THE USE OF ELECTRONIC TRACKING AND MONITORING SYSTEMS AND THE RIGHT TO PRIVACY

M Wekesa, MM Muendo & A Mikinyango

Daystar University School of Law, Nairobi, Kenya

Email: mwekesa@daystar.ac.ke

Abstract

The Right to Privacy is a right that had been recognizes and applied differently all over the world. On the other side Governments have employed electronic monitoring and tracking techniques as part of their security tool kit. The employment of electronic monitoring has an impact on the individual's right to privacy. While conducting electronic monitoring and tracking countries are required to uphold the right to privacy. This paper seeks to analyze the Right to Privacy and to what extent it has been implemented in relation to Electronic monitoring and tracking. The paper will compare legal frameworks from different States on the implementation of the right to privacy in relation to Electronic monitoring. The paper will also give recommendations that can serve as a guide to assist policy makers.

Key words: Privacy, Electronic monitoring and tracking

1. Introduction

Although the concept of privacy is as old as mankind,[1] it was not until about 1890 that the term was defined as 'the right to be let alone'.[2] This description of privacy illustrates the difficulty in pinning down what constitutes 'privacy'. Some Judges have expressed their frustrations at the ambiguity of what comprises privacy.[3] More recently, some scholars have looked at privacy as the 'aura' around the individual which separates the individual from the outside world.[4] Other scholars [5] have sought to break down the term 'privacy' to include the right to be let alone, limited access to the self, secrecy, control of personal information, personhood and intimacy.

[1] A Lukács 'What is Privacy? The History and Definition of Privacy' at http://u-szeged.academia.edu/AdriennLukacs or http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (seen 27 Jan 2019)

[2] SD Warren & LD Brandeis 'The Right to Privacy' 4(1890)5 *Harvard Law Review* p 193, SD Warren & LD Brandeis 'The Right To Be Let Alone' 67 (1891) *Atlantic Monthly* 428-29

[3] *Ettore v. PhilcoTelev. Broad. Corp*., 229 F.2d 48 1, 485 (3d Cir. 1956) (Biggs J), *Paul v. Davis*, 424 U.S. 693, 7 13 (1976) (Rehnquist, J.)..

[4] n1 (Lukacs) p 258.

[5] DJ Solove *Nothing to Hide: the False Tradeoff between Privacy and Security* (New Haven & London: Yale University Press, 2011) p 4.

The need to protect privacy appears to be quite old with Adam and Eve covering themselves with leaves.[6] Under Plato's 'Laws' he envisaged a society that did not leave a person alone. In ancient times, a person belonged to a community, hence, his life could not be private. With the advent of industrialization, people started living in cities – in small places, and privacy became a challenge.[7] At the same time, people in cities could afford some level of 'privacy' as there were no village mates to intrude and control their lives. However, the appearance of the 'gutter' press or tabloid newspapers provided an avenue of intrusion into the 'private' lives of the urbanites.[8] Technological and societal changes and their impact on privacy were thus first documented in 1890.[9]Currently, this right is considered to be made up of[10]

> […] the right to determine to what extent the thoughts, the sentiments and emotions of the individual shall be communicated to others. The right to be let alone basically ensured protection against the unwanted disclosure of private facts, thoughts, emotions etc' […]

Of these, informational privacy has attracted a lot of attention at the ECtHR.[11]Where privacy is diminished,it is thought that the capacity for critical subjectivity shrinks, and the capacity for citizenship becomes impaired. An impaired citizenry is in turn not capable of democratic government. A government that allows too much surveillance of its citizenry by implication ceases to be a democratic government. Citizens in such governments gradually lose their ability to pursue and form agenda for improvement of humanity. Political and economic institutions influence the way citizenship is practiced – the voting, and other forms of decision making. These institutions may encourage, restrict or permit the manner in which citizenship is exercised. Networked information and communication technologies mediate the practice of citizenship.[12] It is recorded that surveillance of the citizenry in the former German Democratic Republic was propelled to dizzying heights through the use of police specifically meant for that purpose and use of relatives and friends to spy on each other. There was not only no freedom of expression but there was also no privacy. People lived in fear. They could not realize their autonomy.[13]

---

[6] MR Konvitz 'Privacy and the Law: a Philosophical Prelude' 31(1966)2 *Law and Contemporary Problems* 272.

[7] n1 (Lukacs)

[8] BE Bratman 'Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy' 69 (2002) *Tennessee Law Review* p 344.

[9] n2 (Brandeis)

[10] n1(Lukacs) p 258, see also Nathan, Eavesdropping, 225 LT 119, 120 (1958) cited in WJ Hoese 'Electronic Eavesdropping: A New Approach' 52(1964)1 *California Law Review* 142; JE Cohen 'What Privacy is for' 126 (2013) *Harvard Law Review* 1904;J Waldo, HSL Lin, LI Milett (eds.) *Engaging Privacy and Information Technology in a Digital Age*(Washington National Academies Press 2007)

[11] *X v United Kingdom* App no 9072/82 (ECHR, 6 October 1982); *Murray v United Kingdom* Series A No. 300-A (ECHR, 28 October 1994); *Leander v Sweden* Series A No. 116 (ECHR, 26 March 1987); *MK v France* App no 19522/09 (ECHR, 18 April 2013)

[12] n11 (Cohen)

[13] A Funder,Stasiland (2002) 57 as cited in U Cheer "The future of privacy. Recent legal developments in New Zealand" (2007) 13 *Canterbury Law Review* 169 at https://ir.canterbury.ac.nz/bitstream/handle/10092/3254/12606673_Cheer_Privacy.pdf?sequence=1

The relationship between an individual, institutions and technology has been painted thus-[14]

> In the networked information society, those experiences are mediated by search engines, social networking platforms, and content formats. Search engines filter and rank search results, tailoring both the results and the accompanying advertising to what is known about the searcher and prioritizing results in ways that reflect popularity and advertising payments. Social networking platforms filter and systematize social and professional relationships according to their own logics. Content formats determine the material conditions of access to information — for example, whether a video file can be copied or manipulated, or whether a news forum permits reader comments. Each set of processes structures the practice of citizenship and also subtly molds network users' understanding of the surrounding world. To an increasing degree, then, the capacity for democratic self-government is defined in part by what those technologies and other widely used technologies allow, and by exactly how they allow it.

Surveillance can be done by both government and private actors.

The jurisprudence from the European Court of Human Rights indicates certain examples of privacy that fall under article 8 as including access to personal data [15], telephone interception [16], choice or change of name [17], sexual life [18], profession or domicile [19], protection against environmental nuisances [20], and the right to establish and develop relationships with others [21]. In all these cases, the ECtHR has had to contend with two aspects of the Convention's article 8, firstly, whether there was infringement of the right to privacy (article 8(1)), and secondly, whether such infringement was within the meaning of article 8(2). The advent of computers and more specifically, the internet, has brought with it the challenge of data protection. Whereas data protection can be seen as a part of privacy, many states have developed specific regimes for protecting data.[22]

[14] N11 (Cohen) p 1913

[15] *Leander v Sweden* judgment of 26 March 1987, no. 9248/81 par. 46, 48; *Gaskin v the United Kingdom* judgment of 07 July 1989, no. 10454/83 par. 36-37

[16] *Klass and Others v Germany* judgment on 6 September 1978, no. 5029/71 par. 41; *Halford v the United Kingdom* judgment on 25 June 1997, no. 20605/92 par. 41, 44, 46; *Malone v the United Kingdom* judgment on 2 August 1984, no. 8691/79 par. 64; *Huvig v France* judgment on 24 April 1990, no. 11105/84 par. 25; *Kruslin v France* judgment on 24 April 1990, no. 11801/85 par. 26

[17] *Guillot v France* judgment on 24 October 1993, no. 22500/93 par. 21-22; *Burghartz v Switzerland* judgment on 22 February 1994, no. 16213/90 par. 24

[18] *Dudgeon v the United Kingdom* judgment on 22 October 1981, no. 7525/76 par. 40-41

[19] *Niemietz v Germany* judgment on 16 December 1992, no. 13710/88 par. 28-33

[20] *López Ostra v Spain* judgment on 09 December 1994, no.16798/90 par. 51

[21] n15 (*Niemietz*) par. 29

[22] 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data , Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)

Privacy allows individuals to grow, experiment, make mistakes and develop.[23]

In Kenya, it has been stated that-[24]

> 64. 'Privacy,' 'dignity,' 'identity' and 'reputation' are facets of personality. Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Personal choices governing a way of life are intrinsic to privacy. Privacy attaches to the person since it is an essential facet of the dignity of the human being.
>
> 66. […] The right of privacy is a fundamental right. It protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices.

It is said that the right to privacy enables an individual to enjoy all other rights such as freedom of expression, freedom from interference with an individual's correspondence, and freedom of association away from social and governmental control.[25] The US Supreme Court has held that-

> The Makers of our Constitution... sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men.[26]

Internationally, this right is considered not to be absolute but subject to certain limitations such as national security, public safety and protection of the rights of others. One may also add the point of public interest. These limitations no doubt are a source of litigation in many countries.[27] The ECtHR considered that privacy includes the choice of sexual orientation and therefore national legislation criminalizing homosexuality has been deemed as an unnecessary intrusion into the right to privacy.[28] The court has also recognized that privacy covers the physical and moral integrity of the person.[29] The court has been emphatic that wire-tapping (interception of communication) violates the right to privacy,[30] that mass surveillance of email correspondence [31]

[23]SE Dorraji& M Barcys 'Privacy in Digital Age: Dead Or Alive?! Regarding the New EU Data Protection Regulations' 4(2014)2 *Social Technologies* p 306–317

[24]*Kumena v KTDA Agency Ltd* [2019] eKLR (HCt)

[25] F Volio 'Legal Personality, Privacy and the Family', in Henkin (ed) *The International Bill of Rights* (Colombia University Press 1981).

[26]*Olmstead v United States* 277 U.S. 438 (1928).at 478 (Brandeis J, dissenting)

[27] A Johns 'The Right to Privacy in the Digital Age: Recent Developments and Challenges' STEP Caribbean Conference St. Lucia April 25–27, 2016

[28]*Dudgeon v United Kingdom* App no 7525/76 (ECHR, 22 October 1981).

[29]*X & Y v Netherlands* App no 8978/80 (ECHR, 26 March 1985) para 22; *Costello-Roberts v United Kingdom* App no 13134/87 (ECHR, 25 March 1993) para 36.

[30]*A v France* App no 14838/89 (ECHR, 23 November 1993); *Halford v United Kingdom*, supra n 7.

and storage of personal data by security agencies without a justifiable reason [32] amounts to an infringement of the right to privacy. The right to respect of private life is the "right to live privately, away from unwanted attention".[33] And that such notion includes activities in business and professional life.[34]

In Marcel v Metropolitan Police Commissioner[35] the Police broke into the plaintiff's premises and retrieved documents that were relied upon in criminal proceedings. Concurrently civil proceedings were also taking place and a subpoena was served on behalf of the parties seeking disclosure of the documents. The Court held that the subpoena should be set aside.
The Judge expressed the following sentiments:

> If the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state.[36]

Thus the right to privacy is a right that is fundamental to people in order to have a full life.

2. Constitutional and statutory underpinnings of the right to privacy

Many international instruments recognise the need to protect the right to privacy including protection against arbitrary search.[37] The European Convention of Human Rights (hereinafter referred to as ECHR) states in Article 8 that:

> Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

---

[31] *Liberty v UK* App no 58243/00 (ECHR, 1 July 2008); *Copland v United Kingdom* App No 62617/00 (ECHR, 3 April 2007) where the Court held that metadata, relating to the location, source and timing of communications (but excluding their content), also fell within the scope of 'correspondence' under Article 8.

[32] *Shimovolos v Russia* App no 30194/09 (ECHR, 21 June 2011).

[33] *Antovic and Mirkovic v Montenegro*Application no. 70838/13 -II *Final* Judgment 28/02/2018 ECtHR (Joint Concurring Opinion of Judges Vucinic&Lemmens, par 3); see also *Smirnova v Russia*,nos. 46133/99 and 48183/99, § 95, ECtHR 2003-IX (extracts); *Sidabras and Džiautas v Lithuania*, nos. 55480/00 and 59330/00, § 43, ECtHR 2004-VIII; *Couderc and Hachette Filipacchi Associésv France* [GC], no. 40454/07, § 83, ECtHR 2015 (extracts); *SatakunnanMarkkinapörssi Oy and Satamedia Oy v Finland* [GC], no. 931/13, § 130, ECtHR 2017 (extracts); and *Bărbulescu v Romania* [GC], no. 61496/08, § 70, ECtHR 2017 (extracts)

[34] n--- (Antovic)

[35] Marcel v Metropolitan Police Commissioner 225-240 Ch[1992]

[36] Marcel v Metropolitan Police Commissioner 240 [1992]

[37] The 1948 United Nations Universal Declaration of Human Rights (Article 12), The 1966 United Nations International Covenant on Civil and Political Rights (Article 17), The 1950 Council of Europe European Convention of Human Rights (Article 8) and The2000 European Union Charter of Fundamental Rights (Article 7)

Regarding article 8(2) the ECtHR has consistently stated that the phrase "in accordance with the law" means that the impugned action must have a basis in domestic law[38] and must accord to the rule of law.[39]It has been said that disclosure of information in the public interest -[40]

> […] must be disclosure justified in the public interest, of matters, carried out or contemplated, in breach of the country's security, or in breach of law, including statutory duty, fraud, or otherwise destructive of the country or its people, including matters medically dangerous to the public; and doubtless other misdeed of similar gravity

In a complaint about authorities conducting a body search for which they did not have a warrant the court stated that this was interference with the applicant's privacy.[41] The court further stated that telephone calls made from home or business premises are covered under the rubric of 'private life' and 'correspondence'.[42]

The ECtHR has previously considered that states require strong criminal laws to protect rights.[43] It has held that the Contracting Parties must set up adequate legal framework in order to protect the respect of the physical integrity of hospital patients[44].

With respect to interception of communication for criminal investigations, the ECtHR has established certain minimum standards [45]which also apply *mutatis mutandis* in case of national security[46] to avoid abuse of power. These are that – [47]

> […] the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed

The ECtHR has also held that-[48]

[38]*Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007
[39]*Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V, *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010, *Roman Zakharovv. Russia* [GC], no. 47143/06, § 171, ECHR 2015
[40]*Beloff v Presdram* [1973] F.S.R. 33 at p.57
[41]*Cacuci and SC Virra&Cont Pad SRL v Romania* Application no. 27153/07-IV judgment of 13 November 2018 (ECtHR)
[42]*Cacuci and SC Virra&Cont Pad SRL v Romania* Application no. 27153/07-IV judgment of 13 November 2018 (ECtHR), *Halford v. the United Kingdom*, 25 June 1997, § 44, Reports of Judgments and Decisions 1997-III (ECtHR)
[46]*X and Y v. the Netherlands*, 26 March 1985, § 24, Series A no. 91;§§ 23, 24 and 27; *M.C. v. Bulgaria*,no. 39272/98, § 150, ECHR 2003-XII § 150
[43]*X and Y v. the Netherlands*, 26 March 1985, § 24, Series A no. 91;§§ 23, 24 and 27; *M.C. v. Bulgaria*,no. 39272/98, § 150, ECHR 2003-XII § 150
[44]*Codarcea v. Romania*, no. 31675/04, §§ 102-104, 2 June 2009
[45]*Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006‑XI; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007
[46]*Roman Zakharovv. Russia* [GC], no. 47143/06, § 171, ECHR 20158
[47]*Big Brother Watch and Others v. The United Kingdom* Applications nos. 58170/13, 62322/14 and 24960/15 Decision of 13 September 2018 (Request for referral to the Grand Chamber pending) p 3
[48]n---- (Big brother)

> 306 […] Foresee ability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to resort to such measures so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures …]

The Telecommunications Industry Dialogue and the Global Network Initiative (GNI), an international NGO that brings together internet, telecommunications and information technology companies, civil society groups including human rights and media freedom activists, academics and investors have issued a joint position on network and internet access shutdowns as follows-

> The protection of national security and public safety are important government concerns. Network shutdowns, and the wholesale blocking of internet services, however, are drastic measures that often risk being disproportionate in their impact. [49] Governments who employ these measures often do so without justifying them as necessary and proportionate under international human rights standards.

Maximillian Schrems, an Austrian citizen who lived in Ireland, had held a Facebook account since 2008.[50] It came to light that Facebook Ireland usually transferred all data in Facebook's Irish subsidiary to servers located in the United States for processing. He brought a complaint of violation of his privacy saying that the laws on privacy in the US did not offer adequate protection of data and that public agencies in the US were at liberty to use that data as they wished. The Commissioner dismissed the complaint saying that the US offered sufficient protection based on the Pearl Harbor agreement. The European Court of Justice found that US authorities had power to overlook the Pearl Harbor agreement and therefore that the data protection laws in the US were not as stringent as those in the EU. The court further observed that the protection of the right to privacy would be meaningless if state authorities are allowed to access electronic communication casually and without due justification based on national security and crime prevention and accompanied with verifiable safeguards.

[49] n--- (Vodafone Group Plc)

[50] *Schrems v Data Protection Commissioner* Case No C-362/14 decided 6 October 2015 (CJEU)

> Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8(1) of the Convention.[51]

In a seminal thesis on the situation in Tanzania-, the author focuses on registration of sim cards justifying it as necessary for the state to monitor who send which message and to whom on grounds of security of the majority. It is acknowledged that the constitutional protection of privacy under Tanzanian law is similar to that of Kenya and both are based on the UDHR document. At the point of registration for a sim card, an applicant is required to divulge a lot of personal information. Officials at government agencies and private companies are obliged to maintain confidentiality as a way of preventing wanton dispersal of personal information. There is no guarantee of privacy of the messages. The document says nothing about use of stored information by public authorities neither does it deal with the thorny issue of interception of communication.[52]

3. Historical development of digitization

Bell invented the telephone in Boston, USA and the first telephone exchange was set up in1877.[53] It is documented that by 1890 there were telegraphs, portable cameras and recording devices on the market. Newspapers which flourished around the same time, created an appetite and market for gossip.[54]

It is recorded that wiretapping in the US started before the telephone was invented.[55] The first statute prohibiting wiretapping was enacted in California in 1892. Two years later saw the first person to be convicted of wiretapping. The defendant listened in on telegraph lines and sold the information to commercial agents. Corporates and private detectives dominated wiretapping until 1920. These were found to be abusing wiretapping. Currently, wiretapping appears to be happening on a massive scale. Wiretapping appears to have metamorphosed into 'dataveillance', that is, not only is the data tapped but its stored and tracked.

Advancements in technology have seen to the spiralling of social networking websites (SNWs) such as Facebook, twitter, whatsapp, telegram and linkedin amongst others.[56] These SNWs provide a medium of expression and dissemination of information in real time. But before one can access them, a person is required to register by divulging personal information. SNWs therefore hold a lot

---

[51] *Rotaru v Romania*, [2000] ECHR 28341/95, paras. 43-44.

[52] KG Ndossy ' Mobile Cellular Communication and its Effect on Personal Data Protection in Tanzania-Practical and Legal Analysis under Tanzanian Law'A Thesis submitted in partial fulfilment of the requirements for the award of the Degree of Master of Laws (Information and Communication Technology Laws) of the University of Oslo, 2014

[53] J Brooks Telephone: The First Hundred Years*Passim* 1976 pp 59-101

[54] n25 (Glancy) p1

[55] A White 'A Brief History of Surveillance in America'*Smithsonian magazine* April 2018 https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/#SQdPTWFJ2qfTMZK3.99

[56] A Marsoof 'Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression' *International Journal of Law and Information Technology*19(2):110-132 May 2011 DOI: 10.1093/ijlit/eaq018

of personal data including information received from others. By 2010 Facebook is said to have had over 400 million users while twitter is recorded as having about 75 million users.[57] SNWs need personal information for purposes of advertising. The more people they can reach the better. Hence, users are lured in presenting and accepting friend requests and even chats that create a false impression of intimacy. The latter is made worse by dating sites on which participants disclose their intimate details. SNWs have therefore created a society that is akin to an e-society. A society in which those with criminal intent can 'steal' other people's identity. Most users are not technologically savvy to be able to protect their own identities. Worse still, the service providers for SNWs may not have full proof protection of individual identities.

Telecommunications companies' core business is connectivity. They operate physical network infrastructure such as satellite, mobile phone towers, fibre-optic cables and data centres which are used to communicate and to access content. These networks are mere conduits but not creators or editors of the content. The so-called 'Over-The-Top' (OTT) internet companies such as Facebook, LinkedIn, Twitter and Google have as their core business the provision of advertising, content and communications services to their clients. They have a greater control over both the services, apps and content (videos, photos and text) hosted on their servers. The OTT use telecommunications networks to facilitate interaction between their customers. Convergence of telephone and TV could enable telecommunications companies to host some content and thereby have some control on the content.[58]

Regarding transmission through the Internet, it has been said that-[59]

> 1. Internet communications are primarily carried over international sub-marine fibre optic cables operated by [Communications Service Providers] CSPs. Each cable may carry several "bearers", and there are approximately 100,000 of these bearers joining up the global Internet. A single communication over the Internet is divided into "packets" (units of data) which may be transmitted separately across multiple bearers. These packets will travel via a combination of the quickest and cheapest paths, which may also depend on the location of the servers. Consequently, some or all of the parts of any particular communication sent from one person to another, […] may be routed through one or more other countries if that is the optimum path for the CSPs involved.

In the UK, it has been reported that the Government Communications Headquarters (GCHQ) was intercepting such data under the codename 'Tempora' while USA was also intercepting such data under the code names of 'Prism' and 'Upstream'. [60]

---

[57] Facebook at http://www.Facebook.com/press/info.php?statistics (accessed-25.08.2010); Twitter at http://themetricsystem.rjmetrics.com/2010/01/26/new-data-on-twitters-users-and-engagement/

[58] Vodafone Group Plc (UK) 'Freedom of Expression and Network Censorship, Digital Rights and Freedoms, at https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_freedom_expression_network_censorship.pdf Accessed on 12 Sept 2019

[59] *Big Brother Watch and Others v. The United Kingdom* Applications nos. 58170/13, 62322/14 and 24960/15 Decision of 13 September 2018 (Request for referral to the Grand Chamber pending) p 3

[60] n--- (Big brother)

In *R v Brown*[61]Lord Hoffman made the following remarks:

> My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.

These sentiments are echoed in today's time period especially with the reliance on Electronic Motor Vehicle Data by law enforcement. Anobserver is able to know almost all the whereabouts of the surveyed subject. This is a threat to one's privacy and needs to be safely guarded and protected otherwise a person will not have a safe haven to hide in or think. A person is entitled to privacy in areas he has an expectation of privacy. A car qualifies as such a place one can do whatever he feels like within the confine of his car so long as it's legal.

4. Challenges to privacy in the digital age

Digital age is characterized by digital information contained in smart phones and the internet and used in all spheres of our lives including but not limited to education, medical, insurance, financial services, construction and social platforms.[62] These technologies have improved the human rights discourse on the one hand and they pose dangers on the other hand through data surveillance, monitoring, and interception. The right to privacy is in danger.

Many people worldwide have embraced information communication technologies. Individuals frequently share personal information about themselves, pictures and videos online. Individuals always leave traces behind whenever they use a computer or a phone. It is easy to track people because they willingly give up their location information through smart phones. Besides, we associate with 'friends' freely and liberally disseminate our private information. Although one may want to blame technology, it is vital for one to pay close attention to matters of one's privacy.[63]Data collected singly or repeatedly can reveal a lot of information such as a person's identity, behaviour, associations, medical condition, sexual orientation, nationality, race, a person's location, all people in a given location such as at a political meeting, interactions over time and so on.

[61]R v Brown 545 1 All ER [1996]

[62] J Damen, L Köhler & S Woodard 'The Human Right of Privacy in the Digital Age' *Staat, Recht und Politik* — Forschungs- und Diskussionspapiere 3, 2017

[63] J Bloem M Doorn SDuivestein T Manen E Ommeren 'Privacy, Technology and the Law: Big Data for Everyone through Good Design' VINT Research Report 3 The Sogeti Trend Lab VINT, 2013 [interactive]. At <http://blog.vint.sogeti.com/ wp-content/uploads/2013/04/VINT-BigData-Research-Privacy-Technology-and-theLaw.pdf>.[accessed on 25 Jan 2019].

ICTs enhance our ability to seek, receive and impart information, thereby promoting the freedom of expression. They provide an opportunity to improve on economic social and cultural rights. Through ICTs people have new avenues for channelling public services, conducting commerce and improving knowledge globally. The use of the internet in the phone enables people to communicate human rights violations in real time and it is a tool for social networking. Criminals use these technologies for hate speech, child pornography and terrorism. Public authorities respond to these criminal activities with surveillance and censorship, thereby obfuscating the positive effects of ICTs on freedom of speech and other associated rights.[64]

With reference to 'Big Data' it has been said that-

> "Big Data" is shorthand for the combination of a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times. The process involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a technique for converting data flows into a particular, highly data-intensive type of knowledge. The technique of Big Data can be used to analyze data about the physical world — for example, climate or seismological data — or it can be used to analyze physical, transactional, and behavioral data about people. So used, it is vastly more nimble than old practices of category-driven profiling developed in the late twentieth century and now widely criticized. According to its enthusiasts, Big Data will usher in a new era of knowledge production and innovation, producing enormous benefits to science and business alike. According to its critics, Big Data is profiling on steroids, unthinkably intrusive and eerily omniscient.[65]

Technology can also be used to enhance privacy. For example, encryption can be used to prevent access without authorization. Digital Rights Management (DRM) technologies can be used to limit access to encrypted information, tracking and limit per use or per device. However, between privacy-invasive and privacy enhancing technologies, modern developments are pointed more towards privacy-intrusive technologies.[66]

The current level of technological development enables individuals to transact business online, establish relationships online, interact with others online, hold meetings online, and lead a life online. This makes the real relationships less and less important. People become a set of data which can be manipulated offline. Nowadays, businesses exploit personal data for commercial gain by profiling customers in order to improve the marketing of their products and retain their customer base. Governments have increasingly introduced 'intrusive electronic surveillance measures to gain information about their own population in the name of public and national

[64] European Parliament 'Information And Communication Technologies And Human Rights' EXPO/B/DROI/2009/24 /June/ 2010

[65] n11 (Cohen) 1921

[66] n---- (Dorraji & Barcs) p

security'.[67] The personal sphere automatically shrinks. The individual is seen only in terms of the information gathered about him. To some people, it is even difficult to imagine that this 'virtual' person exists in real life. Yet he does.[68]

A major challenge to our privacy has been brought about by technologies such as Internet use, smart phones, social networks, drones, biometric identification, CCTV, Satellites monitoring, growing automated surveillance and personal smart phones may track every movement of the individual. Radio Frequency Identification (RFID) systems, online purchases use of credit cards and computers in general are revolutionizing use of personal information.[69] The current threat to protection of privacy has been thus captured:[70]

> Nowadays the significant difference in monitoring is that we are not only being watched, but the information obtained about us is recorded, stored, and more and more aspects of our lives are recorded this way (e.g. security cameras, paying with credit cards, buying airplane tickets, etc.)

The question of encryption technology came up in 2016 in a matter where a telephone manufacturer turned down a request by government to open up an iPhone of one of their clients who had been involved in a gun battle.[71] Apple argued that it would be very dangerous to design software to unlock security features on a phone. This position was supported by United Nations High Commissioner for Human Rights in which it noted that 'encryption and anonymity are needed as enablers of both freedom of expression and opinion, and the right to privacy'.[72] This information can be manipulated.A number of artists, musicians, actors, actresses, singers, and celebrities post their profiles on SNWs with a view to gain exposure to their works and to promote their fame. In a matter involving such manipulation, a defendant was ordered to pay damages. There have been reports of names of popular persons being used in cyberspace for commercial exploitation, ridicule [73] and blackmail.[74] Profiles on such SNWs represent personal data which can be manipulated.

---

[67] n --- (Dorraji&Barcs) p 307

[68] DJ Solove *The Digital Person: Technology and Privacy in the Information Age* (New York and London, New York University Press, 2004)

[69] n --- (Dorraji&Barcs); M Zimmer 'Surveillance, Privacy and the Ethics of Vehicle Safety Communication technologies' 2005 at https://link.springer.com/article/10.1007/s10676-006-0016-0; J van Hoboken & FZ Borgesius 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' 6 (2015) *JIPITEC* 198

[70] L Lessig 'A privátszféraarchitektúrája' 2(2005) *InformációsTársadalom* p 56 cited in n1 p 261

[71] *Apple Inc. v the Federal Bureau of Investigations (FBI)*

[72] Office of the UN High Commissioner for Human Rights, "Apple-FBI case could have serious global ramifications for human rights" (4 March 2016) http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf (seen 12 Jan 2019)

[73] Stuff &Buz, 'Fake Celebrity Pages On Myspace', My Digital Life (2006), www.mydigitallife.info/2006/07/15/fake-celebrity-pages-on-myspace

[74] B Stone 'Keeping a True Identity Becomesa Battle Online' 17 June (2009) http://www.nytimes.com/2009/06/18/technology/internet/18name.html.

In another matter, the defendant had fraudulently accessed the accounts on Facebook and used the technique of 'Phishing' to lure users in logging in fake accounts through which he manipulated the account holders and their friends.[75]

Another aspect of (infringement of) privacy associated with technology is surveillance and interception of communications.[76] This aspect has attracted the attention of the ECtHR.[77]The US Supreme Court has stated that-[78]

> Short-term monitoring of a person's movements on public streets accords with expectations of privacy […] the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.

It has been recognised that the legal protection of privacy has certain limitations, firstly, where the individual has published the information or it has been published with his consent, and secondly, where there are countervailing reasons such as the need for the information to be broadcast.[79]

5. Use of GPS tracking and the right to privacy

Geospatial Positioning Satelite(GPS) is the information technology that is in use when one wishes to trace or monitor motor vehicles. A radio tracking system (LORAN) or Global Navigation systems was the one in use towards the end of the World War 2. Thus, vehicle tracking systems have traditionally been used in World War 2 specifically to trace ships and aircrafts.[80]

However, GPS was invented by the United States Department of Defense in 1973 after Russia launched Sputnick. The US Timation satellite used by the United States Military to determine accurate clocks in space (time) a technology heavily relied upon by the GPS system, and the Ground Based Omega Navigation which was a radio-based satellite navigation system. The system was first named Defense Navigation Satellite System then later as the NAVSTAR GPS. Later GPS was made available to all civilians via presidential decree on 1st May 2000.[81] GPS can be accessed by anyone who owns a GPS Receiver. [82] This marked the beginning of GPS commercialisation. [83]GPS history shows how the system required other sophisticated technologies to be invented to become more efficient and faster.

---

[75] *Facebook Inc v Wallace* [California Northern District Court, Case No: 5:2009cv00798] decided on 29 October 2009 (unreported) US

[76] CNT Falchetta'The Right to Privacy in the Digital Age' 9(2017)1*Journal of Human Rights Practice*, pp 104–118 at https://doi.org/10.1093/jhuman/huw026seen 18 Jan 2019

[77] *Re v The United KingdomApplication no. 62498 Judgment of 11* 27 October 2015, *Basic v Croatia* Application No 22251/13 Judgment of 25 October 2016, *Mustafa SezginTanrikulu v TurkeyApplication no. 27473 Judgment of 06*18/10/2017

[78] *United States v Jones*, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[79] DJ Glancy 'The Invention of the Right to Privacy' 21 (1979)1 *Arizona Law Review*36

[80] Encyclopedia Britannica, https://www.bbc.com/news/science-environment-29758872

[81] https://www.radio-electronics.com/info/satellite/gps/history-dates.php

[82] World War II Tech eLoran Deployed as GPS Backup in the UK, https://tech.slashdot.org/story/14/11/01/1332248/world-war-ii-tech-eloran-deployed-as-gps-backup-in-the-uk

[83] Fleetistics, How GPS Started, https://www.fleetistics.com/resources/gps-history-benefits/

The US Department of Transportation has come up with new laws that make it mandatory for car manufacturers to fit in VSV for new vehicles as well as standardize the format of message transmissions.[84]

GPS and Electronic Motor Vehicle Tracking is in use right now in Kenya and it aids owners and police to have an idea where the motor vehicle is located.[85] The Companies are able to track vehicles in real time which optimises transportation management but Electronic Tracking MV companies keep a database of information about the car, insurance, log book, physical location, the owner of the car, and real-time vehicle tracking data.[86] Most operate with a web-GIS application for vehicle tracking and create a server on the Windows Platform or Google Analytics database server. The servers have various responsibilities, some of the responsibilities are to receive data from the GPS tracking unit, storing it and servicing this information real time or on demand to the user.[87]

This system requires satellites, which transmit to a GPS Device. The GPS device is telecommunicably connected to the Internet which relays the information to a Tracking Database Webserver and Browser simultaneously.

Vehicle safety communication (VSC) technologies involve on-board safety applications which are able to communicate with the surroundings and warn a driver in real time of imminent danger. Both vehicles communicate with each other and the surrounding infrastructure. VSC are useful in traffic signal violation warning, curve speed warning, emergency electronic brake lights, pre-crash warning, lane change warning, and stop sign movement assistance. These technologies also enable information to be gathered about the motor vehicle registration, occupants in a car and whether they are male/female, and young/old. These technologies provide the possibility of surveillance of drivers thereby interfering with privacy.[88]A person's motor vehicle is very personal. It is basically his second home. A person spends a considerable time in his car. If a motor vehicle is tracked the tracker can see all the stops the person has undertaken, all his drop off points and one is able by looking at the trend of the data and see his frequented places. A tracker is able to decipher how long the person frequents certain places and where he visits.

[84] Federal Motor Vehicle Safety Standards
[85] Steve Mbogo, Daily Nation , Vehicle Tracking Systems Gains Popularity in Kenya, 22nd September 2009
[86] ibid
[87] ibid
[88] M Zimmer 'Surveillance, privacy and the ethics of vehicle safety communication technologies' 2005 at https://link.springer.com/article/10.1007/s10676-006-0016-0

The European Court of Human Rights was faced with the opportunity to deal with the issue of GPS Surveillance. In *Klass v Germany*[89] the Court first applied itself to the issue of wire tapping and surveillance. Seeking to implement interception of mail and post and telephone surveillance in the aftermath of the terrorist threats of the 1970's. The Court held that:

> Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the state must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. Therefore, the Court has to accept that the existence of some legislation granting powers of secret surveillance over the mail and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[90]

The Court also emphasised the need for safeguards against abuse and stated that after completion of the investigation the targeted party is to be notified of the surveillance without compromising the investigation. [91]

In *Weber & Saravia v Germany*[92]The Court gave parameters that are to be met by the Government when they seek to extend strategic monitoring. Firstly, that before enacting strategic monitoring there should be detailed safeguards from abuse. Secondly the monitoring should be restricted to short periods. Thirdly, immediate interruption of the measures when they no longer serve their purpose. Lastly they recommended the setting up of an independent superviserfor the monitoring.[93]

In *Uzun v Germany*[94]a GPS surveillance was built into a vehicle. The car was tracked for a long period of time and movements were tracked and later on disclosed to third parties. The Court again reiterated that the private life is a broad term not susceptible to exhaustive definition.[95]There is therefore a zone of interaction of a person with others even in a public context, which may fall within the scope of private life.[96]However the court also stated that the surveillance was authorised and thus not a violation of privacy because the action sought to achieve a legitimate aim. The GPS Surveillance had been employed after less intrusive actions had been employed and proved ineffective.[97]

In *Olmstead v United States*[98]the FBI had placed recording and monitoring devices outside a phone booth the defendant used. The defendant was involved in illegal gambling and opted to use a public phone booth instead of his private phone. Thus the place where this privacy was sought was

[89]*Klass v Germany*, Application No. 5029/71 ECtHR (1978)
[90] n-128 p 19
[91]Ibid p 9
[92]Weber and Saravia v Germany, ECHR (2006)
[93]ibid
[94]Uzun v Germany, ECHR (2010)
[95]Ibid, p 10
[96]Ibid, p 10
[97]Ibid,p 10
[98] Katz v United States, 347 SC(1967)

a public telephone booth and the defendant had closed the door indicating that he sought privacy. Further he had a reasonable expectation that his communication will be private and free from intrusions. The FBI relied on the recordings as evidence. The Supreme Court stated that the fourth amendment protects people, not places.

Similarly, in *United States v Moran*[99] the federal court was faced with the issue whether GPS tracking with visual surveillance amounted to a Fourth amendment search and whether it was permissible. It was held that it was permissible because Moran had no expectation of privacy in the whereabouts of his vehicle on a public roadway.

The Court of Appeal was faced with the issue of a case whereby the Police attached a GPS Surveillance Gadget by crawling under the body of the vehicle. The Court held that not only was this trespass but also an infringement on privacy. While in *People v Weaver*, [100]the Court of Appeals held that the attachment by police agents of a GPS tracking device to the underside of the defendant's vehicle and continuous monitoring of his movements over a period of sixty five days constituted a search for which they were required to obtain a search warrant to perform.[101]The majority noted that the GPS Technology could reveal and record trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment centre, the strip club, the criminal defence attorney, the by the hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. In summary the majority stated and mentioned types of personal information and actions one expects to be private yet the GPS Technology and vehicle car tracking technology will be able to pick up.

When the New York Supreme Court was faced with the question about conversations held in confidential situations the court held that eavesdropping should not be for a long period of time in this case it was two months. Once it surpasses two months it can be categorised as a search and seizure. The court stated that conversation believed by all of the parties to be confidential fall under the reasonable expectation of privacy.[102]

6. Interception of communication and secret surveillance

Wiretapping came into widespread use as an investigative tool in order to combat the use of the telephone by the criminal element in society as an efficient scientific aid to the planning, preparation, and commission of crime.[103]Wiretapping has been acknowledged as an effective tool for information collection and presentation of evidence.[104]

In the first case involving wiretapping, the US Supreme Court ruled that evidence obtained through wiretapping, even if it was done against the law, can be presented as evidence in the Supreme Court. The Court argued that wiretapping does not involve an illegal search and seizure as the wire tappers do not enter to the physical property.[105] In 1934 Congress enacted a law

[99]*United States v Moran* 261 U.S. 321 (1923)
[100]*People v Weaver* 909 N.E. 2d, NY (2009)
[101] n-103
[102]*Berger v New York* 388 U.S. 41 (1967)
[103] FC Sullivan 'Wiretapping and Eavesdropping: A Review of the Current Law' 18(1966)4 *Hastings Law Journal* 59, 60
[104] n1(Sullivan)
[105]*Olmstead v United States* 277 U.S. 438 (1928).

prohibiting the use of wiretapped information as evidence unless there was consent to carry out the recordings. After enactment of the statute, the Supreme Court rendered itself as follows-[106]

> the plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that "no person" shall divulge or publish the message or its substance to "any person." To recite the contents of the message in testimony before a court is to divulge the message.

In a subsequent case, the court extended the exclusion to cover any evidence obtained as a result of wiretapping.[107] The court further stated that only a participant in the intercepted conversation has locus to object to such wiretaps being produced in evidence.[108] Where one party to a conversation consents to or allows another party to listen to the conversation, the court held that there was no 'interception' and that such evidence was not illegal.[109] The challenge with this holding is that an 'informer' can allow police to listen in and such evidence can then be admitted. Courts have since held that it does not matter whether the conversation is recorded or overheard or even whether an extension is put in place for purposes of 'listening in'.[110] A major concern is whether the consent to listen into a conversation is voluntary. The court has said that where a person allows law enforcement officers to listen to a conversation in exchange for leniency, such evidence is admissible.[111]

The use of the pen register, without the consent of the subscriber has been held to be prohibited in as much as it involves communication, and it does not matter whether a call goes through or not.[112] A pen register is a device attached to the telephone exchange which records the number of calls made to a certain location.

In a matter in which government agents placed a listening device through the wall and onto a heating duct, something that enabled them to listen into the conversation, the court held that it was illegal.[113] This was based on physical intrusion. Where concealed microphones and recordings are used, the court has held that such use does not violate privacy as there is no intrusion. However, the minority in *Lopez* expressed the fear that allowing electronic eavesdropping would lead to a police state.[114]

In the matter of *Big Brother*, applicants brought a complaint against the defendants alleging that the defendants had put in place a scheme for intercepting and processing bulk data and for sharing data from a similar scheme with the US, in flagrant violation of their right under article 8(1)

[106] *Nardone v United States*, 302 U.S. 379 (1937) at 382
[107] *Nardone v United States*, 308 U.S. 338 (1939)
[108] *Goldstein v United States*, 316 U.S. 114 (1942).
[109] *Rathbun v United States* 355 U.S. 107 (1957).
[110] *Wilson v. United States*, 316 F.2d 212 (9th Cir. 1963), cert. denied, 377 U.S. 960 (1964); *United States v. Williams*, 311 F.2d 721 (7th Cir. 1963).; *Ferguson v. United States*, 307 F.2d 787 (10th Cir. 1962)
[111] *United States v Zarkin*, 250 F. Supp. 728 (D.D.C. 1966).
[112] *United States v Guglielmo*, 245 F. Supp. 534 (N.D. Ill. 1965)
[113] *Silverman v United States*, 365 U.S. 505 (1961); *Lopez v United States*(373 U.S. 427 (1963)) in which the agent with the recording device had it in his pocket and recorded in the presence of the defendant, it was held not to violate the law.
[114] n1*(Lopez)*

of the Convention. By a majority of five to two, the court held that due to the absence of sufficient safeguard mechanisms there was a violation of article 8(1).[115]

In the United Kingdom the Big Brother Phone hacking scandal revelation mentioned above dealt with mass phone hacking into voicemail of users and celebrities by media and journalists. The scandals led to the closure of a very successful Sunday Newspaper and the editors were prosecuted. However, Surveillance is now justified as a tool or weapon against organised crime, drug trafficking, paedophilia, money laundering terrorism which threaten public peace, public safety and National security. Chief Justice Lord Camden alluded to this when he stated that[116]

> No man can set his foot upon my ground without my license, but he is liable for an action, though damage be nothing…… if he admits the fact, he is bound to show by way of Justification that some positive law has empowered or excused him.

In *R v Khan*[117] Law enforcement employed listening devices to eavesdrop. Police recorded conversations between people suspected of criminal conduct. The court held that in determining whether evidence should be admitted, the illegality of the means used is not decisive. Thus law enforcement can rely on intercepted communications to conduct their investigations. However, in *Khan v UK*[118]this position was overturned because there was no statutory regulatory system.

Bugging devices in the United Kingdom is governed by the Police Act 1997 which provided no interference is unlawful if approved by Surveillance Commissioner under section 91 of the Act. Section 97 approval is also required where the information is likely to yield matters subject to legal privilege, confidential, personal information or confidential journalistic materialistic..[119]

In *Kinloch v HM Advocate*[120]It was argued that unauthorised surveillance breaches article 8 of the Convention and was therefore inadmissible. The Supreme Court held that it did not constitute a breach of Convention rights, on the ground that he had no reasonable expectation of privacy when he was followed in public spaces.

Malone v UK[121] 7 EHRR 14 emphasised that the surveillance practice breached article 8 of the ECHTR although article 8 (1) rights, if there was no prescribed by law.

The Court has also held that audio,[122] video,[123] and eavesdropping within prison cells[124] or holding pens a clear violation of privacy and thus a breach of Article 8 of the EU Human Rights Convention.[125]

In *Matheron v France*[126]the EU Human rights court was faced with the question whether a wiretapping in separate proceedings where the subject of redress was not a party could be relied

[115]*Big Brother Watch and Others v. The United Kingdom* Applications nos. 58170/13, 62322/14 and 24960/15 Decision of 13 September 2018 (Request for referral to the Grand Chamber pending)
[116]*Entick v Carrington* EWHC KB J98 [1765]
[117]*R v Khan* 2 S.C.R. 915, [2000]
[118]*Khan v UK* 31 EHRR 1016 (2001)
[119]Regulation of Investigatory Powers Act 2000, section 28 and 75
[120]*Kinloch v HM Advocate*, HC (83) (2012-13)
[121] (1985) 7 EHRR
[122]*Allan v UK* [2002] EHRR
[123]*Perry v UK* 63737/00 [2003] EHRR
[124]*P.G. and J.H. v U.K*. 44787/98 [2001] EHRR
[125]*Allan v UK* [2002] EHRR

upon against him. The court was categorical that this is a form of unauthorised action, stating that the data subject needs to exercise effective control.

7. Data protection in the EU -

The EU set up the Data Protection [127] Directive and e-Privacy Directive which was later amended and replaced by the Citizens Rights Directive [128] to help manage the challenge of technology. The EU generally requires that consent of the user be sought before traffic and location data can be used. Traffic data is here seen as the information or data processed in the course of an electronic transmission such as the date, time, address of the participants or the IP addresses used. The actual content may not be included. Location data refers to data indicating the location of a user at any one time. This can reveal visits to a hotel, hospital, market or the location of one's bed![129] Member states of the EU are required to handle such information confidentially.[130]

8. The Right to Privacy at the Workplace

Some countries have an elaborate legislation on the protection of privacy, including at the workplace.[131] It has been affirmed that an employee enjoys privacy rights at the workplace.[132] In this same environment, an employer is interested in safeguarding his property where the employee relies on the computer,[133] phone or iPad supplied by the employer. The employer's concern relates to misuse of the work equipment and or diversion of their use to private use, protection of trade secrets, protection of the employer's data in general and use of the employer's time on private matters.

Violation of privacy at the workplace has also come into focus. In one matter, applicants brought an action complaining that the employer had installed video surveillance cameras in the amphitheaters thereby interfering with their right to privacy under article 8(1) of the Convention.[134] The respondent argued that they needed the cameras to protect the property and the students inside the amphitheaters, and also to monitor the lectures. The court held that the respondents had no legitimate reason under article 8(2). The reason of monitoring lectures is not one of the reasons under article 8(2). Further the court found that the reason of security as advanced by the respondents was not necessary through installation of the video cameras inside the amphitheaters. It would have been sufficient to install them outside or at the entrances.

---

[126] *Matheron v France* 57752/00 [2005] EHRR

[127] Council Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (ISDN Directive).

[128] Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

[129] (n33 Hoboken????) J van Hoboken & FZ Borgesius 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' 6 (2015) *JIPITEC* 198 [18]-[19]

[130] Ibid (n--- van Hoboken) [22]

[131] For instance *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 lay out the principles for monitoring of data of individuals.

[132] *Stengart v Loving Care Agency Inc* 817 F Supp 2d 1090 (S.D. Ind. 2011) in which the court held that communication between an employee and her attorney using the employers computer was privileged.

[133] *Falmouth Firefighters Union v Town of Falmouth* G2-11-314- here the court stated that the plaintiff had no reasonable expectation of privacy having sent emails using the employer's computer.

[134] n--- (Antovic)

In another matter, the applicant brought this action complaining that her right to privacy had been infringed by the covert surveillance by way of video cameras by the employer.[135] The employer had suspected two of her employees to have stolen. A video camera was installed for two weeks and this covered the area where drinks and the cash box were. The respondents argued that they needed to be sure to what they should attribute the losses, that they used the video for a limited period, that the surveillance covered only the affected area, and that the data collected was analysed by one person only. The court observed that video surveillance generally infringed the right to privacy. However, it was further observed that the employer had tried well to balance between a right to protect property and the private rights.

In *Barbulescu*, the applicant brought a complaint stating that his right to privacy and non-interference with his communication under article 8(1) had been breached. The applicant was employed in a private company where the employer gave instructions requiring all employees not to use official computers for private communication. The Applicant set up a Yahoo Messenger for real time communication with clients. He also had another one. The employer monitored his correspondences and dismissed him for violating company rules. The ECtHR held that the notion of privacy applied at the workplace as well and covered communications carried out during working hours, and that the employer cannot shrink an employee's private sphere at work. The court found for the applicant.[136]

In order to balance these competing interests, certain principles have been worked out.[137] Accordingly, an employer can monitor an employees activities only during working hours, there must be a legitimate reason for so doing, the purpose for the monitoring should not go beyond the employer's stated legitimate reason, and the employer needs to either seek consent of the employee or warn the employee that monitoring of his/her activities is likely to take place. Such monitoring extents to motor vehicles supplied by the employer. The employee is equally concerned about the possible misuse of data held by the employer.

9. Kenya's position on the use of electronic data

The Constitution of Kenya provides for the right to privacy in the following words:

> 31. Privacy
>
> 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.

Curiously, although this right is similar to that contained in the European Convention of Human Rights, the limitation to this right contained in the European Convention of Human Rights is missing here. However, reading this right together with article 25 of the said Constitution reveals that the right to privacy is not absolute.

[135] *Karin KÖPKE v Germany* Application no. 420/07-V

[136] *Barbulescu v. Romania* Application no. 61496/08 Judgement of 5 September 2017 (GC)

[137] *Barbulescu v Romania* Application no. 61496/08 ECtHR

Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR

70. Today many citizens live major portions of their lives online. Citizens use the computers and cell phones to conduct businesses, to communicate, impart ideas, conduct research, explore their sexuality, seek medical advice and treatment, correspond with lawyers, communicate with loved ones and express political and personal views. Citizens also use the internet to conduct many of their daily activities, such as keeping records, arranging travel and conducting financial transactions. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into the citizens personal and professional lives. They have replaced and consolidated fixed-line telephones, filing cabinets, wallets, private diaries, photo albums and address books.

74. A persons' right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her own personal affairs relatively free from unwanted intrusions. Information protection is an aspect of safeguarding a person's right to privacy. It provides for the legal protection of a person in instances where such a person's personal particulars are being processed by another person or institution. Processing of information generally refers to the collecting, storing, using and communicating of information.

77. Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual. The right of privacy is a fundamental right. It protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices.

83. Limitation of a constitutional right will be constitutionally permissible if (i) it is designated for a proper purpose; (ii) the measures undertaken to effectuate such a limitation are rationally connected to the fulfilment of that purpose; (iii) the measures undertaken are necessary in that there are no alternative measures that may similarly achieve that same purpose with a lesser degree of limitation; and finally (iv) there needs to be a proper relation ("proportionality strictosensu" or "balancing") between the importance of achieving the proper purpose and the special importance of preventing the limitation on the constitutional right.'

Samura Engineering Limited & 10 Others vs. Kenya Revenue Authority [2012] eKLR where it was held that:

> "The right to privacy enshrined in our Constitution includes the right to not to have one's person or home searched, one's property searched or possessions seized. Since searches infringe the right to privacy, they must be conducted in terms of legislation which must comply with the provisions of Article 24. It has been said that the existence of safeguards to regulate the way in which state officials enter the private domains of ordinary citizens is one of the features that distinguish a democracy from a police state."

102. I also agree with the position in Kennedy vs. Ireland [1987] IR 587 as cited in Coalition for Reform and Democracy (CORD) & 2 Others vs. Republic & 10 Others [205] KLR where it was held that:

> "The dignity and freedom of an individual in a democratic society cannot be ensured if his communication of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."

103. In this respect the Petitioner relied on Coalition for Reform and Democracy (CORD) & 2 Others vs. Republic of Kenya & 10 Others [2015] eKLR where it was held that:

> "285 The right to privacy is guaranteed under Article 31 of the Constitution which provides as follows:
>
> *Every person has the right to privacy, which includes the right not to have –*
>
> *(a) Their person, house 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.*
>
> 286. The right to privacy has also been expressly acknowledged in international and regional covenants on fundamental rights and freedoms. It is provided for under Article 12 of the UDHR, Article 17 of the ICCPR, Article 8 of the European Convention on Human Rights (ECHR) and Article 14 of the African Charter on Human and Peoples' Rights.

287. B. Rossler in his book, *The Value of Privacy (Polity, 2005) p. 72*, explains the right to privacy as follows:

The concept of right to privacy demarcates for the individual realms or dimensions that he needs in order to be able to enjoy individual freedom exacted and legally safeguarded in modern societies. Such realms or dimensions of privacy substantialize the liberties that are secured because the mere securing of freedom does not in itself necessarily entail that the conditions are secured for us to be able to enjoy these liberties as we really want to.

288. As to whether there is need to protect privacy, he goes on to write that:

Protecting privacy is necessary if an individual is to lead an autonomous, independent life, enjoy mental happiness, develop a variety of diverse interpersonal relationships, formulate unique ideas, opinions, beliefs and ways of living and participate in a democratic, pluralistic society. The importance of privacy to the individual and society certainly justifies the conclusion that it is a fundamental social value, and should be vigorously protected in law. Each intrusion upon private life is demeaning not only to the dignity and spirit of the individual, but also to the integrity of the society of which the individual is part.

289. The New Zealand Supreme Court in Brooker vs the Police (2007) NZSC 30 at para. 252 stated as follows:

"Privacy can be more or less extensive, involving a broad range of matters bearing on an individual's personal life. It creates a zone embodying a basic respect for persons...Recognising and asserting this personal and private domain is essential to sustain a civil and civilised society...It is closely allied to the fundamental value underlying and supporting all other rights, the dignity and worth of the human person."

290. Applying the normative content of the right to privacy as stated above and what that right seeks to protect, we are clear in our mind that surveillance in terms of intercepting communication impacts upon the privacy of a person by leaving the individual open to the threat of constant exposure. This infringes on the privacy of the person by allowing others to intrude on his or her personal space and exposing his private zone. In the Irish Supreme Court case of Kennedy vs Ireland (1987) I.R 587 it was held that the phone-tapping of the two journalists in question violated their right to privacy. Hamilton J made it clear that the right to privacy must ensure the preservation of the dignity and freedom of the individual in a sovereign, independent and democratic society. In his view:

"The dignity and freedom of an individual in a democratic society cannot be ensured if his communication of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."

104. As regards the declaration of unconstitutionality of sections 44(1) and (2) and 60(1) and (3) of the *Tax Procedures Act, 2015*, reliance was placed on Kennedy vs. Ireland [1987] IR 587 as cited in Coalition for Reform and Democracy (CORD) & 2 Others vs. Republic & 10 Others [205] KLR where it was held that:

> "The dignity and freedom of an individual in a democratic society cannot be ensured if his communication of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."

105. I agree that the right to privacy is tied to the inherent right to dignity of a person and that indeed it is prerequisite right that must be accorded for one to be able to enjoy every other right or freedom deserving of any citizen of a democratic state. In Coalition for Reform and Democracy (CORD) & 2 Others vs. Republic of Kenya & 10 Others [2015] eKLR it was held that:

> "285 The right to privacy is guaranteed under Article 31 of the Constitution which provides as follows:
>
> *Every person has the right to privacy, which includes the right not to have –*
>
> *(a) Their person, house 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.*
>
> 286. The right to privacy has also been expressly acknowledged in international and regional covenants on fundamental rights and freedoms. It is provided for under Article 12 of the UDHR, Article 17 of the ICCPR, Article 8 of the European Convention on Human Rights (ECHR) and Article 14 of the African Charter on Human and Peoples' Rights.
>
> 287. B. Rossler in his book, *The Value of Privacy (Polity, 2005) p. 72*, explains the right to privacy as follows:
>
> "The concept of right to privacy demarcates for the individual realms or dimensions that he needs in order to be able to enjoy individual freedom exacted and legally safeguarded in modern societies. Such realms or dimensions of privacy substantialize the liberties that are secured because the mere securing of freedom does not in itself necessarily entail that the conditions are secured for us to be able to enjoy these liberties as we really want to".

288. As to whether there is need to protect privacy, he goes on to write that:

"Protecting privacy is necessary if an individual is to lead an autonomous, independent life, enjoy mental happiness, develop a variety of diverse interpersonal relationships, formulate unique ideas, opinions, beliefs and ways of living and participate in a democratic, pluralistic society. The importance of privacy to the individual and society certainly justifies the conclusion that it is a fundamental social value, and should be vigorously protected in law. Each intrusion upon private life is demeaning not only to the dignity and spirit of the individual, but also to the integrity of the society of which the individual is part".

289. The New Zealand Supreme Court in Brooker vs the Police (2007) NZSC 30 at para. 252 stated as follows:

"Privacy can be more or less extensive, involving a broad range of matters bearing on an individual's personal life. It creates a zone embodying a basic respect for persons...Recognising and asserting this personal and private domain is essential to sustain a civil and civilised society...It is closely allied to the fundamental value underlying and supporting all other rights, the dignity and worth of the human person."

290. Applying the normative content of the right to privacy as stated above and what that right seeks to protect, we are clear in our mind that surveillance in terms of intercepting communication impacts upon the privacy of a person by leaving the individual open to the threat of constant exposure. This infringes on the privacy of the person by allowing others to intrude on his or her personal space and exposing his private zone. In the Irish Supreme Court case of Kennedy vs Ireland (1987) I.R 587 it was held that the phone-tapping of the two journalists in question violated their right to privacy. Hamilton J made it clear that the right to privacy must ensure the preservation of the dignity and freedom of the individual in a sovereign, independent and democratic society. In his view:

"The dignity and freedom of an individual in a democratic society cannot be ensured if his communication of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."

106. Brooker vs. The Police [2007] NZSC 30 at para 252 holds that:

"Privacy can be more or less extensive, involving a broad range of matters bearing on an individual's personal life. It creates a zone embodying a basic respect for persons…Recognising and asserting this personal and private domain is essential to sustain a civil and civilised society…It is closely allied to the fundamental value underlying and supporting all other rights, the dignity and worth of the human person."

> *59. Communications data is the digital equivalent of having a private investigator trailing a targeted individual at all times, recording where they go and with whom they speak. Communications data will reveal web browsing activities, which might reveal medical conditions, religious viewpoints or political affiliations. Items purchased, new sites visited, forums joined, books read, movies watched and games played – each of these pieces of communications data gives an insight into a person. Mobile phones continuously generate communications data as they stay in contact with the mobile network, producing a constant record of the location of the phone (and therefore its user). Communications data produces an intrusive, deep and comprehensive view into a person's private life, revealing his or her identity, relationships, interests, location and activities.*[138]

In a matter in which a corporate body secretly took a picture of a person and used it for commercial purposes, it was held that use of a person's photograph without the person's consent is an invasion of the person's privacy [139] contrary to the provisions of article 31.[140] The petitioner complained that a communications regulator had placed generic device management system (DMS) for spying on mobile and communication devices without public consultations and or public participation albeit through awareness creation. The respondent argued that the DMS was necessary to help identify stolen and counterfeit mobile sets with a view to switching them off. The Court held that the use of DMS was an intrusion in the privacy of individuals.[141]

In a suit in which the petitioner's nude photograph was leaked by her boyfriend after a breakup to organisers of a beauty pageant leading to her dethronement, she argued that leakage of her private photographs was an infringement of her right to privacy. The court found for her.[142]

In another matter, Police went to the workplace of the petitioner searched and took away books and his mobile phone. The petitioner allowed the police entry and gave them the items they wanted. He alleged that his right to privacy had been infringed. The court held that consent given to the police served as a waiver to the right to privacy.[143]

The Constitution also has some provision on the right to access information held by the state and by private actors.[144] Equally, this right is not absolute. The manner of operationalization of art 35 has been capture in a statute.[145]

---

[138] *10 Human Rights Organizations -vs- The United Kingdom*, APP. NO. 24960/15 [ECtHR]

[139] *Kumena v KTDA Agency Ltd* [2019] eKLR (HCt)

[140] Constitution of Kenya, 2010

[141] *Kenya Human Rights Commission v Communications Authority of Kenya* [2018] eKLR (HCt),
See also *Okoiti v Communication Authority of Kenya* [2018] eKLR (HCt)

[142] *Ebrahim v Ashleys Kenya Limited [2016] eKLR (HCt)*

[143] *Mutinda v Inspector General National Police Service [2014] eKLR (HCt)*

[144] Art 35 Constitution of Kenya, 2010

[145] Access to Information Act, Act No 31 of 2016(Laws of Kenya)

The Access to Information Act [146] defines 'electronic record' to include information generated, transmissible and stored in electronic form. Information is defined to include all records held by a public or private body. These definitions perfectly circumscribe information that can be collected from and about individuals whether in analog or electronic form.The objects of the Act include to provide a framework for disclosure of information held by the state or a private entity and to protect those who disclose such information. This law is silent on protection of privacy in its objects clause. Section five of the Act obligates all public and private persons to provide information sought by any person. Section six sets out circumstances that amount to limitations of access to information. One of them is 'unwarranted invasion of the privacy of an individual'.[147] However, the limitations can be ignored where there a court determines that the public interest in the disclosure by far outweighs any interest sought to be protected.[148]This statute places greater premium on disclosure of information than on protection of privacy.

Under Kenyan law, it is an offence for a person to unlawfully intercept communication and or to disclose the contents thereof.[149] The law also recognizes retention of electronic records and electronic information for future use.[150]

The National Integrated Identity Management System (NIIMS) has authority to collect and store data of persons using biometric data of fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form; and also based on global positioning system (GPS).[151]Under this law, officials are under an obligation to maintain confidentially unless they are requested to disclose the information under a written law.[152]

10. Protection of Privacy and possible defences

Public interest

The court, in *Hosking*, stated the tort of privacy to comprise of firstly, the existence of facts in respect of which there is a reasonable expectation of privacy, and secondly, publicity given to those facts would be considered highly offensive to a reasonable person.[153] The harm to be protected against is humiliation and personal distress. Unlike in the tort of defamation, injury and economic loss are not necessary. The remedy is damages. Injunctive relief may also be available to prevent the publicising of such information. However, the court was also quick to add that any limits imposed on free speech by such a privacy tort should not exceed those justified in a free and democratic society. A defendant therefore can rely on the defence of public interest.

[146] Ibid s 2
[147] s6(1)(d) of Access to Information Act No 31 of 2016
[148] Ibid s 6(4)
[149]Kenya Information & Communications Act (Cap 411A) revised 2012,ss 31 & 32
[150]Ibid, ss 83H & 83I
[151]s 9A The Registration of Persons Act (Cap 107) Laws of Kenya (s 9A is an amendment that commenced on 18 Jan 2019)
[152]Indeed under section 5 of the Access to Information Act, officials are under an obligation to obey the right to access to information under article 35 of the Constitution of Kenya.
[153]*Hosking v Runting* [2005] 1 *NZLR* 1

Protection of Confidentiality

Generally speaking, recipients of personal information have a statutory obligation to keep the information confidential. In some countries breach of confidentiality is sanctioned with the pain of a jail term. Information stored on SNWs is usually shared between the person's contacts and the service provider. Disclosure to friends and relatives has been held not to erode confidentiality in such information.[154] It is, however, difficult to require that all contacts keep one's information confidential. A better view is the suggestion for the development of a standalone tort of 'invasion of privacy' as is the case in New Zealand.[155] This has been confirmed.[156]

Copyright in confidential material

This could be useful in cases where a person has posted certain original material for use by a limited number of people. However, personal photographs and other personal information may not meet the requirements for copy right ability.[157] A certain level of copyright protection has been achieved through the possibility of selling materials deposited on the internet. However, such protection cannot cover personal information on SNWs.

Personality merchandising and false endorsement

This form of protection can be available in a case where the complainant has a reputation or fame and where the intended use of his photograph is trade related.[158] Where a person uploads another's photo to use for endorsement of some merchandise, courts have held in such cases that the right to privacy has been infringed.[159] This form of protection is not possible in cases of defamation.

The link between defamation and right to privacy has been captured thus - [160]

> […] the law of defamation […] is also geared to uphold the human being's right to human dignity by placing controls on the freedom of speech and expression. The press should not seek under the cover of exercising its freedom of speech and expression, make unwarranted intrusions into the private domain of individuals and thereby destroy their right to privacy. Public figures are no exception. Even a public figure is entitled to a reasonable measure of privacy. Therefore, Her Excellency the President even though she is a public figure is entitled to a reasonable measure of privacy to be left alone when she is not engaged in the performance of any public functions. That is a no entry zone which the press must not trespass.

---

[154] *Prince Albert v Strange* (1849) 2 DeG&Sm 652; 64 ER 293 (UK) (Knight Bruce LJ)

[155] BK Murphy 'Developments in the Law of Invasion of Privacy in New Zealand and England', *Auckland U.L. Rev* 9 (2000-2003): 1031 at p.1042; J Hartley 'Tort of Breach of Privacy in New Zealand', *Auckland U.L. Rev* 9 (2000-2003): 267; *L v G* [2002] DCR 234 (NZ); *P v D* [2000] 2 NZLR 591 (NZ)

[156] *Hosking v Runting* [2005] 1 NZLR 1

[157] BK Murphy----

[158] A Marsoof ---

[159] *Irvine v Talksport*[2002] 1 WLR. 2355 (UK), *Healan Laboratories v Topps Chewing Gum* 202 F. 2d 866 (2nd Cir, 1953) (US)

[160] *Sinha Rathnathunge v The State* [2001] 2 Sri LR 172 (SL)per Hector Yapa J at 213

> The case in hand is one where the press has attempted to enter into that no entry zone.

Legitimate aim

This defence is contained in article 8(2) of ECHR and in numerous national legislations. In a matter in which an applicant complained that the search conducted on her home and seizure of her property violated her rights under article 8 (1) on privacy of the home, the court found that the search and seizure were carried out pursuant to criminal proceedings and therefore that the state had a legitimate aim – the prevention of crime under article 8(2).[161]

In another matter in which the applicant complained of violation of security to her person in which she was detained for four days for failing to pay a fine, the Commission held that she was legitimately held following a lawful order.[162]

Exhaustion of internal remedies

The ECmHR has held that where an applicant has not exhausted internal remedies in accordance with general principles of international law his complaint cannot be admitted.[163]In Kenya, this principle is captured in a statute.[164] It can thus form a formidable defence.

11. Conclusion

Some people postulate and predict the death of privacy in the face of technological development.[165]Indeed, the concept of privacy has been severely modified by the emergence of ICTs. It is gratifying to note that most countries are ready to respect the right to privacy. Nevertheless, citizens must be constantly vigilant to protect intrusion of privacy at all costs. The use of technology places individuals in an awkward position where they volunteer intimate and confidential information to WSPs or even on work computers. Nevertheless, governments should not be left to use such data to infringe upon an individual's right without justifiable reasons.

[161] n---- (*Cacuci*)

[162]*Johanna AIREY v Ireland* Application No 6289/73 Decision of 7 July 1977 on the admissibility of the application (ECmHR)

[163]*Gottfried NIEMIETZ v Federal Republic of Germany* Application No. 13710/885 April 1990 (ECmHR)

[164]Fair Administrative Action Act 2 9

[165] n ---- (Bloem ----)

References

A v France App no 14838/89 (ECHR, 23 November 1993)

Access to Information Act, Act No 31 of 2016 (Laws of Kenya)

Allan v UK [2002] ECtHR

Antovic and Mirkovic v Montenegro Application no. 70838/13 -II *Final* Judgment 28/02/2018 ECtHR

Apple Inc. v the Federal Bureau of Investigations (FBI)

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, § 75, 28 June 2007 (ECtHR)

Bărbulescu v Romania [GC], no. 61496/08, § 70, ECtHR 2017 (extracts)

Barbulescu v. Romania Application no. 61496/08 Judgement of 5 September 2017 (GC)-ECtHR

Basic v Croatia Application No 22251/13 Judgment of 25 October 2016 (ECtHR)

Beloff v Presdram [1973] F.S.R. 33 at p.57

Berger v New York, 388 U.S. 41 (1967)

Big Brother Watch and Others v. The United Kingdom Applications nos. 58170/13, 62322/14 and 24960/15 Decision of 13 September 2018 (Request for referral to the Grand Chamber pending)

J Bloem, M Doorn, S Duivestein, T Manen, and E Ommeren 'Privacy, Technology and the Law: Big Data for Everyone through Good Design' VINT Research Report 3 The Sogeti Trend Lab VINT, 2013 [interactive]. At <http://blog.vint.sogeti.com/ wp-content/uploads/2013/04/VINT-BigData-Research-Privacy-Technology-and-theLaw.pdf>.[accessed on 25 Jan 2019].

BE Bratman 'Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy' 69 (2002) *Tennessee Law Review* p 344.

J Brooks Telephone: The First Hundred Years *Passim* 1976

Burghartz v Switzerland judgment on 22 February 1994, no. 16213/90 [ECtHR]

Cacuci and SC Virra & Cont Pad SRL v Romania Application no. 27153/07-IV judgment of 13 November 2018 (ECtHR)

U Cheer "The future of privacy. Recent legal developments in New Zealand" (2007) 13 *Canterbury Law Review* 169 at https://ir.canterbury.ac.nz/bitstream/handle/10092/3254/12606673_Cheer_Privacy.pdf?sequence=1

Codarcea v. Romania, no. 31675/04, §§ 102-104, 2 June 2009 [ECtHR]

JE Cohen 'What Privacy is for' 126 (2013) *Harvard Law Review* 1904;

Constitution of Kenya, 2010

Copland v United Kingdom App No 62617/00 (ECtHR, 3 April 2007)

Costello-Roberts v United Kingdom App no 13134/87 (ECtHR, 25 March 1993)

Couderc and Hachette Filipacchi Associésv France [GC], no. 40454/07, § 83, ECtHR 2015 (extracts)

1950 Council of Europe European Convention of Human Rights (Article 8)

1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

Council Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (ISDN Directive).

Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

J Damen, L Köhler & S Woodard 'The Human Right of Privacy in the Digital Age' *Staat, Recht und Politik* — Forschungs- und Diskussionspapiere 3, 2017

Data Protection Act 1984, http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf

Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

Davis v Secretary of State for the Home Office [2015] EWHC 2092 (Admin).

Digital Rights Ireland v Minister for Communications, Marine and Natural Resource (Joined Cases C-293/12 and C594/12) [2014] 3 WLR 1607

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data

SE Dorraji& M Barcys 'Privacy in Digital Age: Dead Or Alive?! Regarding the New EU Data Protection Regulations' 4(2014)2 *Social Technologies* p 306–317

Dudgeon v United Kingdom App no 7525/76 (ECtHR, 22 October 1981).

Ebrahim v Ashleys Kenya Limited [2016] eKLR (HCt)

Encyclopedia Britannica, https://www.bbc.com/news/science-environment-29758872

Entick v Carrington EWHC KB J98 [1765]

Ettore v. PhilcoTelev. Broad. Corp., 229 F.2d 48 1, 485 (3d Cir. 1956)

2000 European Union Charter of Fundamental Rights (Article 7)

European Parliament 'Information And Communication Technologies And Human Rights' EXPO/B/DROI/2009/24 /June/ 2010

Facebook at http://www.Facebook.com/press/info.php?statistics (accessed-25.08.2010);

Facebook Inc v Wallace [California Northern District Court, Case No: 5:2009cv00798] decided on 29 October 2009 (unreported) US

Fair Administrative Action Act

Falmouth Firefighters Union v Town of Falmouth G2-11-314-

CNT Falchetta 'The Right to Privacy in the Digital Age' 9(2017)1 *Journal of Human Rights Practice*, pp 104–118 at https://doi.org/10.1093/jhuman/huw026 seen 18 Jan 2019

Fleetistics, How GPS Started, https://www.fleetistics.com/resources/gps-history-benefits/

Ferguson v. United States, 307 F.2d 787 (10th Cir. 1962)

Gaskin v the United Kingdom judgment of 07 July 1989, no. 10454/83 [ECtHR]

General Data Protection Regulation 2018, https://gdpr-info.eu/art-4-gdpr/

DJ Glancy 'The Invention of the Right to Privacy' 21 (1979)1 *Arizona Law Review* 36

Goldstein v United States, 316 U.S. 114 (1942).

https://www.radio-electronics.com/info/satellite/gps/history-dates.php

Gottfried NIEMIETZ v Federal Republic of Germany Application No. 13710/885 April 1990 (ECmHR)

Guillot v France judgment on 24 October 1993, no. 22500/93 [ECtHR]
Halford v United Kingdom (1997) 24 [ECtHR] 523
Halford v the United Kingdom judgment on 25 June 1997, no. 20605/92 Decisions 1997-III (ECtHR)
J Hartley 'Tort of Breach of Privacy in New Zealand' *Auckland U.L. Rev* 9 (2000-2003): 267
Healan Laboratories v Topps Chewing Gum 202 F. 2d 866 (2nd Cir, 1953) (US)
Heglas v. the Czech Republic, no. 5935/02, § 74, 1 March 2007
WJ Hoese 'Electronic Eavesdropping: A New Approach' 52(1964)1 *California Law Review* 142;
Hosking v Runting [2005] 1 *NZLR* 1
Huvig v France judgment on 24 April 1990, no. 11105/84 [ECtHR]
Irvine v Talksport [2002] 1 WLR. 2355 (UK)
Johanna AIREY v Ireland Application No 6289/73 Decision of 7 July 1977 on the admissibility of the application (ECmHR)
A Johns 'The Right to Privacy in the Digital Age: Recent Developments and Challenges' STEP Caribbean Conference St. Lucia April 25–27, 2016
Karin KÖPKE v Germany Application no. 420/07-V [ECtHR]
Katz v United States, 347 SC(1967)
Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010 [ECtHR]
Kenya Human Rights Commission v Communications Authority of Kenya [2018] eKLR (HCt),
Kenya Information & Communications Act (Cap 411A) revised 2012, ss 31 & 32
Khan v UK, 31 1016 (2001) ECtHR
Kinloch v HM Advocate, HC (83) (2012-13)
Klass and Others v Germany judgment on 6 September 1978, no. 5029/71 (1978) ECtHR
MR Konvitz 'Privacy and the Law: a Philosophical Prelude' 31(1966)2 *Law and Contemporary Problems* 272.
Kruslin v France judgment on 24 April 1990, no. 11801/85 [ECtHR]
Kumena v KTDA Agency Ltd [2019] eKLR (HCt)
L v G [2002] DCR 234 (NZ)
Leander v Sweden judgment of 26 March 1987, no. 9248/81 [ECtHR]
Leander v Sweden Series A No. 116 (26 March 1987) ECtHR
Liberty v UK App no 58243/00 (ECHR, 1 July 2008) ECtHR
López Ostra v Spain judgment on 09 December 1994, no.16798/90 [ECtHR]
Lopez v United States (373 U.S. 427 (1963))
A Lukács 'What is Privacy? The History and Definition of Privacy' at http://u-szeged.academia.edu/AdriennLukacs or http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (seen 27 Jan 2019)
Malone v the United Kingdom judgment on 2 August 1984, no. 8691/79 [ECtHR]
Marcel v Metropolitan Police Commissioner 225-240 Ch [1992]
A Marsoof 'Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression' *International Journal of Law and Information Technology*19(2):110-132 May 2011 DOI: 10.1093/ijlit/eaq018
Matheron v France 57752/00 [2005] ECtHR
M.C. v. Bulgaria,no. 39272/98, § 150, ECHR 2003-XII § 150 [ECtHR]

MK v France App no 19522/09 (18 April 2013) ECtHR
Millar v Taylor 4 Burr 2303 2379 (1769)
BK Murphy 'Developments in the Law of Invasion of Privacy in New Zealand and England *Auckland U.L. Rev* 9 (2000-2003): 1031 at 1042
Murray v United Kingdom Series A No. 300-A (28 October 1994) ECtHR
Mustafa SezginTanrikulu v Turkey Application no. 27473 Judgment of 0618/10/2017 [ECtHR]
Mutinda v Inspector General National Police Service [2014] eKLR (HCt)
Nardone v United States, 302 U.S. 379 (1937)
Nardone v United States, 308 U.S. 338 (1939)
KG Ndossy' Mobile Cellular Communication and its Effect on Personal Data
Newbold v Commissioner of Police (2014) 84 WIR 8; [2014] UKPC 12.
Niemietz v Germany judgment on 16 December 1992, no. 13710/88 [ECtHR]
Office of the UN High Commissioner for Human Rights, "Apple-FBI case could have serious global ramifications for human rights" (4 March 2016) http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf (seen 12 Jan 2019)
Okoiti v Communication Authority of Kenya [2018] eKLR (HCt)
Olmstead v United States 277 U.S. 438 (1928).
Olmstead v United States 277 U.S. 438 (1928).
P v D [2000] 2 NZLR 591 (NZ)
Paul v. Davis, 424 U.S. 693, 7 13 (1976)
People v Weaver, 909 N.E. 2d, NY (2009)
Perry v UK 63737/00 [2003] ECHR
P.G. and J.H. v U.K. 44787/98 [2001] ECHR
R Posner 'The Right of Privacy' 12 *Georgia Law Review* 409
Prince Albert v Strange (1849) 2 DeG & Sm 652; 64 ER 293 (UK)
Protection in Tanzania-Practical and Legal Analysis under Tanzanian Law' A Thesis submitted in partial fulfilment of the requirements for the award of the Degree of Master of Laws (Information and Communication Technology Laws) of the University of Oslo, 2014
R v Brown [1996] 1 All ER 545
R v Khan, 2 S.C.R. 915, [2000]
Rathbun v United States 355 U.S. 107 (1957).
Re v The United Kingdom Application no. 62498 Judgment of 11 27 October 2015
The Registration of Persons Act (Cap 107) Laws of Kenya (s 9A is an amendment that commenced on 18 Jan 2019)
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)
Regulation of Investigatory Powers Act 2000, section 28 and 75
Roach v Harper 143 W. Va 869, 105 S.E. 2d 564 (1958)
Roman Zakharovv. Russia [GC], no. 47143/06, § 171, ECtHR 2015
Rotaru v. Romania [GC], no. 28341/95, § 52, ECtHR 2000-V

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [GC], no. 931/13, § 130, ECtHR 2017 (extracts)

Schrems v Data Protection Commissioner Case No C-362/14 decided 6 October 2015 (CJEU)

Shimovolos v Russia App no 30194/09 (ECtHR, 21 June 2011).

Smirnova v Russia,nos. 46133/99 and 48183/99, § 95, ECtHR 2003-IX (extracts)

Sidabras and Džiautas v Lithuania, nos. 55480/00 and 59330/00, § 43, ECtHR 2004-VIII

Silverman v United States, 365 U.S. 505 (1961)

Sinha Rathnathunge v The State [2001] 2 Sri LR 172 (SL) per Hector Yapa J at 213

Stengart v Loving Care Agency Inc 817 F Supp 2d 1090 (S.D. Ind. 2011)

DJ Solove *Nothing to Hide: the False Tradeoff between Privacy and Security* (New Haven & London: Yale University Press, 2011) p 4.

DJ Solove *The Digital Person: Technology and Privacy in the Information Age* (New York and London, New York University Press, 2004)

Steve Mbogo 'Vehicle Tracking Systems Gains Popularity in Kenya', *Daily Nation* ,22nd September 2009

B Stone 'Keeping a True Identity Becomes a Battle Online' 17 June (2009) http://www.nytimes.com/2009/06/18/technology/internet/18name.html.

Stuff &Buz 'Fake Celebrity Pages On MySpace', My Digital Life (2006), www.mydigitallife.info/2006/07/15/fake-celebrity-pages-on-myspace

FC Sullivan 'Wiretapping and Eavesdropping: A Review of the Current Law' 18(1966)4 *Hastings Law Journal* 59, 60

Sunshine Act of 1976, Freedom of Information Act 1966

Twitter at http://themetricsystem.rjmetrics.com/2010/01/26/new-data-on-twitters-users-and-engagement/

J Waldo, HSL Lin, LI Milett (eds.) *Engaging Privacy and Information Technology in a Digital Age* (Washington National Academies Press 2007)

SD Warren & LD Brandeis 'The Right to Privacy' 4(1890)5 *Harvard Law Review* p 193, SD Warren & LD Brandeis 'The Right To Be Let Alone' 67 (1891) *Atlantic Monthly* 428-29

The 1948 United Nations Universal Declaration of Human Rights (Article 12)

The 1966 United Nations International Covenant on Civil and Political Rights (Article 17)

United States v Jones, 565 U.S., 132 S. Ct. 945, 964 (2012)

United States v Guglielmo, 245 F. Supp. 534 (N.D. Ill. 1965)

United States v Moran, 261 U.S. 321 (1923)

United States v. Williams, 311 F.2d 721 (7th Cir. 1963)

United States v Zarkin, 250 F. Supp. 728 (D.D.C. 1966).

Uzun v Germany, ECHR (2010)

Vodafone Group Plc (UK) 'Freedom of Expression and Network Censorship, Digital Rights and Freedoms, at https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_freedom_expression_network_censorship.pdf

J van Hoboken & FZ Borgesius 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' 6 (2015) JIPITEC 198

J van Hoboken & FZ Borgesius 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' 6 (2015) *JIPITEC*198 [18]-[19]

F Volio 'Legal Personality, Privacy and the Family', in Henkin (ed) *The International Bill of Rights* (Colombia University Press 1981).

Warren and Brandeis, 'The Right to Privacy' 4 (1890) *Harvard Law Review* Vol 4 at https://www.cs.cornell.edu

Weber and Saravia v. Germany (Dec.), no. 54934/00, ECHR 2006-XI

A White 'A Brief History of Surveillance in America' *Smithsonian magazine* April 2018 https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/#SQdPTWFJ2qfTMZK3.99

Wilson v. United States, 316 F.2d 212 (9th Cir. 1963), cert. denied, 377 U.S. 960 (1964);

World War II Tech eLoran Deployed as GPS Backup in the UK, https://tech.slashdot.org/story/14/11/01/1332248/world-war-ii-tech-eloran-deployed-as-gps-backup-in-the-uk

X v United Kingdom App no 9072/82 (ECHR, 6 October 1982)

X & Y v Netherlands App no 8978/80 (ECHR, 26 March 1985)

M Zimmer 'Surveillance, Privacy and the Ethics of Vehicle Safety Communication technologies' 2005 at *https://link.springer.com/article/10.1007/s10676-006-0016-0*