-kerry-didnt-ou/132085 on 21 November 2015.
[39] 154 Cal.App.3d 1040 (1984)

i. The disclosure of the private facts must be a public disclosure,[40]

ii. The facts disclosed must be private facts, and not public ones[41] and;

iii. The matter made public must be one which would be offensive and objectionable to a reasonable person of ordinary sensibilities.[42]

It similarly recognized that due to the supreme mandate of the constitutional protection of freedom of the press, even a tortious invasion of one's privacy is exempt from liability if the publication of private facts is truthful and newsworthy. It set out the criteria for determining newsworthiness i.e.

(a) the social value of the facts published;

(b) the depth of the article's intrusion into ostensibly private affairs;

(c) the extent to which the individual voluntarily acceded to a position of public notoriety[43] and;

(d) the paramount test i.e. whether the matter is of legitimate public interest which in turn must be determined according to the community mores.[44] The line is to be drawn when the publicity becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.[45]

The summary judgment in the trial court was upheld by the appellate court based on the Restatement Second of Torts section 652D which provides that "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." The court held that the facts disclosed by the articles were not private facts within the meaning of the law as Sipple had been publicly gay[46] and the publications in dispute were newsworthy as they were prompted by legitimate

---

[40] Porten v. University of San Francisco (1976) 64 Cal. App. 3d 825

[41] Kapellas v. Kofman (1969) 1 Cal. 3d 20, Coverstone v. Davies (1952) 38 Cal. 2d 315

[42] Kapellas v. Kofman (1969) 1 Cal. 3d 20, 35; Coverstone v. Davies (1952) 38 Cal. 2d 315

[43] Briscoe v. Reader's Digest Association, Inc. (1971) 4 Cal. 3d 529

[44] Virgil v. Time, Inc. (9th Cir. 1975) 527 F.2d 1129

[45] Virgil v. Time, Inc., 1129

[46] The Los Angeles Times, who were also respondents in the case, were exempt from liability on the ground that they only republished the Chronicle Article which implied that appellant was gay. It is, of course, self-evident that no right of privacy attaches to a matter of general interest that has already been publicly released in a periodical or in a newspaper of local or regional circulation (Sperry Rand Corporation v. Hill (1st Cir. 1966) 356 F.2d 181, 185)

political considerations thus constituted a protective shield from liability based upon invasion of privacy.

Therefore, one cannot claim to have privacy in a public arena if the information that they want to keep hidden is already known as a general truth or has previously been published in a newspaper. Private content, therefore, can be considered public as soon as it's spread to a large number of people who were never intended to receive the content.

II. On social networking sites: Is it possible to have private content online?

In the recent past, Twitter and Facebook have become some of the most popular social networking sites in Kenya.[47] All pointers show that social media in Kenya is not just a fad but a way of life and trending topics, more so on Twitter have become so addictive that we cannot wait to see what hashtag is causing ripples.[48] Kenyans posting tweets have created a community i.e. Kenyans on Twitter (#KOT) which is currently one of the most popular tags on posts that addresses, condemns or makes fun of different issues in the country. Mark Kaigwa, the author and founder of Nendo Ventures, created The A-to-Z of Kenyan Twitter (#AtoZofKOT),[49] a publication that is a strong reflection of how KOT and other social media platforms are a driven, open-minded and powerfully opinionated lot.[50]

All social networking sites have Terms and Conditions of Service which include a Privacy Policy that is to be read by the user before accepting the services of the particular site. Under **Facebook's** privacy policy,[51] one can control what others see about them and how they interact with other people. Users can choose who to share status updates, photos or videos with i.e. with friends, a specific group of people or

---

[47] 'Mr Joel: 5 Most Popular Social Media Platforms in Kenya' *Mixtra Web,* 26 August 2015 http://www.mixtraweb.com/5-most-popular-social-media-platforms-in-kenya/ on 10 December 2015.
[48] 'Josephine Mosongo: Kenyan social media trends' *Daily Nation,* 23 October 2014 http://www.nation.co.ke/lifestyle/buzz/Kenyan-social-media-trends/-/441236/2496394/-/11tboyz/-/index.html on 10 December 2015.
[49] https://twitter.com/MKaigwa/status/521564426139602944 on 11 December 2015.
[50] 'Josephine Mosongo: Kenyan social media trends' *Daily Nation,* 23 October 2014 http://www.nation.co.ke/lifestyle/buzz/Kenyan-social-media-trends/-/441236/2496394/-/11tboyz/-/index.html on 10 December 2015.
[51] https://www.facebook.com/about/basics/ on 11 December 2015.

publicly. A post accidentally shared with the wrong audience can always be changed to the right one.[52]

Nevertheless, some information e.g. age range, language and country is public. A user's Public Profile, which helps to connect with friends and family, is also public and includes name, gender, username and user ID (account number), profile picture, cover photo and networks.[53] If other people share information about a user, even if it's something that was shared privately by the user to friends/family, they can choose to make it public and comments on other people's public posts are public as well. Facebook also gives a warning that public information can:

(a) Be associated with a user even off Facebook,
(b) Show up when someone does a search on Facebook or on another search engine e.g. Google,
(c) Be accessible to Facebook-integrated games, applications and websites that a user and their friends use and;
(d) Be accessible to anyone who uses Facebook APIs e.g. the Graph API which is the primary way to get data in and out of Facebook's platform.[54]

On **Twitter,** public information includes messages Tweeted; the metadata provided with Tweets; the language, country, and time zone associated with an account; and the lists a user creates, people they follow, Tweets marked as likes or Retweets.[55] The default is almost always to make the information provided public, as long as it's not deleted, but one can use settings or features, like direct messages, to make the information more private if required.[56] Twitter also gives a warning to users to be careful about what they are making public as the Twitter Services broadly and instantly disseminate a user's public information to a wide range of users, customers, and services.

Privacy on social networking sites is, therefore, possible but depends on the user's privacy settings. Nevertheless, some information is always public e.g. name and avatar so as to enable connection between multiple users. A user should exercise discretion when posting online as it is very easy to make private information public.

---

[52] https://www.facebook.com/about/basics/what-others-see-about-you/posts/ on 11 December 2015.
[53] https://www.facebook.com/help/203805466323736 on 11 December 2015.
[54] https://developers.facebook.com/docs/graph-api/overview on 11 December 2015.
[55] https://twitter.com/privacy on 11 December 2015.
[56] https://twitter.com/privacy on 11 December 2015.

3.2 Arguments for a right to privacy in the public space

For many, privacy is valuable, is worth protecting as either a moral or legal right, or both, because it functions to protect and promote other important ends.[57] Alan Westin affirms that privacy promotes important human ends in a democratic, free society: it enhances personal autonomy (which he understands as "the desire to avoid being manipulated or dominated wholly by others"[58]), it creates a protected realm for emotional release, provides a context in which an individual can "exert his individuality on events",[59] and the creates the possibility of limited and protected communication.

Ruth Gavison additionally elaborates upon the essential role of privacy in safeguarding or promoting other deeply held values including liberty of action, "mental health, autonomy, growth, creativity, and the capacity to form and create meaningful human relations".[60]

These approaches have in common a version of the idea that privacy protects a "safe haven", or sanctuary, where people may be free from the scrutiny and possibly the disapprobation of others. Within these private spheres people are able to control the terms under which they live their lives.[61] By exercising control over intimate and sensitive information about themselves, people may exercise control over the way they portray themselves to others, especially those others with whom they engage in lasting relationships. Helen Nissenbaum opines that these two forms of privacy, namely, control over information and control over access, establish the conditions for a free society and, among other things, enhance people's capacity to function as autonomous, creative, free agents.[62]

I. Traditional theories of privacy

These traditional theories of privacy take the dichotomy of private versus public as their guideposts, asserting that privacy is morally violated only when private

---

[57] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' 17 *Law and Philosophy* (1998), 29.
[58] Westin AF, 'Privacy and Freedom' 25 *Washington and Lee Law Review* (1968), 33.
[59] Westin AF, 'Privacy and Freedom', 36.
[60] Gavison RE, 'Privacy and the Limits of the Law' 89 *The Yale Law Journal* (1980), 442.
[61] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 29.
[62] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 29.

information or the private sphere is inappropriately revealed. They consider privacy norms as relevant only to private or intimate information.[63]

Both William Parent and Tom Gerety propose traditional theories of privacy and try to expound upon the concept of privacy. Gerety worries that the problem for the concept of privacy "*comes not from the concept's meagreness but from its amplitude, for it has a protean capacity to be all things to all lawyers. ... A legal concept will do us little good if it expands like a gas to fill up the available space.*"[64] While he characterizes privacy as an "*island of personal autonomy*,"[65] he limits the scope of this autonomy to the "*intimacies of personal identity.*"[66] Parent mirrors Gerety by defining a right to privacy that covers only information that is both personal in nature and not documented anywhere in a public place, for example, reported in a newspaper. About all other information, he concludes that it "*cannot without glaring paradox be called private.*"[67] Therefore, a tweet, for example, isn't covered under Parent's definition of right to privacy as Twitter considers messages Tweeted to be public information[68] and even though personal, tweets are put in the public sphere.

Charles Fried, who believes in both a moral and legal right to privacy, is equally explicit about its limits and states that although a right to privacy would be recognized by law, it would extend only over a limited, conventionally designated, area of information, "*symbolic of the whole institution of privacy*".[69] According to him, this designated area, whose content may differ considerably from society to society, would include intimate or sensitive information, and exclude the so-called "public" sphere from its scope of protection. Fried's rationale for the *"inevitable fact that privacy is gravely compromised in any concrete social system*" is because of "*the inevitably and utterly just exercise of rights by others...*"[70]

---

[63] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 22-23.
[64] Gerety T, 'Redefining Privacy' 12 *Harvard Civil Rights-Civil Liberties Law Review* (1977), 234.
[65] Gerety T, 'Redefining Privacy', 271.
[66] Gerety T, 'Redefining Privacy', 281.
[67] Parent W, 'Privacy, Morality, and the Law' 12 *Philosophy & Public Affairs* (1983), 271.
[68] https://twitter.com/privacy on 11 December 2015.
[69] Fried C, 'Privacy' 77 *The Yale Law Journal* (1968), 488-489.
[70] Fried C, 'Privacy', 487.

II. Contextual integrity

The concept of **contextual integrity** can be referred to as the norms—explicit and implicit—which govern how much information and what type of information is fitting for different transactions, situations and relationships in which people engage.[71] This refers to the fact that people don't object to divulging information, even if it is quite personal or intimate,[72] that is applied appropriately to a particular situation e.g. people are comfortable with letting doctors know about their physical conditions as opposed to giving that information to a stranger met on a plane. There are a number of theorists who support this viewpoint as illustrated below.

James Rachels, for example, argues that a right to privacy ought to include the right not only to control whether information is shared, but when and with whom it is shared.[73] Through sharing information discriminately, people can define the nature and degree of intimacy of different relationships:

"The same general point can be made about other sorts of human relationships: businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on. In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have."[74]

The capacity to define the nature and degree of closeness of relationships is an important aspect of personal autonomy, Rachels argues, and ought to be protected. Having to enter relationships or settings with little or no control over what is known about one, may lead to a sense of having been demeaned, embarrassment, disempowerment, or even fear.[75]

Ferdinand Schoeman has a similar viewpoint as he states that people have, and it is important that they maintain, different relationships with different people because

---

[71] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 20.
[72] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 22.
[73] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 21.
[74] Rachels J, 'Why Privacy is Important' 4 *Philosophy & Public Affairs* (1975), 328.
[75] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 22.

information appropriate in the context of one relationship may not be appropriate in another.[76] He gives the following example;

"A person can be active in the gay pride movement in San Francisco, but be private about her sexual preference vis-a-vis her family and co-workers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?"[77]

Helen Nissenbaum opines that people's judgments that privacy has been violated concur more systematically with breaches of contextual integrity than with breaches of only intimate or sensitive realms.[78] Popular judgment takes contextual integrity as its benchmark and whereas traditional theories of privacy consider privacy norms as relevant only to private or intimate information, the former considers privacy norms as potentially relevant to any information.[79]

Larry Hunter, while talking about data aggregation with regard to public surveillance, brings about an element of lack of privacy as the records of surveillance subject people to change the way they act in public.

"Consider what happens if I write down everything I see out my window, and all my neighbours do, too. Suppose we shared notes and compiled the data we got just by looking out our own windows. When we sorted it all out, we would have detailed personal profiles of everyone we saw. If every move anyone made in public were recorded, correlated, and analysed, the veil of anonymity protecting us from constant scrutiny would be torn away. Even if that record were never used, its very existence would certainly change the way we act in public."[80]

---

[76] Schoeman F, 'Privacy and Intimate Information' in Schoeman F (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press, 1984, 408.
[77] Schoeman, F. "Gossip and Privacy" in Goodman RF and Ze'ev AB (ed.) *Good Gossip*, University Press of Kansas, 1994, 73.
[78] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 22.
[79] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 22-23.
[80] Hunter L, 'Public Image', 295.

With reference to social media, if employers use these platforms to observe potential employees, then people will change the way they act on these public sites so as to fit into the ideal employee. This will neither benefit the employer, who may employ someone with doctored values, nor the applicant who will lose the freedom to freely express their true thoughts on issues online. People who have an awareness of what or how much others know about them may be able to protect their privacy more effectively as opposed to those who don't, but at the expense of developing a wariness, self-consciousness, suspicion, and even tentativeness in their relations with others. This was described as "a chilling effect" on behaviour by Judith DeCew.[81]

3.3 Arguments against a right to privacy in the public space

I. Knock-down normative argument

This objection to the right to privacy is proposed by theorists who, even though they recognize the importance of privacy, opine that it must be balanced against other competing forces. Privacy in public is frequently a victim of such balancing as it regularly succumbs to the apparently overwhelming weight of competing interests.[82] Jeffrey Reiman, who characterizes privacy as a social practice involving "*a complex of behaviours that stretches from refraining from asking questions about what is none of one's business to refraining from looking into open windows one passes on the street*"[83] and who argues that privacy is essential for the formation of a conception of the self, nevertheless concedes that the social practice of privacy "*does not assert the right never to be seen even on a crowded street.*"[84] If you have chosen to expose yourself and information about yourself in public view with the result that others have access to you, or to information about you without intruding upon your private realm, then any restrictions on what they may observe, record and do with this information cannot be justified. Not only is this unreasonable, but it is wrong because it imposes an unacceptable restraint on the freedom of others.[85]

Larry Hunter grants that "*although we consider it a violation of privacy to look in somebody's window and notice what they are doing, we have no problem with the*

---

[81] DeCew JW, 'In Pursuit of Privacy: Law, Ethics, and the Rise of Technology' *Cornell University Press* (1997), 64.
[82] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 10.
[83] Reiman JH, 'Privacy, Intimacy and Personhood' 6 *Philosophy & Public Affairs* (1976), 43-44.
[84] Reiman JH, 'Privacy, Intimacy and Personhood', 44.
[85] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 11.

reverse: someone sitting in his living room looking out his window."[86] Consequently, placing any restraint on such activity would constitute an unacceptable restraint on liberty. Justice O'Connor, referring to police officers in ***Florida v. Riley***, wrote that people cannot be expected to "*shield their eyes when passing by.*"[87] Hence, the burden placed on others to promote the right to privacy cannot interfere with the normal activities of their daily lives. A person cannot expect another to avoid looking at their online social media profile in the name of privacy as this interferes with the latter's right to information and restricts them from freely accessing internet resources.

In ***California v. Greenwood,***[88] which involved people's right to privacy in their garbage, the Supreme Court ruled that police had not violated the Fourth Amendment when they arranged for Greenwood's trash collector to segregate his trash and turn it over to them for inspection. The court held;

> *Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it," respondents could have no reasonable expectation of privacy in the inculpatory items that they discarded.*

Asserting the decision in California v. Greenwood, the court in ***United States v. Scott***[89] defended the actions of IRS agents, who had reassembled documents which the defendant had shredded before disposing of them in the garbage, arguing;

> *In our view, shredding garbage and placing it in the public domain subjects it to the same risks regarding privacy, as engaging in a private conversation in public where it is subject to the possibility that it may be overheard by other persons. Both are failed attempts at maintaining privacy whose failure can only be attributed to the conscious acceptance by the actor of obvious risk factors. In the case of the conversation, the risk is that conversation in a public area may be overheard by a third person. In the disposal of trash, the risk is that it may be rummaged through and deciphered once it leaves the*

[86] Hunter L, 'Public Image', 295.
[87] 488 U.S. 445 (1989).
[88] 486 U.S. 35 (1988).
[89] 975 F.2d 927 (1st Circ.1992).

control of the trasher. In both situations the expectation of privacy has been practically eliminated by the citizen's own action. ***Law enforcement officials are entitled to apply human ingenuity and scientific advances to collect freely available evidence from the public domain.***[90]

The supporters of the knock-down normative argument maintain that prohibition of the collection and aggregation of information that people have made no effort to hide from view would violate the freedom of those who would observe, record, and aggregate it. They argue that because the "cat is out of the bag" already, there is no good reason to stifle the ingenuity of entrepreneurs who would sell and thereby profit from this information.[91]

II. Reasonable expectation of privacy

One of the most common concerns among applicants is that employer investigations will invade their right to privacy and will reveal information that they believe should not be used in the decision-making process.[92] Privacy in the workplace has been an increasingly prominent area of legal discussion, particularly with respect to the off-duty activity of applicants, which applicants strongly believe should not be the prospective employer's concern.[93]

However, claims of invasion of privacy require that the claimant have a *reasonable* expectation of privacy.[94] Applicants are not always aware of this hence often seek the ability to control their off-duty conduct regardless of a reasonable expectation of privacy.[95] Applicants believe that what they do out of the office/job "should be of no concern to their employer" and should not be a factor in employment decisions[96] i.e. they want to partake in off-duty conduct without fear of suffering possible negative consequences at the hands of their employers as a result of such conduct.[97]

---

[90] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 13.
[91] Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', 25.
[92] Byrnside I, 'Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants' 10 *Vanderbilt Journal of Entertainment & Technology Law* (2008), 8.
[93] Sugarman SD, '"Lifestyle" Discrimination in Employment', 24 *Berkeley Journal of Employment & Labor Law* 2003, 32.
[94] California v. Greenwood, 486 U.S. 35, 39-40 (1988).
[95] Sugarman SD, '"Lifestyle" Discrimination in Employment', 380.
[96] Sugarman SD, '"Lifestyle" Discrimination in Employment', 380.
[97] Sugarman SD, '"Lifestyle" Discrimination in Employment', 406.

Essentially, applicants are seeking "a notion of personal autonomy or self-identity."[98]

Many users are unaware of the fact that they can tailor their social media profiles to allow only for specific certain viewers of their content, and "only a small number of members change the default privacy preferences, which are set to maximize the visibility of user profiles."[99] This creates in users "a sense of false security that they're broadcasting only to their personal crowd."[100] Despite applicants' beliefs that much of what they do online is private this is not the case and employers continue to access this information.

Based on the above arguments, there can be no privacy for what has been made public. Therefore, there is no privacy in a public space in so far as no steps have been taken by the individual to ensure that the information they are transmitting over the internet is secure and shielded from prying eyes. Consequently, employers should be able to vet an employee based on social media profiles in so far as the employer accesses only public information with the goal of finding the best fit for his/her company. In the event that an employer requires applicants to provide their social networking passwords during the job application process, the employer should be guilty of gross violation of a fundamental human right and hence should be held liable for discrimination in employment.

---

[98] Sugarman SD, '"Lifestyle" Discrimination in Employment', 406.
[99] Gross R and Acquisti A, 'Information Revelation and Privacy in Online Social Networks', *Workshop on Privacy in the Electronic Society* (2005), 10.
[100] 'Professor Ira Steven Nathenson: Facebook: Job-Hunting, Non-Invisibility, and the Creepiness Factor' *Professor Nathenson Blog*, 12 June 2006 http://www.nathenson.org/2006/06/facebook/ on 16 December 2015.

CHAPTER 4 – COMPARATIVE STUDY OF LEGISLATION IN THE US, THE UK AND KENYA

Employers often seek as much information as possible about job applicants to ensure the best fit between an applicant and the employer's organization.[101] In order to obtain such information, employers have utilized a vast number of information-gathering techniques; the techniques employed depend largely on the position to be filled. [102] Ultimately, employers seek employees with characteristics that will maximize work productivity[103] and minimize costs and liability.

Historically, employment pre-screening techniques for gathering information about applicants have included written applications, questionnaires, interviews, references (personal references and previous employment references), background checks, credit checks, and a variety of pre-employment tests, such as polygraph, psychological, medical, drug, and ability tests.[104] Over the past few years, in an effort to increase the productivity of their work forces and decrease their potential liability, employers have begun gathering an increasing amount of information about applicants through various new sources[105] due to technological advancements. These advances, e.g. social networking sites, are constantly making it easier for employers to obtain information about applicants and employees.[106] *"[T]he more economical it becomes to obtain information about a potential employee's private life, the greater the likelihood employers will use it."*[107]

4.1 The United States

In the US, some of these methods may raise issues of discrimination under **Title VII of the Civil Rights Act of 1964 (Title VII)**[108] and the **Americans with Disabilities**

---

[101] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 14 *Hofstra Labor Law Journal* (1997), 3.
[102] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 5.
[103] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 4.
[104] Byrnside I, 'Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants', 4.
[105] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 5.
[106] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 6-7.
[107] Byrnside I, 'Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants', 9.
[108] Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e to 2000e-17 (2000)

Act (the ADA).[109] Title VII is the primary federal anti-discrimination statute[110] and it prohibits employers from discriminating against applicants and employees "*because of such individual's race, colour, religion, sex, or national origin.*"[111] However, while most courts have held that, under Title VII, employers may ask "*questions that elicit information concerning protected class status*," so long as the information is not used in the decision-making process, [112] such questions may suggest discrimination or a discriminatory intent. [113] Moreover, proving that discrimination was absent from the decision-making process after asking these questions may be hard.

The Equal Employment Opportunity Commission's Guide to Pre-Employment Inquiries [114] (hereafter EEOC Guide) advises against asking questions directly concerning protected class status and neutral questions that may have a disparate impact on members of a protected class, as such questions could provide "*evidence of discrimination prohibited by Title VII.*" [115] The EEOC Guide explains that employment decisions based upon such questions violate Title VII "*unless the information is needed to judge an applicant's competence or qualification for the job in question.*"[116]

In the same vein, the ADA prohibits discrimination in employment decisions against "*an individual with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires.*"[117] However, it permits employers to inquire as to the ability of applicants to perform job-related functions. [118] The EEOC claims that this prohibition "*helps ensure that an applicant's possible hidden disability (including a*

---

[109] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 18; Americans with Disabilities Act, 42 U.S.C. §§ 12111-12117 (2000)
[110] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 17.
[111] 42 U.S.C. § 2000e-2.
[112] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 17; *Bruno v. City of Crown Point*, 950 F.2d 355, 363-65 (7th Cir. 1991).
[113] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 17.
[114] http://www.eeoc.gov/laws/practices/ on 9 December 2015.
[115] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 18.
[116] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 18.
[117] 42 U.S.C. § 12111(8)
[118] 42 U.S.C. § 12112(d) (2)

prior history of a disability) is not considered before the employer evaluates an applicant's non-medical qualifications."[119] According to the EEOC, employers may not ask applicants any disability-related questions or any questions indirectly related to an applicant's disability status.[120] Therefore, employers asking questions related to disabilities may be in violation of the ADA even if such information is not used in the decision-making process.[121]

Employers aren't allowed to discriminate based on a number of criteria including sexual orientation and race but all this information can be found on the profile of a prospective employee on their social networking website. Therefore, when an employer views a social networking site e.g. Facebook for the profile of an applicant and is able to access information that, under the aforementioned Acts, will be considered protected for discrimination purposes, then they may have discrimination lawsuits against them in the event that the qualified applicant in a particular protected class isn't selected for that particular job. This is because it will be difficult to defend against a discrimination claim if social networking profiles are the basis of their hiring of applicants.[122] Even though questions regarding topics such as religion and race aren't essentially illegal, employers avoid asking them as they typically have "no legitimate, job-related reason for asking them, and they are suggestive of unlawful discriminatory motives."[123]

4.2 The United Kingdom

In the UK, an Advisory, Conciliation and Arbitration Service (ACAS) Research Paper in 2013 found that 34.5%[124] of employers use social media to recruit employees while 15.5%[125] planned to start doing so in the future. Employers are

---

[119] Equal Employment Opportunity Commission, Notice No. 915.002, Ada Enforcement Guidance: Pre-employment Disability-Related Questions and Medical Examinations 1 (1995) http://www.eeoc.gov/policy/docs/preemp.html on 14 December 2015.

[120] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 19.

[121] Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 19.

[122] 'Frauenheim E: Caution Advised When Using Social Networking Web Sites for Recruiting, Background Checking' *Workforce*, 14 November 2006 http://www.workforce.com/section/06/feature/24/58/49/245851.html on 16 December 2015.

[123] Byrnside I, 'Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants', 19.

[124] Broughton A, Foley B, Ledermaier S and Cox A, 'The use of social media in the recruitment process' *ACAS* (2013), 60.

[125] Broughton A, Foley B, Ledermaier S and Cox A, 'The use of social media in the recruitment process', 56.

therefore urged to adhere to the Employment Practices Data Protection Code of 2002 [126] as the term 'worker' in the Code encompasses both successful and unsuccessful applicants, former applicants, employees and staff, former employees and staff, and others in the workplace, e.g. volunteers and interns.[127] This Code was created by the Information Commissioner pursuant to Section 51 of the Data Protection Act which requires him to promote compliance with the Act[128] and after consultation, to prepare Codes of Practice giving guidance on good practice.[129] The Code doesn't create new legal obligations but reflects and simplifies the contents of the Act. It also deals with the impact of data protection on the employment relationship. With regard to employment applications, it requires employers to:

i. Only seek personal information that is relevant to the recruitment decision to be made;[130]

ii. Explain the nature of and sources from which information might be obtained about the applicant in addition to the information supplied directly by the applicant;[131] and

iii. Assess whether the collection of sensitive data is relevant to the recruitment process and explain the purpose of collecting such sensitive information.[132]

The Code is concerned with personal information which it defines to include information about a living person and affects that person's privacy and identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.[133] It, therefore, includes automated and computerized personal employee information kept by employers.[134]

---

[126] Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016.
[127] Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016, 6.
[128] Section 51 (1), Data Protection Act (1998)
[129] Section 51 (3), Data Protection Act (1998)
[130] Section 1.2.2, Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016.
[131] Section 1.2.4, Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016.
[132] Section 1.2.5, Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016.
[133] Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016, 6.
[134] Employment Practices Data Protection Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf on 8 January 2016, 7.

On 22 July 2014, the House of Lords ordered the Communications Committee, a Select Committee established in 2007 by the House of Lords to look at a broad range of communications and broadcasting public policy issues and highlight areas of concern to Parliament and the public,[135] to print a report on Social Media and Criminal Offences[136] to be printed. The court, in the report, stated that,

"...there are aspects of the current statute law which might appropriately be adjusted and certain gaps which might be filled. We are not however persuaded that it is necessary to create a new set of offences specifically for acts committed using the social media and other information technology."[137]

Therefore, even though the UK courts recognize the presence of social media vetting, there is currently no law to deal with the issue as the court feels that the issue can be resolved using existing legislation. This is still a step ahead of Kenya whose courts have been mum on the issue and there are no cases to date that have been filed with the complaint.

4.3 Kenya

As it stands, there is no law in Kenya that governs the use of social media to vet employees in the workplace and there has been no case law touching on the same. Nevertheless, various instruments deal with the right of privacy which is a right enshrined in the COK (2010). It specifically states that all individuals have a right to privacy under Article 31 and this includes privacy of communications[138] which should reasonably include social networking sites in the event that the messages or pictures posted are set to be private in nature on the platform. An employer, therefore, cannot circumvent these privacy settings so as to gain information about an applicant as this will be against the right to privacy.

Article 27 (5) also states that a person shall not discriminate directly or indirectly against another person on any ground, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience,

---

[135] http://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/role/ on 8 January 2016.

[136] House of Lords Special Committee on Communications, *Social Media and Criminal Offences*, 22 July 2014.

[137] House of Lords Special Committee on Communications, *Social Media and Criminal Offences*, 22 July 2014 http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm#n18on 8 January 2016.

[138] Article 31 (d), COK (2010)

belief, culture, dress, language or birth. The COK (2010) is echoed by the Employment Act[139] which stipulates that there shall be no discrimination in the workplace against an employee or a prospective employee or harassment of an employee or a prospective employee under Section 5 (3). The Employment and Labour Relations Court Act[140] gives the court exclusive original and appellate jurisdiction to hear and determine all disputes relating to or arising out of employment between an employer and an employee.[141] This jurisdiction extends to issues that arise during employment hence this court will have the jurisdiction to listen to a case claiming discrimination in employment due to the use of social media.

Article 2 (5) and (6) state that the general rules of international law shall form part of the law of Kenya and that any treaty or convention ratified by Kenya shall form part of the law of Kenya respectively. Therefore, the International Labour Organisation (ILO) standards apply to employment practices in Kenya and in particular, the ILO Convention Concerning Discrimination in Respect of Employment and Occupation (No 111)[142] precludes discrimination in employment under Article 1.

The National Youth Employment Authority Bill of 2015 states that its purpose includes facilitation and promotion of equity and diversity; and elimination of discrimination in the employment youth[143] in the national and county governments, the private sector and the informal sector.[144] The National Youth Employment Authority is required to keep an updated register consisting of all the youth seeking employment in the country[145] containing information about these youth including their ethnicity and disabilities. In this case, no discrimination occurs as the Bill proposes that express consent has to be given by the youth as to what information to share with prospective employers[146] and contravention of this attracts a fine of up to

---

[139] Act No. 11 of 2007
[140] Chapter 234B

[141] Section 12 (b), Labour Relations Court Act (Chapter 234B)
[142]Geneva, 42nd ILC session, 25 Jun 1958 http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312256:NO on 10 October 2015.
[143] Section 3 (e), National Youth Employment Authority Bill (2015)
[144] Section 4, National Youth Employment Authority Bill (2015)
[145] Section 25, National Youth Employment Authority Bill (2015)
[146] Section 26, National Youth Employment Authority Bill (2015)

one million shillings.[147] This is because the Authority is to take the rights of the youth very seriously especially the right to privacy.[148] The Bill, nonetheless, doesn't make any reference to privacy on social media.

The US, as opposed to Kenya, has more decisions on privacy in the public space based on the laws that it has hence can be considered many strides ahead of Kenya in answering the question of the use of social media in hiring decisions in employment.

[147] Section 28, National Youth Employment Authority Bill (2015)
[148] Section 27, National Youth Employment Authority Bill (2015)

CHAPTER 5 – RECOMMENDATIONS AND CONCLUSION

Since there is currently no direct law to apply to social media in employment, then the normal provisions of the Employment Act with regard to discrimination should apply. Parliament should come up with laws that address such emerging sectors of the society as such cases may lead to oppression before proper guidelines are established on what to do in these situations. It should consider creating laws that better define the right to privacy especially in the context of online privacy. These laws should consider that privacy cannot be offered in a public space but in the event that a person takes reasonable steps to protect themselves e.g. through engaging privacy measures on social networking sites, then circumventing these measures should be considered as an invasion of privacy.

Laws protecting the employer's right to seek information should also be enacted with technological advancements in mind. For example, employers should be able to ask for social networking profiles of job applicants depending on the nature of the site such as professional networks e.g. LinkedIn[149] as opposed to social networking sites that have a mix of both professional and personal information that might lead to bias during the hiring process e.g. Twitter and Facebook. Nevertheless, information that can lead to discrimination of an applicant should not be part of the information required in the hiring process.

Employers should publicize the methods used to vet applications and make this known with reasons to applicants. This will help them prevent violation of employment laws in the event that they inform applicants that social media profiles are considered in the vetting process. However, employers should keep in mind that many candidates edit their profiles so as to appeal to a potential employer and so their social media search may be fruitless. [150]

Using social media accounts to vet applicants should be undertaken late in the hiring process so as to prevent the loss of talented applicants based solely on their online profiles. Employers should also work hand in hand with employees to create clear

---

[149] https://www.linkedin.com/ on 6 January 2016.

[150] Using Social Media in the Recruitment Process, Robert Walters *Insight Series*, https://www.robertwalters.co.uk/content/dam/robert-walters/country/united-kingdom/files/whitepapers/rw-social-media-whitepaper.pdf on 8 January 2016, 10.

policies on the use of social media in the recruitment process[151] so as to make the exercise effective.

Article 33 of the COK (2010) guarantees the freedom of expression which includes freedom to seek, receive or impart information or ideas; freedom of artistic creativity; and academic freedom and freedom of scientific research. Therefore, every individual [152] has the right to post whatever they want on their social networking sites but they should be prudent as information on the internet is permanent and may have serious repercussions on a person's life. Individuals should, therefore, delineate their professional from their personal lives and contextual integrity should be exercised as applicants cannot claim privacy for content that has been made public.

[151] Pre-employment checks: an employer's guide, http://www.cipd.co.uk/binaries/pre-employment-checks_2013.pdf

[152] Article 19 (3) (a), COK (2010)

BIBLIOGRAPHY

Book Chapters

1. Schoeman F, 'Privacy and Intimate Information' in Schoeman F (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.
2. Schoeman F, 'Gossip and Privacy' in Goodman RF and Ze'ev AB (ed.) *Good Gossip*, University Press of Kansas, 1994.
3. Hunter L, 'Public Image' in Johnson D and Nissenbaum H, *Computers, Ethics, and Social Values*, Englewood Cliffs: Prentice Hall, 1995, 294.

Journal Articles

1. Befort SF, 'Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place', 14 *Hofstra Labor Law Journal* (1997).
2. Brandenburg C, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare' 60 *Federal Communications Law Journal* (2007).
3. Broughton A, Foley B, Ledermaier S and Cox A, 'The use of social media in the recruitment process' *ACAS* (2013).
4. Byrnside I, 'Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants' 10 *Vanderbilt Journal of Entertainment & Technology Law* (2008).
5. DeCew JW, 'In Pursuit of Privacy: Law, Ethics, and the Rise of Technology' *Cornell University Press* (1997).
6. Fried C, 'Privacy' 77 *The Yale Law Journal* (1968).
7. Gavison RE, 'Privacy and the Limits of the Law' 89 *The Yale Law Journal* (1980).
8. Gerety T, 'Redefining Privacy' 12 *Harvard Civil Rights-Civil Liberties Law Review* (1977).
9. Gross R and Acquisti A, 'Information Revelation and Privacy in Online Social Networks', *Workshop on Privacy in the Electronic Society* (2005), 10.
10. Kluemper DH and Rosen PA, 'Future employment selection methods: evaluating social networking web sites' 24 *Journal of Managerial Psychology* (2009), http://www.internetlivestats.com/internet-users/ on 2 March 2015.

11. Madera JM and Chang W, 'Using Social Network Sites to Investigate Employees in the Hospitality Industry' *International CHRIE Conference-Refereed Track*, Amherst, 27 July 2011, http://scholarworks.umass.edu/cgi/viewcontent.cgi?Articleicle=1643&context=refereed on 8 August 2015.
12. Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' 17 *Law and Philosophy* (1998).
13. Parent W, 'Privacy, Morality, and the Law' 12 *Philosophy & Public Affairs* (1983).
14. Rachels J, 'Why Privacy is Important' 4 *Philosophy & Public Affairs* (1975).
15. Reiman JH, 'Privacy, Intimacy and Personhood' 6 *Philosophy & Public Affairs* (1976).
16. Sprague R, 'Orwell was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees' 42 *John Marshall Law Review* (2008).
17. Strahilevitz JL, 'A Social Networks Theory of Privacy' 72 *The University of Chicago Law Review* (2005).
18. Sugarman SD, '"Lifestyle" Discrimination in Employment', 24 *Berkeley Journal of Employment & Labor Law* (2003).
19. Wall DS, 'The Internet as a Conduit for Criminals' in Pattavina A (ed), *Information Technology and the Criminal Justice System*, Sage Publications Inc., revised 2015.
20. Westin AF, 'Privacy and Freedom' 25 *Washington and Lee Law Review* (1968).