Strathmore University
Law School

Strathmore
UNIVERSITY

The Prosecutor in Your Pocket: A Study on the Constitutional Issues Arising Out Of the Use of Social Media Evidence in Government Investigations With a Specific Focus on the Right to Privacy

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE BACHELOR OF LAWS DEGREE

SUBMITTED BY:

STUDENT'S NAME: MUIGAI KENA MICHAEL

STUDENT'S REGISTRATION NUMBER: 072271

SUBMITTED TO:

STRATHMORE UNIVERSITY LAW SCHOOL

NAME OF SUPERVISOR: _____

SIGNATURE OF SUPERVISOR: _____

DATE: _____ DOUGLAS GICHUKI

Table of Contents

Acknowledgements

To the unmoved mover, my inexhaustible appreciation for existence, this rock orbiting our star and the patience to watch us mess it up without smiting us.

To my family and especially my mother, Salome Muigai, I am honoured to be a direct descendant of you and yours. Thank you for everything.

To Dr Franceschi, Mrs Muindi, Mr Muchemi and the rest of the Strathmore Law School my immortal gratitude for your patience and indulgence. Special mention to my mentor and supervisor Mr Gichuki, I shall not forget the long and fruitful discussions on the intricacies of law and life.

Finally to my companions upon this path Garnet and Co, FALS, Nyamongo, Githaiga, Ombachi, Mtula and Mwangi, my undying gratitude for your support and friendship, may this be merely the first lap.

Abstract

Today, individuals network and interact with each other in radically different ways, using social networking sites such as Facebook and Twitter. Utilizing this new media, individuals are able to share intimate details of their lives, coordinate activities, and exchange ideas with friends, family and others in ways previously accomplished only in person, by telephone, or in written letters stored in one's home. At the same time, social networking sites are increasingly being utilized by terrorist entities for both recruiting purposes and for the planning, financing, and execution of terrorist acts, as well as by other criminal actors. As such social networks have become a valuable source of intelligence for the law enforcement and intelligence communities, enabling the collection of information pertaining to individuals in ways not previously possible. However, the law pertaining to surveillance in cyberspace has failed to keep pace with society's adoption of social networking and other cloud computing technologies. This paper examines the privacy safeguards inherent in the article 31 of the Kenyan Constitution 2010 and Fourth Amendment to the American Constitution and the need to strike an appropriate balance between an individual's reasonable expectations of privacy in one's online communications and the government's intelligence requirements necessary to combat emerging criminal and terrorist threats.

List of Abbreviations

CAK - Communications Authority of Kenya

CCK – Communications Commission of Kenya

CoK – Constitution of Kenya 2010

DPP - Director of Public Prosecutions

ECOWAS - Economic Cooperation of Western African States

FBI- Federal Bureau of Investigation

HTTP - Hypertext Transfer Protocol

ICCPR - the International Covenant on Civil and Political Rights

IP - Internet Protocol

ITU - International Telecommunication Union

KICA - Kenya Information and Communications Act

LSK - Law Society of Kenya NEWS - Network and Early Warning systems

NIS – National Intelligence Service

NSA- National Security Agency

SMTP - Simple Mail Transfer Protocol

TOS – Terms of Service

UDHR - the Universal Declaration of Human Rights

UN – United Nations

WWW- World Wide Web

List of Cases

Chapter 1

Nothing was your own except the few cubic centimetres inside your skull.

-George Orwell, Nineteen Eighty-Four

Background

We are no doubt living the Chinese curse[1]; interesting times are indeed upon us. The information age, the digital and perhaps most apt the Big Data age, are all titles that have been used to describe the current period of existence. Upon the foundation of the internet, social media companies have built titanic repositories of data; Facebook collects data on all a person's significant life events, education and job achievements, family members and friends, locations they visit, telephone numbers, photos taken by the user and photos of the user, to name but a few. Google collects all this and more through 'Plus', their social network, and browser history, patterns and searches, of all users of their overwhelmingly popular search engine. The currency of the internet is your data. The big social media companies collect, collate, and organise your data in terms of various demographics such as gender, age, interests, shopping history and search results. This data and information is however not limited to its commercial use[2], police investigators and prosecutors have discovered a digital goldmine of potential evidence in profiles, tweets, friends lists, messages, chat log, tags, videos, GPS locations and login timetables.[3] Government involvement is however only reasonable considering the rise of diversified online criminality, ranging from the recruitment of mujahideen to join the Islamic state via social media[4] and the proliferation of dissemination of child pornography[5] via channels such as the dark net in jurisdictions such as ours without specific laws to address these emerging issues.

---

[1] This saying is apocryphal, as no verifiable Chinese source has been proved. See Bryan W. Van Norden. *Introduction to Classical Chinese Philosophy,* Indianapolis: Hackett, 2011, 53

[2] http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal, Jonathan Shaw

[3] Quagliarello v. Dewes, No. 09-4870, 2011 WL 3438090 at 2 (E.D. Pa. Aug. 4, 2011) ("As the use of social media such as MySpace and Facebook has proliferated, so too has the value of these websites as a source of evidence for litigants.")

[4] Faisal Irshaid, How Isis is spreading its message online, 19th June 2014, available at: http://www.bbc.com/news/world-middle-east-27912569, retrieved 21st of January 2016.

[5] Patrick Howell O'Neill, How the world's police are taking on the Dark Net, Sep 22, 2015, available at: http://www.dailydot.com/politics/fbi-dark-net-cybercrime-global-police/ ,retrieved 21st of January 2016.

Social media evidence in government investigations and criminal litigation has emerged as a new legal grey area, especially with regard to the manner in which this evidence is obtained. Here in Kenya the National Intelligence Service Act, 2012 at section 45 grants security agencies the powers to monitor communications as well as to "search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing." It describes the term 'monitor' as the "means to intercept, listen to, record or copy using any device." The article further states that, a member of the intelligence service needs to obtain a warrant for authorisation to conduct monitoring. That said, the law does not state in detail what kinds of communications may be monitored and does not use the term 'interception'. Kenya does not have a stand-alone law on interception of communications.

However there exist the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations, 2012, January 4, 2013,[6] which at section 15 state, "A licensee shall grant the Commission's officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations." Effectively allowing for the unwarranted seizure of all telecommunication records (read telephone and cellular data, records).

Given the aggressive, intrusive and possibly unconstitutional nature of these regulations and the relative calm with which they were accepted by the Kenyan populace,[7] it is not unreasonable to point out the internet, and particularly social media websites, as the next platform open to whimsical or at least unwarranted seizure by the government.

Statement of Problem

Given the abundance of both public and private information available on the social media platform; should, and to what extent should, evidence obtained via social media be limited by article 31 of the Constitution of Kenya 2010?

---

[6]Section 15, Kenya Information and Communications Regulations (2012). Available at http://216.154.209.114/regulations/downloads/REGISTRATION_OF_SUBSCRIBERS_OF_TELECOMMUNICATION_SERVICES_REGULATIONS.pdf.

[7] This apathy may be attributed to the fact that a majority of Kenyans were raised at least partially during the Moi regime and therefore do not consider the idea of telecommunication records being openly available to the government as particularly outlandish.

Statement of objectives

To shed light on the possible loopholes present in Kenyan law in regard to the government's use of social media in criminal investigations, this includes the manner in which said evidence is obtained and the admissibility and constitutionality of this evidence and the Kenyan criminal cases it is used in.

Research Questions

i. Do the current Kenyan laws on warranted and unwarranted search apply to private social media accounts, in the same way they apply to physical private property?
ii. Is the acquisition of a user's private social media information in violation of article 31 of the Constitution?
iii. Is the term privacy in social media analogous to the constitutional interpretation of privacy?

Literature Review

Ken Strutin; Social Media and the Vanishing Points of Ethical and Constitutional Boundaries

Strutin opines that the tension in social networking investigations is in drawing the line between public and private information. The privacy dilemma lies at the centre of a triangle formed by the private enclaves envisioned in the First, Fourth, and Fifth Amendments; service providers" terms of service agreements (TOS) and their definitions of privacy; and the meaning of "reasonableness" as expressed in the practices and habits of millions of online users.

He goes on to pose the question, how do privacy settings and terms of service affect the expectation of privacy in social media? If the expectation is that online profiles are as private as a person's home, desk drawer, or combination safe, then pretexting[8] by private parties becomes problematic. However, this protean media does not offer clarity in its definitions of

[8] 'Pretexting' the practice of presenting oneself as someone else in order to obtain private information.

privacy, and those definitions change with advances in technology and public outcry. Meanwhile, courts are relying on subjective expectations to define privacy in social space.

Social media are analogous to open mikes. However, the unguarded remarks of millions who publish their thoughts, criticisms, and gossip on personal profiles are made under an assumed veil of privacy. The public privacy of social networking has not yet been clearly assigned a specific level of First, Fourth, or Fifth Amendment protections. In relation to Kenya, this argument can be made for article 31 which encompasses all the privacy issues highlighted in the three amendments to the United States' constitution.

Susan W. Brenner, The Privacy Privilege: Law Enforcement, Technology and the Constitution[9]

The First Amendment protects the privacy of the identity and associates of an individual; the Fourth Amendment protects the privacy of the activities of an individual; and the Fifth Amendment protects the privacy of the thoughts of an individual. The degree to which they protect these different privacy interests has evolved significantly since Justices Brandeis and Warren wrote in 1890.[10] This evolution is directly attributable to the increased sophistication and proliferation of technology. This evolution is also responsible for the shift from the *Olmstead*[11] holding to the *Katz*[12] holding. When the decision was made by the *Olmstead* Court, wiretaps were in their infancy and were therefore an exceedingly uncommon event. By the time the decision was made by the Katz Court, surveillance technology had become very sophisticated, due in large part to advances made during World War II, and the ability of the government to spy on the activities of people had become a matter of public concern. In changing the focus of the privacy protections of the Fourth Amendment from places to people, the *Katz* Court sought to create a more dynamic standard, one that could be used to address the increasing invasiveness made possible by technology.

---

[9] Brenner, Susan W., The Privacy Privilege: Law Enforcement, Technology and the Constitution, *Journal of Technology Law and Policy*, Volume 7, 2002.
[10] Brandeis and Warren, The Right to Privacy, *Harvard Law Review,* Volume IV December 15, 1890 .
[11] Olmstead v. United States 277 U.S. 438, 48 S. Ct. 564, 72 L. Ed. 944 (1928)
[12] Katz v. United States 389 U.S. 347 (1967)

Justin P. Murphy and Adrian Fontecilla: Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues

In this Article Murphy and Fontecilla while discussing a defendant's constitutional rights regarding social media evidence, tackled the issue through an analysis of three main American Cases; *People v Harris* [13], *United States v Warshack*[14] and *United States v Meregildo.*[15]

In *People v Harris*, the Defendant, Malcolm Harris, was one of hundreds of people arrested on disorderly conduct charges for marching onto the Brooklyn Bridge on Oct. 1, 2011, as part of the Occupy Wall Street protests. The district attorney's office subpoenaed Twitter for a broad swath of information about Harris, including the content of his tweets, his subscriber information, and the Internet Protocol (IP) addresses that correspond to each time he used Twitter over a three-and-a-half month period – information that would reveal Harris's location whenever he was using Twitter. Harris moved to quash the subpoena. In April, a judge ruled that Harris had no standing to challenge the Twitter subpoena. The judge also determined that the subpoena is lawful and ordered Twitter to comply with it. Harris subsequently filed a motion to reargue, and Twitter weighed in with a motion to quash the court's order.

The authors highlight a number of issues:

a) The court's rejection of the defendant's move to quash the subpoena, based on the argument that the Fourth Amendment did not protect his tweets. It is important to note that the defendant was only able to file his motion, due to Twitter's Policy on notifying its users of requests for their information prior to disclosure.[16] Not only does Twitter inform its users of such request, it also litigates against such third-party government subpoenas.[17]

---

[13] People v Harris, 945 N.Y.S.2d (N.Y. Criminal Court 2012)
[14] United States v Warshack, 631 F.3d (6th Cir. 2010).
[15] United States v Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y August 10, 2012)
[16] Guidelines for Law Enforcement, TWITTER, http://support.twitter.com/entries/41949- guidelines-for-law-enforcement#section9 (last visited Jan, 15, 2013).
[17] Somini Sengupta, Twitter's Free Speech Defender, N.Y. TIMES, Sept. 3, 2012, at B1, available at http://www.nytimes.com/2012/09/03/technology/twitter-chief-lawyeralexander-macgillivray-defender-free-speech.html?pagewanted=all&_r=0.

b) The court's rejection of Twitter's move to quash the government's subpoena based on the same reasons. Although the appeal is still pending, Twitter handed over the data on the Trial Judge's threat of civil contempt and fines. This information eventually led to a guilty plea in December 2012.

On appeal, Twitter argued that the government was in clear violation of the Fourth Amendment which (it claimed) protected the user's tweets due to the fact that the government conceded that the tweets it sought had not been made public by the defendant. If a defendant has a reasonable expectation of privacy, the Fourth Amendment, as recognised in regard to non-public e-mail (as affirmed in *United States v Warshak*), not granting the same protection to non-public tweets would create "arbitrary line drawing."

The line-drawing concerns, that the Fourth Amendment's reasonableness requirement depends on the privacy settings used by the account in question, were underscored in the case of *United States v Meregildo*, wherein the courts held that "where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment."[18] Further, some courts have concluded that individuals have "a reasonable expectation of privacy to [their] private Facebook information and messages." Those courts, while recognizing the importance of properly understanding how Facebook works, distinguished between "private messaging" and posts to a user's Facebook wall. Using privacy setting distinctions to determine social media users' constitutional rights may result in arbitrary line drawing that might evaporate as social media evolves. Indeed, with Facebook's customizable and post-specific privacy settings, a person who shares a message by posting it on another user's wall can actually make it as private as information shared via a Facebook message.

Theoretical Framework

According to the social contract, we trade the state of nature to form a society and enjoy protection, security, and property.[19] To protect our values, we create laws tasked with the goal of "securing a situation whereby moral goals which, given the current social situation in the

[18] United States v. Meregildo.

[19] John Locke, *The Second Treatise of Government* 48–50 ,Thomas P. Peardon ed., The Bobbs-Merrill Co. 1952, (1690); Jean Jacques Rousseau, *The Social Contract* 12–15 ,Willmoore Kendall trans., Henry Regnery Co. 1954, 1762.

country whose law it is, would be unlikely to be achieved without it." The law should serve the common interest and secure values that will be broadly useful to society. Once established, the law must be enforced since the government derives authority from creating and enforcing laws. Thus, there is an immediate, positive benefit when we protect a valued good like privacy. Additionally, there is a broader benefit, as enforcing the law gives the government credibility and creates a stable society.[20]

The privacy claim is best seen as a statement about the social contract and the rights granted the sovereign therein. The sovereign, as a beneficiary under, or party to, the social contract, is not the entity that should have the authority to interpret the social contract. Since sovereignty in our system is in the people, the legislature, speaking for the majority, is the organ generally exercising sovereignty. The legislature, then, should not have the authority to determine the scope of authority given the sovereign. Instead, that branch of government most removed from the sovereign, the courts, should make such decisions.[21]

Research Design & Methodology

The paper shall be based on the collation of qualitative data obtained from primary, secondary and tertiary sources. These include, but are not limited to, analysis of information from online resources, journals and articles, reports from relevant organisations, text books, case law, news articles, and statute.

Limitations

The research shall be founded and based mainly upon the geographical region of Kenya, with significant reference to American jurisprudence, journals and other relevant publications. However, information on the field of research may be drawn from other regions for purposes of comparison and guidance in coming up with solutions to the problem.

Chapter Breakdown

Chapter 1: The Research Proposal

Chapter 2: Conceptual Framework

---

[20] http://www.regent.edu/acad/schlaw/student_life/studentorgs/lawreview/docs/issues/v25n1/05Sundquistvol.25.1.pdf

[21] Kevin W. Saunders, Privacy and Social Contract: A Defense of Judicial Activism in Privacy Cases, 33 *Arizona Law Review* 811, (1991).

In this chapter the conceptual framework upon which modern privacy law is based is explored. Four conceptualisations of privacy are highlighted, analysed and their criticisms mentioned in order for us to form a balanced and diverse lens of ideas through which to view the issues addressed in this paper through.

Chapter 3: Web 2.0, Big Data and Governments

The third chapter defines the Internet, the World Wide Web, and technologies inherent in their architecture, enabling widespread creation and storage of personal data from persons with access to this technology. A discussion on social media terms of service agreements in relation to governmental requests and the manner in which courts have handled them is held.

Chapter 4: An analysis of the current state of the Kenyan law relevant to Social media Evidence acquired by Government Institutions and its constitutionality

The penultimate chapter deals with the Kenyan laws and international obligations in force in Kenya, relevant to the issues of privacy and social media.

Chapter 5: Conclusion and recommendations.

The final chapter summarises the issues and arguments raised throughout the paper and suggests a number of recommendations to the problems highlighted and discussed.

Chapter 2: Conceptual Framework

The soul selects her own society

Then shuts the door;

On her divine majority

Obtrude no more.[22]

The Concept, Privacy

Privacy as a term has proved difficult to pin down under one particular definition or specific meaning. The concept of privacy is even more sweeping, dealing with solitude in one's home, control over information about oneself, their family and personal affairs,[23] freedom of thought and control of one's body, freedom from surveillance and protection from interrogations and searches. Numerous attempts to accurately conceptualise it have been attempted over the years by a myriad of minds from across the board of scholastic endeavour.[24] The twentieth century essayist Arthur Miller describes it as "exasperatingly vague and evanescent."[25] Robert Post declares that "*privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.*"[26] "*Perhaps the most striking thing about the right to privacy*," Judith Jarvis Thomson observes, "*is that nobody seems to have any very clear idea what it is.*"[27] William Beaney has noted that "*even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right.*"[28] Privacy has "a protean capacity to be all things to all lawyers,' opines Tom Gerety.[29]

---

[22] Brinnen JM, ' Poems by Emily Dickenson' (1890), *in* Brinnen JM, *Emily Dickenson,* 17-18

[23] Article 31The constitution of Kenya (2010) article 31

[24] Inness JC., *Privacy, Intimacy, And Isolation,* Oxford University Press, (1992), 3.

[25] .Miller AR, *The Assault on Privacy: Computers, Data Banks, and Dossiers* , Signet, (1971) 25.

[26] Post R., 'Three Concepts of Privacy', 89 *Georgetown Law Journal*, 2087 (2001).

[27] Thomson J J, *'The Right to Privacy', in Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press (1984), 272.

[28] Beaney WM., 'The Right to Privacy and American Law', 31 *Law and Contemporary Problems* (Spring 1966) 253, *255*

[29] Gerety T, 'Redefining Privacy', 12 *Harvard Civil Rights-Civil Liberties Law Review, (1977)* 233, 234

For the purpose of establishing a lens (or perhaps more aptly several lenses) through which to perceive the topic at hand today, this chapter shall consist of an analysis of several conceptions of privacy and their respective critiques.

The Right to Be Let Alone

In the year 1890, two young Boston lawyers and recent graduates of Harvard University, authored what is debatably the most influential piece of privacy law literature the world has seen so far, simply named, The Right to Privacy.[30] The article ignited considerable public debate and inspired significant interest and attention to the privacy field; it created four common law tort actions in the defence of privacy and framed the discussion of privacy in the United States throughout the twentieth century and to this very day.[31]

Warren and Brandeis started off by noting the adoption of new technology and the potential threat it posed,[32] before going on to set out a framework enabling the common law to protect the interest they referred to as privacy. The writers however did not spend much time actually exploring the concept of privacy, the definition they used was "the right to be left alone" which they adopted from Judge Thomas Cooley's decision in 1880.[33] The right to be left alone according to Justice Cooley was used to explain that attempted physical touching was a tort injury; Warren and Brandeis however used the phrase in a manner consistent with the purpose of their article in order to prove that the right to privacy already existed in the common law. [34]

In the year 1888, a mere two years before Warren and Brandeis produced the seminal publication, the Right to Privacy, the Supreme Court of United States adopted Cooley's

---

[30]. Warren SD & Brandeis LD., The Right to Privacy, 4 *Harvard Law Review* (1890) 193

[31] Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy,* 10 *Northern Illinois University Law Review* 1990; 10(3): 479-520.Turkington observed:
"The article has acquired legendary status in the realm of legal scholarship. It is likely that *The Right to Privacy* has had as much impact on the development of law as any single publication in legal periodicals. It is certainly one of the most commented upon and cited articles in the history of our legal system."

[32] Dorothy J. Glancy, "The Invention of the Right to Privacy" ,*Arizona Law Review*, (1979),v.21, n.1 p 8:
"By 1890 there were also telegraphs, fairly inexpensive portable cameras, sound recording devices, and better and cheaper methods of making window glass."

[33] Thomas M. Cooley, Law Of Torts (2d ed. 1888). "As well said by Judge Cooley: 'The right to one's person may be said to be a right of complete immunity; to be let alone."' *Union Pac. Ry. Co. v. Botsford*, 141 U.S. 250,251 (1891).

[34] Solove, Daniel J., Conceptualizing Privacy, *California Law Review*, Vol. 90, p 15.

analysis of direct Fourth and Fifth Amendment protections against governmental invasions of individual privacy. In *Boyd v. United States*, Judge Bradley ruled:

"*The very essence of constitutional liberty and security is affected by all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property. . . .*" [35]

Warren and Brandeis went on to declare that the underlying principle of privacy was "that of inviolate personality." That the value of privacy was found not in the right to profit from the publication, but rather on the peace of mind stemming from the ability to prevent any such publication at all.[36] They opined that the mental pain and distress an individual could be subjected to through invasion of their privacy could prover far greater than that inflicted by bodily harm.[37] Yet this sort of harm received no form of protection under tort law. While defamation laws protected injuries to reputation, "injury to feelings," a psychological form of pain difficult to substantiate in that era of tort, which focused more on tangible injuries.[38]

Thirty eight years later, Brandeis now a Judge of the United States' Supreme Court, penned his powerful dissenting opinion in the famous case of *Olmstead v United States*.[39] In which he declared that the framers of the Constitution (US) "*conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilised men.*"[40] This opinion would prove the foundation upon which the right to privacy would be interpreted as having constitutional protection, specifically under the fourth amendment.

The *Olmstead* decision was eventually ruled in the 1967 Supreme Court case of *Katz v United States*,[41] in which the court adopted Brandeis's view and once again invoked the

---

[35] *Boyd v. United States*, 116 U.S. 616, 630 (1886).
[36] Warren, S & Brandeis L, The Right to Privacy, p 205
[37] Warren, S & Brandeis L, The Right to Privacy P 200
[38] Warren, S & Brandeis L. The Right to Privacy), P 197
[39] Olmstead v. United States, 277 U.S.
In which the court held that wiretapping was not a violation under the Fourth Amendment of the United States' Constitution because it was not a physical trespass into the home.
[40] Olmstead v. United States, 277 U.S, p 478 (Brandeis, J., dissenting).
[41] Katz v. United States 389 U.S. 347 (1967)

conceptualisation of the right to privacy as the right to be left alone.[42] According to Justice Douglas:

"The right of privacy was called by Mr. Justice Brandeis the right "to be let alone." That right includes the privilege of an individual to plan his own affairs, for "outside areas of plainly harmful conduct, every American is left to shape his own life as he thinks best, do what he pleases, go where he pleases."[43]

The right to be let alone can therefore be viewed as a sort of immunity. A major criticism of this definition is one that applies to the privacy debate as a whole, it is simply too broad. As the legal scholar Anita Allen puts it "*If privacy simply meant 'being let alone,' any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom.*"[44] Edward Bloustein, a noted legal theorist of privacy, observed that instead of developing a conception of privacy, Warren and Brandeis's article focused mostly on the gaps in existing common-law torts.[45]This particular school of thought is well summarised by D.J Glancy when she states "All that Warren and Brandeis ever claimed to have invented was a legal theory which brought into focus a common "right to privacy" denominator already present in a wide variety of legal concepts and precedents from many different areas of the common law."[46]

Limited Access to Self

This conceptualisation of privacy recognises humankind's desire for being apart from other people and their desire for concealment. It therefore overlaps heavily with the right to be left alone theory, and can be expressed as a more complex formulation of that right.

This definition however makes it rather easy to mistake limited access for a general leaning towards hermitage and seclusion, the distinction between these is best explained by the legal

---

[42] *See, e.g.,* Eisenstadt v. Baird, 405 U.S. 438, 454 n.10 (1972); Stanley v. Georgia, 394 U.S. **557,** 564 (1969); *Katz,* 389 U.S. at 350.

[43] Doe v. Bolton, 410 U.S. 179, 213 (1973) (Douglas, J., concurring)

[44] Anita L. **Allen,** Uneasy Access: Privacy For Women **In A** Free Society 7 (1988).

[45] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An* ***Answer*** *to Dean Prosser,* 39 *New York University Law Review* (1964), p 907

[46] Dorothy J. Glancy, "The Invention of the Right to Privacy", *Arizona Law Review*, v.21, n.1

scholar David Solove as he opines "*The limited-access conception is not equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of limited-access conceptions as well as of the right-to-be-let-alone conception, but these theories extend far more broadly than solitude, embracing freedom from government interference as well as from intrusions by the press and others. Limited-access conceptions recognize that privacy extends beyond merely being apart from others.*" [47]

The earliest proponent of the limited access is E.L Godkin a noteworthy late nineteenth century writer. Seemingly by coincidence Godkin writing in 1890 (the same year Brandeis and Warren published the Right to Privacy) defined privacy as the "right to decide how much knowledge of a person's personal thought and feeling.., private doings and affairs ... the public at large shall have."[48]

Without a specific notion of what issues are private, the limited access conception fails to specifically convey the substantive matters over which access would implicate privacy. It is certain that not all access to the self can be labelled privacy infringement, only access to particular information and specific dimensions of the self. As a result, this theory neither provides the amount of control a person should have over access to self nor an understanding of the degree of access necessary to constitute a breach of privacy. Therefore, much like the right to be left alone conception before it, the limited-access theory suffers from being too vague and too broad.[49]

Secrecy

A leading understanding of the concept of privacy constitutes it as the veil of secrecy over certain matters. From this perspective a violation of privacy occurs when previously concealed information is revealed to the public. According to Judge Richard Posner:

> *"The word 'privacy' seems to embrace at least two distinct interests. One is the interest in being left alone-the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theatre billboard or shouted obscenity.... The other privacy interest,*

[47] Solove, Daniel J., Conceptualizing Privacy. *California Law Review*, Vol. 90 pg 18
[48] E.L. Godkin, *The Rights of the Citizen, IV-To His Own Reputation,* SCRIBNER'S MAGAZINE, July-Dec. 1890, at 65
[49] Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90 pg 19

concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertain."[50]

The latter privacy interest, "*concealment of information*," involves secrecy. When talking about privacy as secrecy, 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. People "*want to manipulate the world around them by selective disclosure of facts about themselves*."

The conception of privacy as concealing information about the self forms the foundation for what is known as the constitutional right to information privacy. The constitutional right to information privacy is an offshoot of the United States Supreme Court's substantive due process "right to privacy" cases such as *Griswold v Connecticut*[51] and *Roe v. Wade*.[52] In *Whalen v. Roe*,[53] the Court held that the constitutionally protected "zone of privacy" not only protected an individual's "independence in making certain kinds of important decisions" but also encompassed the "individual interest in avoiding disclosure of personal matters." Consonant with the notion of privacy as secrecy, this formulation views privacy as avoiding disclosure.

A major criticism of the secrecy conception appears in complete contrast to the issues faced by the previous two conceptions. It is the opinion of a number of theorists that the conceptualisation of privacy as secrecy gives it too narrow a scope. They argue that equating secrecy to privacy fails to capture the possibility that an individual may want to keep some things private from some people and but not others. This is strengthened by the opinions of many courts which view secrecy as tantamount to total secrecy as opposed to a more selective interpretation. As Kenneth Karst aptly puts it, "*a meaningful discussion of privacy requires the recognition that ordinarily, we deal not with an interested in total nondisclosure but with an interest in selective disclosure.*"[54] In conclusion, as stated by the Philosopher Judith Wagner DeCew, privacy and secrecy are not coextensive, oftentimes secret information is not

---

[50] Posner, Richard A. (1981). *The Economics of Justice*. Harvard University Press, 103.
[51] Griswold v Connecticut 381 U.S. 479 (1965).
[52] Roe v Wade 410 U.S. 113 (1973).
[53] Whalen v Rose 429 U.S. 589 (1977
[54] Kenneth L. Karst, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 Law and Contemporary Problems, 342, 344 .

private (such as is the case with military strategy while) and matters considered private are not always secret (say an individual's debts.).[55]

> *"Then the eyes of both of them were opened, and they realized they were naked; so they sewed fig leaves together and made coverings for themselves[56]."*
>
> *"Then the LORD God called to the man, and said to him, "Where are you?" He said, "I heard the sound of You in the garden, and I was afraid because I was naked; so I hid myself." And He said, "Who told you that you were naked? Have you eaten from the tree of which I commanded you not to eat?"[57]*

Ubuntu and Privacy

> *"This person has Ubuntu! Because in our culture there is no such thing as a solitary individual, we say that a person is a person through other persons. That we belong in the bundle of life. And I want you to be all you can be because that is the only way I can be all I can be."[58]*

Ubuntu is hard to characterize concisely, yet could be best portrayed as a community based ideology in which the welfare of the group is held in greater regard than the welfare of a single individual in the community.[59] Ubuntu upholds a value system in appearing disagreement with current Western qualities. Western societies are fundamentally established on the political logic of Libertarianism, which puts a solid emphasis on the rights of the person with a specific intention of protecting and empowering them. On the opposite side of the range dwells the political philosophy of Communitarianism, which puts an accentuation on the

---

[55] Judith Wagner Decew, In Pursuit Of Privacy: Law, Ethics, And The Rise Of Technology, Cornell University Press, 1997, 48.

[56] The Bible, New International Version Genesis 3:7

[57] The Bible, New International Version Genesis 3:9-11

[58] Nobel Peace Prize recipient, Archbishop Desmond Tutu explains Ubuntu to the Semester at Sea class of Spring 2007.

[59] Kwamwangamalu, Nm. & Nkonko, M. Ubuntu in South Africa: a Sociolinguistic Perspective to a Pan-African Concept, *Critical Arts Journal* (1999), *Vol.13, No. 2: 24-42.*

good of the community, and particularly amid moral choices the contrast between the two sides gets to be obvious.[60]

Much of privacy legislation drafted so far seeks to protect the individual against the potential exploration and exploitation by powerful role players in possession of such personal information.

Justice Mokgoro clarifies that Ubuntu is basically an African philosophy of life, which mirrors the African approach and perspective while considering social, cultural and political parts of life.[61] Further, Justice Mokgoro states that Ubuntu is a metaphor that portrays community solidarity in a manner that the survival of the group relies on this solidarity of individuals to the community. The individual's presence and personality is with respect to the gathering. and is characterized by the gathering as well. This unmistakable difference is in glaring contrast to the Cartesian concept of individuality that states, "*I think, therefore I am*". The Ubuntu idea of uniqueness is more complex and multi-facetted and proposes an assortment of "I's" – one for every relationship the Ubuntu individual is included in.[62]

According to Van Binsbergen:

"Ubuntu recognises the following four attributes of human beings: · Human dignity and equality

- *Universal brotherhood*
- *Sacredness of life*
- *"Being" is the most desirable state of life (i.e. community-based living)*

---

[60] H. N. Olinger, J. J. Britz, and M. S. Olivier. "Western Privacy and Ubuntu — Influences in the Forthcoming Data Privacy Bill". In: Ethics of New Information Technology — Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005). Ed. by P. Brey, F. Grodzinsky, and L. Introna. Enschede, The Netherlands, July 2005, pp. 291–306

[61] Mokgoro, JY. 1997. *Ubuntu and the Law in South Africa*. Seminar Report of the Colloquium. Konrad-Adenauer Stiftung. Johannesburg.

[62] Louw, DJ. 1999. Ubuntu: An African assessment of the Religious Other. *The Paideia Project. Proceedings from the Twentieth World Congress of Philosophy. 10-15 August 1998*

Human beings are recognised as being all equal, sharing a common basic brotherhood, having the right to life and finding their ultimate meaning and purpose within communities."[63] The last attribute is in stark contrast to the extreme individualism of Western cultures."

While dissecting the ideas and values of Ubuntu one can gather specifically the suggestions for privacy and the attitude individual security. The statements made before about the welfare of the community being more critical than that of the individual, clearly demonstrate that there is a tension between privacy and social good. The case here is that individual privacy may be viewed as not being beneficial to the community. An individual right may be acknowledged only if it serves the community and in Ubuntu it is hard make a case for the social advantage of personal privacy. The culture of openness and transparency in Ubuntu would not comprehend the requirement for personal privacy or be able to justify it. In this manner personal privacy would rather be translated as "secrecy". This "secrecy" would not be seen as positive since it implies that the Ubuntu individual is attempting to conceal something as opposed to protecting the community.[64]

According to Scorgie, some privacy is appreciated in Ubuntu communities despite the fact that privacy is seen as secondary to relationships and relationship-building.[65] Individuals are understood to have their own distinct ideas, thoughts, qualities and achievements. These are considered the private belonging of a person. This thought does not run counter toward the Western idea of privacy as dignity and as a part of a person's personhood.

One last point to be made for privacy in the context of the Ubuntu society is that of consent. The understanding that an individual can't order their life without consent from family, tribe and the community.[66] This understanding is in contradiction to the notion of independence to make one's own choices. To that end privacy is required to guarantee individual

---

[63] Van Binsbergen, W. 2002. Ubuntu and the globalisation of Southern African Thought and Society. *Philosophical Faculty, Erasmus University, Rotterdam, The Netherlands.*

[64] H. N. Olinger, J. J. Britz, and M. S. Olivier. "Western Privacy and Ubuntu — Influences in the Forthcoming Data Privacy Bill". In: Ethics of New Information Technology — Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005). Ed. by P. Brey, F. Grodzinsky, and L. Introna. Enschede, The Netherlands, July 2005, pp. 291–306

[65] Scorgie, F. 2004. *Ubuntu in Practice.* HIVAN Research Associate. (Comments received by email.) Email to: HN Olinger (Hanno.Olinger@Kumbaresources.com) [6 November 2004]

[66] Kwamwangamalu, NM. & Nkonko, M, Ubuntu in South Africa: a Sociolinguistic Perspective to a Pan-African Concept, *Critical Arts Journal, Vol.13, No. 2, 1999, 24-42.*

independence and henceforth give the capacity to settle on those free good choices. To conclude, it is clear that in the context of the Ubuntu culture, privacy has been consigned to a position of lower significance than in the Western societies more focused on Libertarianism as opposed to the more African communitarianism.

Chapter 3: Web 2.0, Social media and Governments

Web 2.0 and Data

As more and more and more people around the world embrace the technological super network that is the internet, it is important to highlight a number of key historical and technical developments that enable it to be the colossal repository of user data it is today.

The internet is a computer network consisting of various similar networks.[67] Internet communication takes place when the source computer splits digitised data into smaller pieces known as packets and submits these packets through a router and into the network. Each subsequent network the packet passes through transfers the packet through its router to the next using basic information stored in the packets such as the Internet Protocol (IP) addresses of the source and destination computers.[68]

The World Wide Web (WWW) on the other hand, is an information sharing-model built upon the internet that makes use of the HTTP[69] language to transmit data, services and allows applications to communicate over the networks. Web browsers such Google's Chrome, Mozilla's Firefox and Microsoft's Internet Explorer/ Edge are used to access Web documents referred to as web pages which are connected by hyperlinks.

It is important to keep in mind that the web is just a section of the internet through which information can be disseminated and shared. The internet is used for other services such as the e-mail functionality that uses the SMTP[70] structure as opposed to HTTP.

The Web before 1999 (Web 1.0) is often named the "Read-Only" web. This term find its origin in the fact that average internet users were limited to only being able to read the information already presented by the creators of the webpage. This effectively made the information flow unidirectional (from producer to consumer) and did not allow users not technically skilled in the technology any functionality except observation.

Web 2.0 is a broad term enveloping the new stage of web enabled programs built around user-generated and user-manipulated data such as blogs, wikis, podcasts and social media sites.[71]

---

[67] Dimitri Bertsekas & Robert Gallagher, *Data Networks* (2d Ed. 1992), Prentice Hall, 1991, 80.
[68] Dimitri Bertsekas & Robert Gallagher, *Data Networks*, 81, 327, 332-35.
[69] Hypertext Transfer Protocol
[70] Simple Mail Transfer Protocol

The advent of web 2.0 technology enables all internet users to become Internet Content Producers (ICPs), effectively enabling them to create, collaborate and curate content on the internet including personal information shared with varying degrees of people.[72]

The defining difference between Web 1.0 and Web 2.0 technologies is that Web 1.0 was greatly limited in terms of content creators with the knowledge necessary to create web pages, with a great proportion of web users simply having access to the already published webpages. Web 2.0 on the other hand allowed any person with access to a computer the ability to themselves become a content creator without any but the most basic training. This was achieved by the implementation of various technological aids specifically purposed around the maximisation of content creation.[73]

Social media is another general term that encompasses many functionalities allowing participants to meet and maintain communication with people online, form communities with persons with similar interest and share content.[74] The functionalities included under this umbrella include:

1. Social Networks- By far the most commonly used variation of this technology. Examples Include Facebook, Twitter, Google plus and Linkedin.
2. Content Sharing- This enables members to share an assortment of media. These tools create, share and curate
3. Discussion –Video conferencing / chatting, text messaging. Examples Include: Skype, WhatsApp, and Googe talk.
4. MicroBlogging – mini publishing that enables quick and frequent sharing and that has helped to provide officials and the public with on the ground situational awareness during natural emergencies such as the earthquake and tsunami in Japan as well in

---

[71] Web 2.0, *The Pew Internet and American Life Project Retrieved from http://www.pewinternet.org/topics/Web-20.aspx. On 21 January 2016.*

[72] Gaffin, Elizabeth, Friending Brandeis: Privacy and Government Surveillance in the Era of Social Media (April 30, 2012). Available at SSRN: http://ssrn.com/abstract=2049013

[73] Graham Cormode and Balachander Krishnamurthy Key differences between Web 1.0 and Web 2.0 *First Monday*, Volume 13 Number 6 - 2 June 2008

[74] *Pew Internet and American Life Project*, Retrieved from http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx, *On 21 January 2016.*

more social crises such as the Arab Spring uprisings in Egypt and Iran. Examples include Twitter, which is limited to 140 characters and Tumblr.

5. Location based networks – Used for reviewing businesses as well to report and track an individual's attendance at a site. Examples include Four Square and Yelp.
6. Social Games –Stand-alone or applications on other social network platforms. Examples include Sims Social and Farmville.
7. Virtual Worlds – online environments where one can create personalities or avatars and interact with other personalities or avatars. Examples include Second Life, There and Imvu.
8. Massive Multiplayer Online Games – combination of social games and virtual worlds. Usually there is a common goal or community where participants can interact with one another. Examples include League of Legends, Clash of Clans and Dota.[75]

These profiles may contain personal information as well as the lists of "friends" or others that they maintain contact with online. Many services enable users to exercise some measure of control over with whom they chose to share their profiles by invoking available privacy settings. Regardless of the privacy settings a user selects, service providers, pursuant to their "terms of use" agreements, often retain the ability to access and collect user's data so that they can deliver targeted advertising to the user thus raising revenues to sustain its operations. Typically these agreements are lengthy, complicated, and difficult to understand, casting doubt on whether users are providing meaningful consent.[76] Prof. Lorrie Cranor noted, online privacy policies are difficult to understand. Most privacy policies require a college reading level and an ability to decode legalistic, confusing, or jargon-laden phrases."[77] Buried within the terms of use agreements is language where providers include their policies for responding to requests from law enforcement.[78] Privacy disclosure policies vary from site to site. The

[75] O'Neill Communication, (n.d.). "All the different types of social media," Retrieved from www.oneillcommunications.com. *On 21 January 2016*

[76] McDonald, A., & Cranor, L. F, The Cost of Reading Privacy Policies, *ACM Transactions on Computer-Human Interaction*, (2008), 389(3), 1

[77] Cranor, L. F., Kelley, P.G., McDonald, A., & Reeder, R. W, A Comparative Study Of Online Privacy Policies and Formats, Springer Berlin Heidelberg, (2009).

[78] *See* Facebook (2012). Information for law enforcement authorities. Retrieved from

control and collection of data pertaining to an individual is an aspect of the expectation of privacy in cyberspace which is the subject of a huge debate currently occurring in classrooms, academia, corporate boardrooms, and homes across the world.[79]

Finally, in the very near future, Internet technologies will evolve to a new level with the advent of Web 3.0 technologies and "the semantic web,"[80] a term coined by one of the original pioneers of the Internet, Sir Ted Berners-Lee. The extent of the new functionalities that will become available with Web 3.0, or the semantic web, is still unknown. However, they will most likely enable machines to read web pages and better tailor the computing experience to the user. While some theorize that if constructed properly, privacy considerations can be can embed into emerging Web 3.0 technologies (privacy by design), others fear that the consolidation of so much data will make surveillance much easier.

A final definition to note is that of the cloud and cloud computing. This can be defined as a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres.[81] Over the last few years, consumers, corporations and governments have rushed to

---

https://www.facebook.com/safety/groups/law/guidelines/ *See also* Google (2012). Privacy Policy. Retrieved from
https://www.google.com/intl/en/policies/privacy/ which provides notice of their policy with respect to disclosure to the government:

> For legal reasons
> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information I reasonably necessary to:
> - meet any applicable law, regulation, legal process or enforceable governmental request.
> - enforce applicable Terms of Service, including investigation of potential violations.
> - detect, prevent, or otherwise address fraud, security or technical issues.
> - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

[79] Gaffin, Elizabeth, Friending Brandeis: Privacy and Government Surveillance in the Era of Social Media, 31.
[80] The Semantic Web, a collaborative effort of W3C and industry partners, "provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries."
See W3C. (2011). W3C Semantic Web Activity. Retrieved from http://www.w3.org/2001/sw/
[81] Hassan, Qusay, "Demystifying Cloud Computing" , *The Journal of Defense Software Engineering* (CrossTalk) 2011 (Jan/Feb): 16–21.

move their data to "the cloud,"[82] adopting web-based applications and storage solutions provided by companies that include Amazon, Google, Microsoft and Yahoo. This trend is only going to continue, with industry analysts predicting that cloud computing related revenues will grow to somewhere between $40 and $160 billion over the next few years.[83] Cloud computing services provide consumers with vast amounts of cheap, redundant storage and allow them to instantly access their data from a web-connected computer anywhere in the world. Unfortunately the shift to cloud computing needlessly exposes users to privacy invasion and fraud by hackers. Cloud-based services also leave end users vulnerable to significant invasions of privacy by the government, resulting in the evisceration of traditional Fourth Amendment protections of a person's private files and documents. These very real risks associated with the cloud computing model are not communicated to consumers, who are thus unable to make an informed decision when evaluating cloud based services.[84]

Government Investigations and Social Media

While it is little known to most consumers, government requests to Web 2.0 companies have become a routine part of business.[85] Practically all cloud computing providers have dedicated legal compliance departments,[86] some open 24 hours per day, through which law enforcement agents can obtain emails, logs of search requests, and other stored customer data through a formalized process.[87] While Google has widely publicized its initial refusal to deliver search records in response to a request by the U.S. Department of Justice in 2006, it has been far less willing to discuss the huge number of subpoenas it receives per year, to which it does comply and delivers its customers' data to law enforcement agencies.[88] Furthermore, the company's

---

[82] Peter Mell & Tim Grance, National Institute of Standards and Technology., Perspectives on Cloud Computing And Standards 3 (2008), http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008 12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf.

[83] Geoffrey A. Fowler & Ben Worthen, *The Internet Industry Is on a Cloud—Whatever That May Mean*, WALL ST. J., Mar. 26, 2009, http://online.wsj.com/article/SB123802623665542725.html

[84] Soghoian, Christopher, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era, on *Telecomm. and High Technology Law*. (August 17, 2009). 359; Berkman Center Research Publication No. 2009-07.

[85] Saul Hansel, *Online Trail Can Lead to Court*, New York Times, Feb. 4, 2006, at C6

[86] For a list of the legal compliance departments at hundreds of phone/Internet companies, see: Search.org, ISP List, http://www.search.org/programs/hightech/isp/

[87] Saul Hansel, *Online Trail Can Lead to Court*, p 100

[88] Posting of Ryan Singel to Threat Level Blog, Google To Anonymize Data—Updated, http://www.wired.com/threatlevel/2007/03/google_to_anony, On January 23 2016

CEO has publicly stated that one of the main reasons the company retains detailed data on consumers' online activity is to assist the government with lawful investigations.[89]

Is this Constitutional?

In The American context, the Fourth Amendment guarantees a measure of control around their bodies and possessions that the government cannot enter or search without reasonable cause. Thus, a person's diary, personal letters, and other such property are normally provided with constitutional protection. Americans have become used to these rights, and often take for granted that private matters are usually kept private. Unfortunately, as society has shifted to communicating and working online, these constitutional protections have been left behind. Fourth Amendment protections against unreasonable search and seizure depend upon a person's reasonable expectation of privacy. Unfortunately for users of Internet based services, existing case law does little to protect their digital documents and papers which are now increasingly being stored on the remote servers of third parties. The cause of this departure from the Fourth Amendment is the third-party doctrine, which establishes that people have no expectation of privacy in the documents they share with others.[90] Rather than revisit *Smith v. Maryland* and *United States v. Miller* at length, a single quote from the Supreme Court should be enough:

> "*The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorizes, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.*[91]

The situation is much the same in the Kenyan context, with article 31(d) explicitly providing for the protection of an individual's communications. The right to privacy under article 31 is however not absolute and can be limited to the extent that it is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, as is expressed in article 24 (1) of the CoK on the limitation of rights and fundamental freedoms.

---

[89] Interview by Robert Siegel with Eric Schmidt, CEO, Google (Oct. 2, 2009), *available at* http://www.npr.org/templates/story/story.php?storyId=113450803

[90] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735(1979).

[91] United States v. Miller, 425 U.S. 435 , p 443

The Kenyan courts in the 2015 criminal case of *Alan Wadi v The Republic*,[92] demonstrated reasoning in line with the third party doctrine. At first instance, Mr Wadi a 4th year University student was successful charged with the offence of hate speech contrary to Section 13(1) (a) (b) and (2) of the National Cohesion and Integration Act and undermining authority of a public officer contrary to Section 132 of the Penal Code, based on two messages he posted on his Facebook wall on the 18th and 19th of January respectively. By posting the results on his wall he made the information public and therefore no action of breach of privacy was raised.

Social Media Terms of Service Agreements

In this section, I shall highlight specific sections from the Terms of Service agreements, Privacy Policies and Transparency reports of two social media companies, Facebook and Twitter. With the aim of outlining their specific policies on dealing with government warrants and subpoenas as well as indicating how they have dealt with these situations in the past.

Twitter

Industry-Accepted Best Practices. Twitter requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

> *"Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter."*[93]

In addition to a law enforcement guide, Twitter publishes a transparency report.

Inform users about government data demands. Twitter promises to provide advance notice to users about government data demands, but does not promise to provide notice after an emergency has ended or a gag has been lifted. Instead, Twitter says that it may provide post-notice:

> *"Yes. Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account*

[92] *Alan Wadi v The Republic*. 2015 eKLR Criminal Appeal No.1 Of 2015
[93] https://support.twitter.com/articles/41949#7, On 15th March 2016.

compromises). We may also provide post-notice to affected users when prior notice is prohibited."[94]

Disclose data retention policies. Twitter publishes information about its data retention policies, including retention of IP addresses and deleted content:

> *"Log Data: When you use our Services, we may receive information ("Log Data") such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device information (including device and application IDs), search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. We may also receive Log Data when you click on, view or interact with links on our Services, including links to third-party applications, such as when you choose to install another application through Twitter. Twitter uses Log Data to provide, understand, and improve our Services, to make inferences, like what topics you may be interested in, and to customize the content we show you, including ads. If not already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after a maximum of 18 months."*[95]

Twitter has had numerous opportunities to exercise these provisions, with perhaps the most influential being the case of *People v Harris* mentioned in the first chapter. In the case New York appellate court heard arguments regarding Twitter's appeal of two court orders in the prosecution of an Occupy Wall Street[96] protestor. The trial court held that the defendant

---

[94] https://support.twitter.com/articles/41949#7 On 15th March 2016

[95] https://twitter.com/privacy?lang=en On 15th March 2016

[96] About Us | OccupyWallSt.org. (2016). [online] Occupywallst.org. Available at: http://occupywallst.org/about/ [Accessed 14 Apr. 2016].
"Occupy Wall Street is a people-powered movement that began on September 17, 2011 in Liberty Square in Manhattan's Financial District, and has spread to over 100 cities in the United States and actions in over 1,500 cities globally. #ows is fighting back against the corrosive power of major banks and multinational corporations over the democratic process, and the role of Wall Street in creating an economic collapse that has caused the greatest recession in generations. The movement is inspired by popular uprisings in Egypt and Tunisia, and aims

lacked standing to move to quash the government's third-party subpoena to Twitter for his account records and that his Tweets were not protected by the Fourth Amendment. The trial court similarly denied Twitter's motion to quash the government's subpoenas for the defendant's Twitter records for the same reasons, among others. Notably, the defendant was only able to move to quash the subpoena because as noted above, "Twitter's policy is to notify users of requests for their information prior to disclosure."

Twitter also protects its business by litigating against such third-party government subpoenas. Twitter argued on appeal that the defendant has standing to quash the government's subpoena because he has a proprietary interest in his Tweets, pointing to the express language of Twitter's Terms of Service. Moreover, Twitter argued that the defendant's Tweets are protected by the Fourth Amendment, primarily because the government concedes that the Tweets it sought were not made public by the defendant (they were in the defendant's drafts) And, if a defendant has a reasonable expectation of privacy under the Fourth Amendment in his or her non-public emails[97], Twitter argued that not affording that same protection to users' non-public Tweets would "create arbitrary line drawing." Finally, even assuming the Tweets in question were public, Twitter argued that the government still requires a search warrant under the Federal and New York constitutions. Notwithstanding Twitter's pending appeal, Twitter complied with a court order requiring it to promptly submit the Defendant's Tweets under seal.

Facebook

Facebook requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

> *"A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any*

---

to fight back against the richest 1% of people that are writing the rules of an unfair global economy that is foreclosing on our future."

[97] As was held in United States v. Jones, 132 S. Ct. 945, 949 (2012)

account, which may include messages, photos, videos, wall posts, and location information."[98]

Facebook promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

"Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct."[99]

Facebook publishes information about its data retention policies, including retention of IP addresses and deleted content:

"We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services."[100]

The Kenyan Government and Social Media

Locally, despite the penetration of social media use in Kenya to the tune of 4.5 million users a month as reported in September 2015 by the Facebook's Africa office[101] 95% of which originated from mobile phones and the increasing availability and accessibility of mobile

[98] https://www.facebook.com/safety/groups/law/guidelines/ On 15th March 2016
[99] https://www.facebook.com/safety/groups/law/guidelines/ On 15th March 2016
[100] https://www.facebook.com/safety/groups/law/guidelines/ On 15th March 2016
[101] http://www.reuters.com/article/us-facebook-africa-idUSKCN0RA17L20150910

handsets which retail for as low as 999 Kenya Shillings (United Stated Dollar 9.78)[102] and come pre-installed with the Facebook application (implying an exponential social media usage growth possibility). There exist no Kenyan cases in which social media evidence has been requested by the government via subpoena or been submitted for consideration before a court and challenged. There are two main reasons for this, first, the cases that have made it to trial, such as R v Alan Wadi mentioned above, have all relied on evidence readily available to the public due to them being published either on facebook walls / timelines or as public tweets. Second, as is discussed in greater detail in chapter 4, the Kenyan government has systems in place capable of monitoring and intercepting local communications networks without following the legal step of seeking a warrant and issuing the relevant companies with a subpoena.

The cases that have made it to court however tend to fall under two categories with heavy political involvement, these are hate speech and criticism of the government and government officials. To start with the former, in the 2015 case of Republic v Moses Kuria[103], the accused was charged with two counts of incitement to violence and disobedience of the law contrary to Section 96(a) of the Penal Code. These charges stemmed from messages posted on his public Facebook timeline allegedly with the intent of stirring up ethnic hatred between the Kikuyu, Luo and Somali communities. The case encountered several issues amongst them applications made by The Director of Public Prosecutions (DPP) and the Law Society of Kenya (LSK) seeking the denial Mr Kuria's bail and citing the breach of an earlier conciliation pact with the National Cohesion and Integration Commission.[104]

At no point however was the social media evidence, or the means of its acquisition brought into question despite the court rejecting another piece of evidence generated and annexed by the prosecution consisting of a forensic transcript of a translation from Kikuyu to English

[102] Currency conversion accurate as of the 8th of January 2016.
[103] Republic v Moses Kuria [2016] eKLR
[104] Moses Kuria's hate speech case put off. (2016). Daily Nation. Retrieved 29 March 2016, from http://www.nation.co.ke/news/Court-puts-off-Moses-Kuria-hate-speech-case-/-/1056/2810604/-/3ief7q/-/index.html

language, of a video in which Mr Kuria addressed a crowd, for the courts perusal on the grounds that it lacked a certificate to authenticate its credibility.[105]

The case was eventually quashed by the Prosecutor stating: "*The prosecution has asked the court to free Kuria on condition he will not utter further inflammatory statements.*" The Court cannot proceed with the case when the prosecutor decides to withdraw it from the cause list. This behaviour frustrates all attempts to proceed with hate speech through judicial process due to political influence. The success of hate speech in the criminal justice does not only need evidence and burden of proof but most importantly the political good will.[106] The unseen political influence in this particular case in favour of the accused, appears to be a recurring theme in this genre of cases. In the following cases the influence took the side of the prosecution.

Abraham Mutai, a blogger known for his investigations on corruption, was arrested for posting a blog about corruption and charged with "using a media platform to cause public anxiety" in January 2015. He was released a day later after significant social media attention called for his release.[107]

Nancy Mbidala, an intern at the Embu county government office, was arrested in January 2015 for a series of posts she wrote on her Facebook wall from 2013-2014 that allegedly abused a local governor. She was later released and pardoned of all charges after apologizing to the governor.[108]

Geoffrey Andare, a web developer, was a charged in March 2015 with misuse of a telecommunications system, for his Facebook post that accused an employee of a non-profit educational organization of trading scholarships for sexual favours. Mr Andare used the charge as an opportunity, in partnership with Article 19, to file a petition challenging the constitutionality of section 29 of the Kenya Information and Communications Act (KICA),

---

[105] "DPP Loses Bid To Cancel Moses Kuria's Bond". 2016.Businessdailyafrica.com. Accessed March 20 2016. http://www.businessdailyafrica.com/Court-rejects-bid-to-cancel-Moses-Kuria-s-bond/-/539546/2879440/-/mfkvnxz/-/index.html.

[106] Onyoyo P.O, Criminality in "Hate Speech" Provision in the Laws of Kenya- Jurisprudential Challenges.

[107] Njeri Wangari, "Blogger Abraham Mutai Arrested and Released for reporting on Corruption in Isiolo County," *Kenya Monitor, January 17, 2015.*

[108] Njeri Wangari, "24 Year old Nancy Mbindalah Held in Custody then Pardoned for Undermining the Embu Governor,' *Kenya Monitor,* January 22, 2015, http://bit.ly/1M0vF9a.

which he argued violates Kenyan citizens' constitutional right to freedom of expression. The petition had not been heard as of mid-2015.[109]

[109] Shitem Khamadi, "Web developer challenges constitutionality of infamous charge 'misuse of licensed telecommunication equipment'," *Kenya Monitor,* May 6, 2015, http://bit.ly/1GP5jFR.

Chapter 4: An analysis of the current state of the Kenyan law relevant to Social media Evidence acquired by Government Institutions and its constitutionality.

Obligations under International Law

As of the promulgation of the Constitution of Kenya (CoK 2010), the Sovereign Democratic Republic of Kenya is a monist state. This effectively means that general rules of International law and any treaties and conventions signed and ratified by Kenya, shall consist a part the nation's laws without going through the process of incorporation and transformation. This is provided for under article 2 of the CoK 2010, specifically sub-articles 5 and 6 which state:

> *"(5) The general rules of international law shall form part of the law of Kenya.*
> *(6) Any treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution."*[110]

The question that naturally arises next is what position in the hierarchy of laws international law is to take. Judicial institutions are so far yet to come up with a consistent philosophy on the hierarchy and the legislature has yet to amend the Judicature Act with the intention of specifying the exact position of International law. This said, the supremacy of the constitution has been respected in the post 2010 superior courts' jurisprudence and the mischief is between international law and the various municipal legislations in case of conflict between these sources of law.[111]

Kenya is a signatory to a number of international conventions and treaties necessitating the protection of individual privacy rights from unnecessary exploitation by various figures except when prescribed by law and/or necessary to achieve a legitimate aim and proportionate to the aim pursued.[112] These include the Universal Declaration of Human Rights (UDHR)[113], the

---

[110] Article 2: (5) and (6), *Constitution of Kenya* (2010).
[111] Kabau T and Ambani JO, 'The 2010 Constitution and the Application of International Law in Kenya: A Case of Migration to Monism or Regression to Dualism?', 36-55, 1 Africa Nazarene University Law Journal 1, (2013).
[112] Article 29, *Universal Declaration of Human Rights*; (10 December 1948) General Comment No. 27
[113] Article 12, *Universal Declaration of Human Rights.*

International Covenant on Civil and Political Rights ('ICCPR')[114] , which is of particular relevance due to the Human Rights Committee imparting on state parties of the ICCPR a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right (privacy)."[115] The United Nations Convention on Migrant Workers[116], UN Convention of the Protection of the Child[117], the African Charter on the Rights and Welfare of the Child[118] and the African Union Principles on Freedom of Expression.[119]

The UDHR, specifically provides for the privacy protection at article 12, which states:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."* [120]

This lays the foundation for human rights protection from unwarranted privacy violations relevant to our topic such as search and seizure as well as protecting the correspondence of individuals.

Article 12 can also be cited as a clear and heavy influence on article 31 of the CoK 2010 with numerous overlapping attributes, such as explicit mention of the right to privacy's protection of the home, family, and correspondence/communications.

The ICCPR aside from creating the obligation to legislate privacy protection mentiond earlier in this chapter, also specifically provides for the right in two separate articles, these are article 14 (1) which states:

> *"All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and*

---

[114] Article 17 ,*International Covenant on Civil and Political Rights*, which reinforces Article 12 of the *Universal Declaration of Human Rights.*

[115] General Comment No. 16 (1988), para. 1

[116] Article 14 , *United Nations Convention on Migrant Workers.*

[117] Article 16, *United Nations Convention of the Protection of the Child.*

[118] Article 10, *African Charter on the Rights and Welfare of the Child.*

[119] Article 4, *African Charter on the Rights and Welfare of the Child.*

[120] Article 12, *Universal Declaration of Human Rights.*

impartial tribunal established by law. The press and the public may be excluded from all or part of a trial for reasons of morals, public order (order public) or national security in a democratic society, or when the interest of the private lives of the parties so requires, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children"[121]

As well as article 17, which states:

"1. 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.
2. Everyone has the right to the protection of the law against such interference or attacks."[122]

Article 14 while setting out the principle for free and fair trial also protected in The CoK 2010 at article 50 (1) and (2) and rendered immune to limitation by any other at article 25 (c), provides for the protection of an individual's privacy rights even during trial, in situations wherein the glare of the public would potentially limit the interests of justice.
Article 17 of the ICCPR similar to article 12 of the UDHR and article 31 of the CoK 2010, protects the family, home and communications from interference.

A particular similarity that is of vital importance to this discussion, all of the privacy protections found in the international obligations above only prevent the unlawful violation of privacy. It is universally accepted in both international law instruments and municipal legislation that the right to privacy is not a fundamental right that may not be limited and

[121] Article 14 (1), *International Covenant on Civil and Political Rights.*
[122] Article 17, *International Covenant on Civil and Political Rights.*

situations may arise in which a legally approved party may rightly breach the privacy of the family, home and correspondence of an individual.

Domestic Laws

The right to privacy is explicitly provided for under article 31 of the CoK 2010. Which states:

> *"Every person has the right to privacy, which includes the right not to have—*
> *(a) their person, home or property searched;*
> *(b) their possessions seized;*
> *(c) information relating to their family or private affairs unnecessarily required or revealed; or*
> *(d) the privacy of their communications infringed."*[123]

Privacy is also recognised and protected under various pieces of state legislation, including: The Kenya Information and Communications Act 2009, which at article 31 provides that:

> *"A licensed telecommunication operator who otherwise than in the course of his business—*
> *(a) intercepts a message sent through a licensed telecommunication system; or*
> *(b) discloses to any person the contents of a message intercepted under paragraph ; or,*
> *(c) discloses to any person the contents of any statement or account specifying the telecommunication services provided by means of that statement or account, commits an offence and shall be liable on conviction to a fine not exceeding three hundred thousand shillings or, to imprisonment for a term not exceeding three years, or to both."*

Article 83 W

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

---

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

(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.

Article 93 (1)

No information with respect to any particular business which—

(a) has been obtained under or by virtue of the provisions of this Act; and

(b) relates to the private affairs of any individual or to any particular business, shall, during the lifetime of that individual or so long as that business continues to be carried on be disclosed by the Commission or by any other person without the consent of that individual or the person for the time being carrying on that business.

Section 15 (1) of the Kenya Information and Communications (Consumer Protection) Regulations, 2010, states that:

"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."

Admissibility of Electronic Evidence

The Evidence Act[124] provides for the admissibility of digital and electronic evidence in any legal proceedings at section 78A. Subsection 3 of the same section goes on to provide for factors that may affect the weighting of such evidence, these are:

"(a) the reliability of the manner in which the electronic and digital evidence was generated, stored or communicated;

[124] Section 78A, *Evidence Act*, (Cap 80) 2012 (Revised 2014).

(b) the reliability of the manner in which the integrity of the electronic and digital evidence was maintained;

(c) the manner in which the originator of the electronic and digital evidence was identified and

(d) any other relevant factor."[125]

It is clear that the authors of this subsection drafted it with the intention of ascertaining the authenticity of the evidence. It is a simple logic step however to encompass social media evidence as electronic evidence considering the information used is both created and viewed on electronic platforms such as mobile phones and computers.

Government Access to Data

A reading of the relevant Kenyan laws up to this point paints a favourable picture if the protection of the right and the adherence to the international obligations ratified by the state. The Kenyan government has however left itself various avenues of exploitation allowing them to clawback the entirety of the legislation stated above, leaving only the constitutional provision uninterrupted, and that only due to the fact the Constitution is the supreme law of the land.[126]

The first of these and most relevant to the specific topic of social media, is found under the Kenya Information and Communication Act. This relevance stems from the fact that 80% of Kenyans now have access mobile phones, further, 99% of the new internet connections in the last year came from mobile phones, pushing the total Kenyan internet user numbers to a staggering 23 million people.[127] The majority of internet service providers according to population are therefore the mobile service providers, which are governed by the Information and Communication Act.

---

[125] Section 78A (3), *Evidence Act*.

[126] Though a case can be made that Article 31 of the *Constitution of Kenya* is not an inalienable right as it is not provided for under article 25, therefore it may constitutionally be limited by law. This is the case in matters of security and begins to explain the reason dome of the claw backs exist.

[127] http://www.irishtimes.com/news/world/africa/mobile-phones-ring-changes-in-kenya-with-internet-access-1.2242054 on 11th January 2016.

According to section 31 of the Kenya Information and Communication Act, licensed telecommunication operators are legally prohibited from implementing technical requirements necessary to enable lawful interception, further, section 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010, states that a licensee (licensed under the KIC Act) "*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*".

However, the recently adopted Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2014[128] permits access to private or confidential information on consumers without a court order. Section 13 reads:

> *"A licensee[129] shall grant the Commission's officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations."*

The obligation the regulations place on telecommunications service providers to provide access to their systems and data without a court order violates the right to privacy. A possible loophole however exists in the form of the provisions for unwarranted search found in our law, specifically Section 60 of the National Police Service Act[130] and section 26 of the Criminal procedure Code[131]. The courts however have yet to determine whether the laws for unwarranted search apply in the same manner and form in cases of data seizure and interception as they would for physical search of a person and their premises.

Currently dominating Kenya's mobile subscription market is Safaricom limited with 67% of the market share.[132] The majority shareholders in Safaricom are Vodafone with a 40% share percentage. According to Vodafone's transparency report, Law Enforcement Disclosure

---

[128] Legal Notice No. 10 to the *Kenyan Communications and Information Act*, 7 February 2014.
[129] Means a person or entity licensed under the Act to own and operate a telecommunication system or to provide telecommunication services or both.
[130] *National Police Service Act* (Cap 84 of the laws of Kenya)
[131] *Criminal Procedure Code* 2010(Cap 75 of the laws of Kenya) (Revised 2012)
[132] Quarterly Sector Statistics Report Third Quarter Of The Financial Year 2014/15 (Jan-Mar 2015), p 9

Report[133], published In June 2014, Vodafone have "*not received any agency or authority demands for lawful interception assistance*"[134] in Kenya. Hopeful as this may sound it is not due to the fact that the government is not interested, on the contrary, the inference from this disclosure is that the Kenyan authorities have direct access to Vodafone's network, which allows the government to monitor communications directly without having to go to the company to seek the data of their customers.[135] This type of unfettered access permits uncontrolled mass surveillance of Vodafone's customers and anyone in contact with those customers, which amounts to a direct and unconstitutional interference with the right to privacy.

This level of access is particularly worrying as it effectively translates to government agencies having uninhibited, warrantless, access to the every bit of data a person send or receives via the internet or any telecommunication network while in Kenya. Unfortunately, this only the beginning of the clawbacks.

The Kenya National Intelligence Agency was established by the 2012 National Intelligence Service Act[136], and is both the domestic and foreign intelligence agency of Kenya. Article 36 reads:

> "*(1) The right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with.*
>
> *(2) The Service shall, prior to taking any action under this section, obtain a warrant under Part V."*

Article 45 states:

---

[133] Vodafone, Law Enforcement Disclosure Report – Country-by-country section, in Sustainability Report 2013/14. , pp. 61-80

[134] Vodafone, Law Enforcement Disclosure Report – Country-by-country section, in Sustainability Report 2013/14. , pp. 77

[135] [135] Vodafone, Law Enforcement Disclosure Report – Country-by-country section, in Sustainability Report pp. 69, 2013/14.

[136] *National Intelligence Service Act* , No. 28 Of 2012.

"....an officer of the Service the power to obtain any information, material, record, document or thing and for that purpose –

(a) to enter any place, or obtain access to anything;

(b) to search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing;

(c) to monitor communication; or

(d) install, maintain or remove anything."

The National Intelligence bodies despite being granted these powers, are not regulated by any further pieces of legislation under Kenyan laws, this effectively grants them carte blanche to breach privacy rights protections. For instance, section 35 of the Prevention of Terrorism Act 2012[137] grants extensive powers to state authorities to limit fundamental freedoms and encroach on the right to privacy through surveillance. [138] In view of the 2013 terrorist attack on the Westgate shopping mall and the 2015 Garissa University College attack with a combined fatality count of about 300 people, the Act has been presented as a positive tool to tackle threats to national security.

Communications Monitoring

The Information and Communications (Amended) Act 2013 and related Regulations as well as the Prevention of Terrorism Act 2012 illustrate the overarching powers government authorities have to monitor individuals' communications and access their personal data.

In March 2012, the telecommunications industry regulator, the Communications Commission of Kenya (CCK) today known as the Communications Authority of Kenya (CAK), announced[139] it was setting up a system to allow the authorities to monitor incoming and outgoing digital communications. CCK requested that all telecommunication service providers

---

[137] *Prevention of Terrorism Act*, No. 30 of 2012.

[138] Section 35 (3),*Prevention of Terrorism Act*.
Section 36 is also of interest as it concerns the power to intercept communication and the admissibility of intercepted communication without making any mention of a warrant. Being suspected of the crime of terrorism seems to effectively dissolve the right granted under the constitution.

[139] Communications Commission of Kenya, Kenya and ITU sign administrative agreement for KE-CIRT/CC, 17 February 2012.

cooperate in the installation of internet traffic monitoring equipment; known as Network and Early Warning Systems (NEWS). The CCK cited a rise in cyber security threats as a justification for this move. NEWS is an initiative of the UN's International Telecommunication Union (ITU)[140] and is presented as a tool to identify threats and provide advice on how to respond.

In January 2013, the Blue Coat PacketShaper appliance, a device capable of monitoring, surveillance, as well as filtering application traffic by content category, was found to be operating in 18 countries worldwide including Kenya.[141]

In June 2015 the anonymous, whistle blower website, WikiLeaks released e-mail correspondence between NIS agents and representatives of an Italian based company known as Hacking Team for the purchase of a stealth interception known as Remote Control. This software is designed to attack, infect and monitor targeted personal computers and smartphones as well as allow access to all the information located therein including (and specifically mentioned in the correspondence) "skype calls, Facebook, Twitter, WhatsApp. Line, Viber and many more" accounts.[142] To test the product, the NIS agents on May 6th requested Hacking Team to bring down Kahawa Tungu, a website affiliated with the controversial blogger Robert Alai.[143] This particular request was however denied by means of emails sent by their Operating Manager, Ms Daniele Milan, to the company's key account manager in charge of Kenya, Mr Emad Shahata, noting that the request originated from a private individual claiming to represent a cyber-security outfit. In the email Ms Milan stated "*The person who wrote to us is from a private communication company that sells pay TV service, and the URL, they asked us to tear down is a news website that is highlighting corruption and other wrongdoings in the Kenyan Government. I don't think we want to be*

---

[140] ITU News, Making an IMPACT on global cybersecurity, October 2009, Available at https://www.itu.int/net/itunews/issues/2009/08/22.aspx on 2nd February 2016.
[141] Morgan Marquis-Boire et al., *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Citizen Lab, January 15, 2013, http://bit.ly/1hNzLcN, 22nd March 2016.
[142] Vincent Achuka and Walter Menya, "Wikileaks: NIS purchased software to crack websites,"*Daily Nation,* July 11, 2015, http://bit.ly/1LyRP2U, 22nd March 2016.
[143] Italians reject bid to close Kahawa Tungu," *Daily Nation,* July 12, 2015, http://bit.ly/1PtYTnw, 22nd March 2016.

involved in this." WikiLeaks published more than a million emails linking Hacking Team with many paying countries including Sudan, UAE, Egypt and Russia to name but a few.[144]

The possible use of NEWS, Remote Control, and other undisclosed communications monitoring technology is reminiscent of Edward Snowden's revelations of the NSA's use of similar software such as the XKEYSORE application.

This paints a worrying picture of the country's privacy landscape, due to the fact that this surveillance is entirely unwarranted and in violation of article 31 of the CoK 2010. It is only logical for one to worry about the implications of the use of information acquired using such methods, questions arise such as whether due process will be followed in the use of this information or whether in keeping with the established precedent, the follow up will be of an extra-judicial manner.

Data Protection

Kenya does not currently have in its laws any legislation specifically concerning data protection. There however exists the Data Protection Bill 2013,[145] which was forwarded to the Attorney General for publication and the Cabinet Secretary for Information Communication and Technology announced the Bill was expected to be presented in Parliament by the end of May 2014. Its fate currently hangs in legislative limbo.

The Bill while a positive step in the right direction, wanes in comparison to the (Economic Cooperation of Western African States) ECOWAS Supplementary Act A.SA.1/01/10 on Personal Data Protection, on which the Kenyan bill is based or the European Data Protection Directive,[146] on which the ECOWAS Act is based.

There are two major weaknesses in the bill. First, the draft bill only applies to public bodies. This limitation has a profound effect on the ability of citizens to both obtain and control the use of their personal information held by private bodies including private employers, banks, telecommunications companies, water, electricity, health and insurance companies and other

---

[144] Daniel Finnan, "Kenyan government asked Hacking Team to attack dissident website," *Radio France Internationale,* July 17, 2015, http://rfi.my/1Kkbq4V, 22nd March 2016.

[145] Available at http://www.cickenya.org/index.php/legislation/item/174-the-data-protection-bill-2012#.U3sfr1hdU01 on 1st February 2016.

[146] Directive 95/46/EC

private institutions.[147] Thus, the draft bill fails to meet the requirements under Section IV (3) of the Declaration of Principles on Freedom of Expression in Africa which states "Everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies."

Second, article 5 of the draft bill prohibits the collection of personal information "by unlawful means". However, under Article 3, public bodies can ignore requirements that the collection and processing of personal information if "on reasonable grounds" for the purposes of enforcing any law by any public sector agency. This loophole sets a very low threshold for bypassing of laws and if not amended will be at the whim of courts to interpret. Possibly leading us to a conflicting situation in respect to the admissibility of the obtained evidence as mentioned in the common law case of *Reg v Leathem*[148] and the East African case *Kuruma v The Queen.*[149] If this takes place I trust that the courts will be guided by Article 50(4) of the Cok 2010, which provides for the exclusion of any evidence obtained in a manner contrary to any of the right and fundamental freedoms protected in the Bill of Rights.[150]

---

[147] Article 19, *Kenya Draft Data Protection Bill* critically limited, Available at: https://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited on 29th January 2016.

[148] [1861] Cox C C 498

[149] I1954) Court of Appeal of East Africa.

[150] Kiage J, *Essentials of Criminal Procedure*, Law Africa, 26.

Chapter 5: Conclusion

The right to privacy in its various forms, be it the right to be let alone as espoused by Warren and Brandeis or secondary privacy found under the communitarian Ubuntu philosophy, is essential to the enjoyment of our ethnic, cultural and religious diversity as protected under our constitution and public international law.

Unfortunately, today's world faces the relentless scourge of terrorism. Al-Qaeda, the Islamic state / Daesh and Boko Haram are some of the characters in a performance on a global stage. The post 9/11 government surveillance and counter terrorism measures are a natural and expected response. Regionally, the Somali based Al-Shabab terrorist organisation continues to threaten the nation's security and the peace of mind of the populace. Every successful terrorist attack mounts further pressure on the nation's armed forces and intelligence agencies to increase their efforts and prevent the possibility of another attack. It is with this in mind that compromises to the right to privacy and other fundamental rights were envisioned in article 24 of the CoK. The implementation of these limitations must be strictly for the purposes envisioned in the law and not for political reasons as has been demonstrated in the past.

Further, as a nation consisting of 47 distinct cultural groups, politically motivated, divisive rhetoric is a tool still heavily used by the ruling class as a means of maintaining the status quo. This has greatly contributed to several instances of inter-cultural violence such as the 1992 tribal clashes and the 2007/08 post-election violence. Anti-hate speech and incitement laws are already in place and their use in partnership with the proper procedures for acquisition of electronic and social media evidence provided for in the Criminal Procedure Code as well as the law enforcement guidelines found under the Social Media company's Terms of Service agreements, will result in fair trial for the accused and proper administration of justice.

Recommendations

1. Ensure that an amended Data Protection Bill, is passed into law, this will protect the right to privacy of citizens in accordance with international human rights law;
2. Ensure that government authorities expand existing protections for the right to privacy and data protection in relevant national laws to guarantee respect for these rights in the context of digital communication;

3. Introduce safeguards to ensure that the rights of mobile telephone subscribers and internet users in relation to their personal data are guaranteed;
4. Revoke the Regulations adopted under the 2009 Information and Communications Act which unlawfully limit the right to privacy;
5. Appoint an independent authority to investigate communications monitoring and surveillance programmes conducted by the Kenyan government and ensure that these practices respect the government's national and international obligations to protect the privacy of its citizens and their personal data;
6. Take steps to assess communication surveillance national policies and practices with a view to complying with the International Principles on the Application of Human Rights to Communications Surveillance.

Bibliography

Books

1. Adam Moore, *Privacy Rights, Moral and Legal Foundations*, University Park: The Pennsylvania State University Press, 2010.
2. Anita L. Allen, *Uneasy Access: Privacy for Women in A Free Society*, Rowman & Littlefield, 1988.
3. Brinnen JM, ' *Poems by Emily* Dickenson', 1890.
4. Cranor, L. F., Kelley, P.G., McDonald, A., & Reeder, R. W, A Comparative Study Of Online
5. Dimitri Bertsekas & Robert Gallagher, *Data Networks* (2d Ed. 1992), Prentice Hall, 1991.
6. George Orwell, *Nineteen Eighty-Four* , 8 June 1949 (Secker and Warburg, London)
7. Inness JC., *Privacy, Intimacy, And Isolation,* Oxford University Press, Oxford, 1992.
8. Jean Jacques Rousseau, *The Social Contract*, Swan Sonnenschein & Co, *1895.*
9. Judith Wagner Decew, *In Pursuit Of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997.
10. Kiage J, *Essentials of Criminal Procedure*, Law Africa, Nairobi, 2010
11. Miller AR, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, Signet, 1971.
12. Posner, Richard A. *The Economics of Justice*. Harvard University Press, 1981.
13. Privacy Policies and Formats, Springer Berlin Heidelberg, 2009.
14. The Bible, New International Version
15. Thomas M. Cooley, *Law of Torts* (2d ed. 1888).

Journal Articles

1. Atwell, Maureen, The Use of Social Media Evidence in Criminal Child Support Prosecutions (2013). 7 *Phoenix Law Review 1* (2013)

2. Beaney WM., 'The Right to Privacy and American Law', 31 *Law and Contemporary Problems* (Spring 1966)

3. Brenner, Susan W, The Privacy Privilege: *Law Enforcement, Technology and the Constitution. Journal of Technology Law and Policy*, Vol. 7, (2002).

4. Dorothy J. Glancy, "The Invention of the Right to Privacy", *Arizona Law Review*, (1979).

5. E.L. Godkin, *The Rights Of The Citizen, IV-To His Own Reputation,* Scribner's Magazine, July-Dec. 1890, At 65

6. Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An answer to Dean Prosser, 39 *New York University Law Review* (1964).

7. Gaffin, Elizabeth, Friending Brandeis: Privacy and Government Surveillance in the Era of Social Media (April 30, 2012).

8. Geoffrey A. Fowler & Worthen B, *The Internet Industry Is on a Cloud—Whatever That May Mean*, Wall Street. Journal, March 26, 2009.

9. Gerety T, 'Redefining Privacy', 12 *Harvard Civil Rights-Civil Liberties Law Review, (1977).*

10. Graham Cormode and Balachander Krishnamurthy Key differences between Web 1.0 and Web 2.0 *First Monday*, Volume 13, (2008).

11. Hassan, Qusay, "Demystifying Cloud Computing" , *The Journal of Defense Software Engineering* (CrossTalk) 2011 (Jan/Feb)

12. John Locke, *The Second Treatise of Government*, Barnes & Noble Publishing, 1690.

13. Justice Louis Brandeis and Samuel Warren, The Right to Privacy, *Harvard Law Review*, Volume IV December 15, 1890

14. Justin P. Murphy and Adrian Fontecilla, Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues, 19 *Richmond. Journal of Law & Technology* (2013)

15. Justin P. Murphy, Matthew A.S. Esworthy, The ESI Tsunami: A Comprehensive Discussion about Electronically Stored Information in Government Investigations and Criminal Cases, the *American Bar Association's Criminal Justice Magazine.* Spring 2012 issue.

16. Kabau T and Ambani JO, 'The 2010 Constitution and the Application of International Law in Kenya: A Case of Migration to Monism or Regression to Dualism? *1 Africa Nazarene University Law Journal* 1, (2013).

17. Ken Strutin, Social Media and the Vanishing Points of Ethical and Constitutional Boundaries, 31 *Pace Law Review* 228, (2011).

18. Kenneth L. Karst, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 Law and Contemporary Problems,

19. Kevin W. Saunders, Privacy and Social Contract: A Defense of Judicial Activism in Privacy Cases, 33 *Arizona Law Review* 811, (1991).

20. Kwamwangamalu, NM. & Nkonko, M, Ubuntu in South Africa: a Sociolinguistic Perspective to a Pan-African Concept, *Critical Arts Journal, Vol.13, No. 2, (1999).*

21. Louw, DJ. 1999. Ubuntu: An African assessment of the Religious Other. *The Paideia Project Proceedings from the Twentieth World Congress of Philosophy,* (August 1998)

22. McDonald, A., & Cranor, L. F, The Cost of Reading Privacy Policies, *ACM Transactions on Computer-Human Interaction*, (2008)

23. Mokgoro, JY. 1997. *Ubuntu and the Law in South Africa.* Seminar Report of the Colloquium, Konrad-Adenauer Stiftung. Johannesburg.

24. O'Connor, James R., Asocial Media: Cops, Gangs, and the Internet (2013). James R. O'Connor, Note, 42 *Hofstra Law Review.* 647, 2013

25. Post R, 'Three Concepts of Privacy', 89 *Georgetown Law Journa*l, 2087 (2001).

26. Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy,* 10 *Northern Illinois University Law Review,* (1990).

27. Soghoian, Christopher, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era, on *Telecomm. and High Technology Law.* (August 17, 2009). 359; Berkman Center Research Publication No. 2009-07.

28. Solove, Daniel J., Conceptualizing Privacy, *California Law Review,*

29. Thomson J J, *'The Right to Privacy', in Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press (1984).

30. Van Binsbergen, W. Ubuntu and the globalisation of Southern African Thought and Society. *Philosophical Faculty, Erasmus University, Rotterdam, the Netherlands, (2002).*

Conference Papers

1. H. N. Olinger, J. J. Britz, and M. S. Olivier. "Western Privacy and Ubuntu — Influences in the Forthcoming Data Privacy Bill". In: Ethics of New Information Technology — Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005). Ed. by P. Brey, F. Grodzinsky, and L. Introna. Enschede, The Netherlands, July 2005.

2. Scorgie, F. 2004. *Ubuntu in Practice.* HIVAN Research Associate. (Comments received by email.) Email to: HN Olinger (Hanno.Olinger@Kumbaresources.com) [6 November 2004]

Institutional Publications

1. Article 19, *Kenya Draft Data Protection Bill* critically limited, Available at: on 29th January 2016.

2. Communications Commission of Kenya, Kenya and ITU sign administrative agreement for KE-CIRT/CC, 17 February 2012.

3. Quarterly Sector Statistics Report Third Quarter Of The Financial Year 2014/15 (Jan-Mar 2015),

4. Vodafone, Law Enforcement Disclosure Report

International Instruments

1. *International Covenant on Civil and Political Rights,* 1 May 1972, 999 UNTS 171 *Vienna Declaration and Programme of Action: Report of the World Conference on Human Rights*, Vienna, 14-25 June 1993, UN Doc A/CONF.157/23 (1993); 32 ILM 1661 (1993)
2. UNGA, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III).
3. African charter on the Rights and Welfare of the Child, July, 1990, OAU Doc. CAB/LEG/24.9/49.
4. UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, 3.

National Law

1. *Constitution of Kenya (2010)*
2. *Criminal Procedure Code* 2010(Cap 75 of the laws of Kenya) (Revised 2012)
3. *Evidence Act*, (Cap 80) 2012 (Revised 2014).
4. Legal Notice No. 10 to the *Kenyan Communications and Information Act*, 7 February 2014
5. *National Intelligence Service Act*, No. 28 Of 2012.
6. *National Police Service Act* (Cap 84 of the laws of Kenya)
7. *Prevention of Terrorism Act*, No. 30 of 2012.

Internet Sources

1. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008_12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf
2. http://www.cickenya.org/index.php/legislation/item/174-the-data-protection-bill-2012#.U3sfr1hdU01

3. http://www.irishtimes.com/news/world/africa/mobile-phones-ring-changes-in-kenya-with-internet-access-1.2242054

4. http://www.npr.org/templates/story/story.php?storyId=113450803

5. http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx

6. *http://www.pewinternet.org/topics/Web-20.aspx.*

7. http://www.regent.edu/acad/schlaw/student_life/studentorgs/lawreview/docs/issues/v25n1/05Sundquistvol.25.1.pdf

8. https://support.twitter.com/articles/41949#7

9. https://twitter.com/privacy?lang=en

10. https://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited

11. https://www.facebook.com/safety/groups/law/guidelines/

12. https://www.google.com/intl/en/policies/privacy/

13. https://www.youtube.com/watch?v=ftjdDOfTzbk

News Articles

1. Njeri Wangari, "Blogger Abraham Mutai Arrested and Released for reporting on Corruption in Isiolo County,"

2. Njeri Wangari, "24 Year old Nancy Mbindalah Held in Custody then Pardoned for Undermining the Embu Governor,' *Kenya Monitor,* January 22, 2015, http://bit.ly/1M0vF9a.

3. Shitem Khamadi, "Web developer challenges constitutionality of infamous charge 'misuse of licensed telecommunication equipment'," *Kenya Monitor,* May 6, 2015, http://bit.ly/1GP5jFR.

4. Morgan Marquis-Boire et al., *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Citizen Lab, January 15, 2013, http://bit.ly/1hNzLcN.

5. Vincent Achuka and Walter Menya, "Wikileaks: NIS purchased software to crack websites,"*Daily Nation,* July 11, 2015, http://bit.ly/1LyRP2U.

6. Daniel Finnan, "Kenyan government asked Hacking Team to attack dissident website," *Radio France Internationale,* July 17, 2015, http://rfi.my/1Kkbq4V, 22nd March 2016.

7. ITU News, Making an IMPACT on global cybersecurity, October 2009, Available at: https://www.itu.int/net/itunews/issues/2009/08/22.aspx

8. Italians reject bid to close Kahawa Tungu," *Daily Nation,* July 12, 2015, http://bit.ly/1PtYTnw,