International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

https://gssrr.org/index.php/JournalOfBasicAndApplied/index

The Implications of New Technologies on Privacy Rights

Pelinzen Ndoke Leonel[a*], Prof. Mbifi Richard[b]

[a,b]*PhD Candidate faculty of law and political science university of Bamenda, P.O. Box 39, Bambili, Cameroon*

Proffessor of law,University of Bamenda, P.O. Box 39, Bambili, Cameroon

[a]*Email: ndokeleonel@gmail.com*

[b]*Email: rmbifi@yahoo.com*

Abstract

The rise in new technologies is very essential in this contemporary world and it has facilitated the communication sector, improve health and economic development. These new digital tools has made life somehow comfortable and accelerated economic growth in the universe. Nevertheless, these digital tools are a threat to privacy of persons.in the course of manipulating these gadgets, they infringe on the rights of privacy of individuals. Some people misuse these gadgets and they do not use it responsibly.Tehila Schwarz noted that"privacy is in the hands of a digital world". A smartphone has multiple functions to invade the privacy of individual, because a smartphone can record messages, videotape events, likewise Close Circuit Television Cameras (CCTV), which are installed in homes and streets, they monitor individuals silently, they are installed for security purpose but in the course of monitoring the activities of individuals, they cross the boundary to invade privacy of persons, because they monitor everybody under the vicinity of the camera. Similarly, an instrument like Global Positioning System (GPS) is capable to detect the position or location of persons, it is use to track individual's movement and position and even cars .These tools are all imperative for our wellbeing but it intrudes on the privacy of individuals.

Keywords: Implication; New technologies; Privacy; Rights.

Received: 2/20/2023
Published: 4/24/2023

---

* Corresponding author.

1. Introduction

The advancement in technology has impacted privacy in a positive and negative way, one cannot undermine the importance of modern technology in this contemporary world for it has its merits and in the same vein, it has its demerits on the right to privacy.

This article focuses on the various types of digital instruments and how they have helped the population and at the same time, explaining and discussing the extent as to how these digital instruments are invading the privacy of individuals.

Modern technologies has brought technological advancement and these instruments are of different designs and functions and each of them has a particular benefit and at the same time most User's misuse these instruments to invade the privacy of others.

Modern technologies and technological advancement has manifested positive impact on individuals, it has improved the standard of living of the general population in the domain of health, education, communication, and the emergence of the internet has improved the system of communication, from whatsapp, instagram, twitter, Facebook, and all these is done over the mobile phone and computers.

Nevertheless, all these digital instruments are worth appreciating, but at the same time, they are being used to violate the privacy of individuals. Some Users of these instruments are unknowingly invading the privacy of others with objects like smartphones, CCTV cameras, and photographing.

Furthermore, internet platforms provides a plethora of elements which are good for communication and friendship between people but these platform is the highest point of privacy invasion, where there is tapping of information and invasion of user's data.

In the field of health, digital tools in the health sector are also a threat to privacy, though they are necessary for the wellbeing of the patients.

The various digitals instruments listed below are essential for modern communication, and for health purposes, nevertheless, they have various ways on how they invade the privacy of individuals.

1.1 Close Circuit Télévision(CCTV) and the Invasion of Privacy Right

The "Watching Eye Effect" refers to the behaviour modification that can occur upon the perception of being observed by something. Researchers have shown that this phenomenon can play an important role in reducing anti-social behaviour of individuals in public. One could argue that such behavioral modification is an unwanted intrusion into people's lives. Moreover, the widespread deployment of smart cameras throughout private and public spaces could lead to significant privacy concerns.

In the pre-IoT (internet of things) era, security cameras took the form of Closed Circuit Television Cameras

(CCTVs). Research regarding the perceptions and behaviours surrounding CCTV can inform our understanding of the widespread use of cameras in smart spaces. CCTV surveillance cameras have been widely adopted by municipalities and businesses around the world to reduce crime and increase public safety. Studies suggest that CCTV's can lead to crime reduction in some cases, particularly for property crimes, and that camera surveillance is most suitable for small, well- defined areas, such as to reduce vehicle crimes in a parking garage, reduce theft in homes and business centers.

Even when they are deployed in public spaces, CCTVs can raise a number of privacy concerns. One's autonomy and dignity can be reduced due to being under surveillance. Even when the presence of a CCTV camera is known, people typically cannot make a determination on who is really behind that camera. Not knowing who is watching can influence how people behave. Surveillance can also have chilling effects on civil liberties and freedoms and can be particularly harmful to vulnerable populations, such as prisoners or students. Despite these concerns, the well-established use of CCTVs for public safety leads to different privacy perceptions and expectations compared to other camera-based technologies, such as smartphones or drones.

One challenge with CCTV is whether and how people are notified that they are under video surveillance. The most widely used way to inform people of CCTVs is to put up a sign indicating that people are within coverage of a camera. When they are clearly visible, even these notices themselves can increase the level of deterrence. However, in many cases such notices are far from effective since people rarely notice them or may become habituated to them over time. Surveillance notices also tend to provide little or no information about what happens with the captured recordings. Video technologies are also becoming smarter, with increasing capabilities toward facial and activity recognition. Again, though, surveillance notices tend to give little indication of the kind of processing that occurs, and there is typically no way for the public to access and control the data collected about them.

In recent years, (internet of things) IoT cameras have joined the ranks of CCTVs and are now being used throughout residential areas to provide for homeowners' security, but also collectively for neighborhood safety and security. While their motivation may be similar to CCTVs,to provide for the safety and security of one's home and belongings, this expansion of surveillance into more private spaces has increased privacy risks. Privately owned (internet of things) IoT cameras are likely even less visible than CCTVs, with no notice at all to passersby. People will remain unaware of the extent to which they are being recorded as they drive down a road or walk down a sidewalk. Rather than prevent crime, knowledge of recording may have chilling effects on behaviour in one's own private spaces. For example, residents may be less likely to speak freely in their own yard or to briefly step outside in a bathrobe if they expect to be recorded by a neighbour's camera.

In summary, the privacy challenges of security cameras are as follows:

Firstly, being recorded can change one's behaviour which can reduce crime but may also be perceived as a violation of one's privacy, since it is in constant surveillance of persons and properties.

Secondly, People are often unaware of, or get habituated to, surveillance notices. Such notices also typically do not reveal the identity of the recipient or how they process the recordings, and they do not allow for access and control.

Thirdly, privately owned (internet of things) IoT cameras further exacerbate these privacy issues, as they tend to inconspicuously survey more private spaces.

CCTV surveillance has a number of technical principles and practical applications that are the same as a photo camera. More specifically, CCTV surveillance could give rise to privacy concerns that are similar to photo applications.

These are electronic devices used for monitoring the activities of individuals.CCTV cameras are placed in the streets, in the offices, at homes, hotels, and many other institutions. They are found in most cities in Cameroon and they are used to monitor the activities of individuals at the work place, at home and others are found in the streets.

The republic of Cameroon now employ surveillance cameras in public places as a primary tool to monitor population movements and to prevent crime and terrorism both in the private and public sectors. Closed circuit television (CCTV) is a system of video cameras, display devices and data network that is used to detect and deter criminal activities. Video surveillance systems are used in public and private places such as schools, homes, or public places for crime prevention purposes.

However, CCTV cameras are used to intrude or invade privacy of individuals, while it is monitoring individuals for security purposes, it is also invading the privacy of others. The CCTV camera operator may want to see the activities of the person in a premises, the person may not have any bad intention but the fact that a camera is around watching your actions is worrisome, it gives some psychological imbalance. The camera is normally invading privacy because most often, many people are not aware of the presence of CCTV installations around the area that they are operating their activities.

Furthermore, CCTV cameras are invading the privacy of individuals, because it all depends on what the security operator is looking for, it may be for the watching of the camera to prevent theft but what if the camera is placed inside a toilet, it means the nakedness of the victim will be disclosed to the CCTV operator, of which may be, was not the actual motive of placing the gadget.

Some people may say that we should not have CCTV cameras in public places, because they want to hide their privacy but some school of thought argues that, once in a public space, there is nothing like privacy right. CCTV cameras invade the privacy of individuals because it covers the footage of all persons passing around the vicinity and such records are not deleted.

The fact that most CCTV cameras are installed in premises without the consent of visitors, implies that, there is a breach in privacy, because the purpose of the CCTV may not be the intention of the operator, because the CCTV operator may have malicious intentions and spying out of the scope and purpose of the gadget.

Nevertheless, criminals are less likely to commit crimes in the area where CCTV cameras are installed, because they are monitored. CCTV cameras invade privacy but sometimes for the general interest of all, for instance, the potential value of public surveillance technology was demonstrated all the way back in April 2013 when investigators identified the two suspects in the Boston Marathon bombing ,after sifting through video images captured by the city's cameras;

CCTV cameras do invade privacy, it is an infringement on one's civil liberty, because innocent people are being filmed doing nothing criminal in public places and some cameras may be placed in public rest rooms. CCTV Cameras are now common in Cameroon, CCTV's are now being installed in towns and cities across Cameroon, with the result that public area surveillance is an inescapable fact of life for a growing number of Cameroonians. Although it appears that there is considerable public support for the use of CCTV cameras, the spread of this technology has serious implications on privacy rights and the relationship between citizens and the state. In particular, CCTV cameras represent a substantial threat to individual privacy and to the exercise of rights such as freedom of expression and freedom of association. As a consequence, it is vital that those responsible for the management and operation of these systems are aware of the dangers of public area surveillance, and that they work to ensure that CCTV operations does not threaten fundamental human rights.

All of us need a degree of privacy. Without it, it would be impossible to maintain a sense of dignity, develop meaningful relationships with others, or simply find time to be alone with our thoughts. Privacy is crucial to the development of the self, because it frees us from having to worry about being constantly watched and judged by those around us, and it enables us to control how and when we share information about ourselves with others. It is for these reasons that most countries recognize at least some basic right to privacy, and limit the ability of individuals, private organizations, and the state to collect information about people's personal lives, or to monitor them without their knowledge or consent.

It is important to recognize that the right to privacy does not disappear as soon as we step outside our homes. Although no sensible person would expect to enjoy the same level of privacy in the street as they would in their own living room, most of us do expect to enjoy a certain degree of privacy and anonymity as we go about our business in public. Indeed, one of the great joys of living in cities is the ability to lose oneself in the crowd, and to be free of the demands of our families, friends, and colleagues. In part, it is this promise of anonymity and the freedom that goes with it that attracts many people to town and city streets. Equally, although few would expect to meet a friend at a restaurant or a coffee shop and be entirely free from scrutiny, there are strong social conventions that help us to enjoy a reasonable level of privacy in such circumstances. While nowhere near as extensive as in such obviously private spaces as the home or car, it is clear that we do have a right to some privacy in public.

By its very nature, public area CCTV undermines this right. By exposing us to scrutiny every time we walk down the street, cameras strip us of the possibility of anonymity and make us visible to the watchful eyes of the state and enterprises. While we obviously surrender a great deal of privacy every time we go out in public, it is still no defense for users of CCTV to point out that other members of the public are also watching us. Being watched, and possibly recorded, by a camera is different from being looked at by a stranger. The former type of

observation is typically longer, more intense, and intimately connected with the power of the state or the institution concerned. This is because we cannot see or question the person behind the camera, it is hard for us to know how to respond to being watched, or to decide what we should do about it, because the images captured by the cameras are kept and the operators have access to them, we cannot be sure that they will not be misinterpreted or used in objectionable ways. As philosopher and criminologist Andrew von Hirsch has observed, being watched by CCTV "is like conducting one's activities in a space with a one-way mirror; while one may know that someone is watching behind the mirror, one does not necessarily know who they are or what they are looking for.

Aside from the obvious intrusion, it is this uncertainty that poses one of the greatest threats to our experience of privacy in public. Faced with the prospect of constant video surveillance, it is reasonable to expect that some members of the public will feel the loss of privacy keenly and change how they behave; not because they believe they are doing anything wrong, but because they don't want to be the subject of police attention or risk having their actions misinterpreted by the surveyors. As Giovanni Buttarelli, the Assistant European Data Protection Supervisor has argued:

"*Being watched changes the way we behave. Indeed, when watched, many of us might censor our speech and our behaviour. This is certainly the case with widespread or continuous surveillance Knowing that every move and gesture is monitored by a camera may have a psychological impact and change behaviours. This constitutes an interference with our privacy.*"

How should operators and managers of CCTV systems seek to ensure that the use of public area surveillance does not fundamentally undermine the right of privacy or negatively change the way in which people enjoy public spaces. First and foremost, it is essential for such systems to be operated in accordance with local and national laws, and every effort must be made to prevent abuse of the cameras and breaches in system security. Secondly, the cameras should only be used for those purposes originally identified when the decision to install them was taken: gradual "function creep" must be avoided. Finally, systems must be open and transparent, and those responsible for running them directly accountable to the public. Although the installation of surveillance cameras in public places has inevitably have a negative effect on individual privacy, by ensuring that the above steps are taken CCTV operators and managers can help to minimize the loss of privacy and ensure surveillance is both lawful and appropriate.

1.2 USB Flash Drive

The USB Flash drive which is also referred to as the thumb drives or memory sticks, are an affordable and convenient way to store and travel with your files. The downside of this tiny devices is that, they can easily be misplaced, or stolen, making important information on the flash drive vulnerable to the person who is in possession of the device.

A USB can absorb large amount of individual information, including vital information such as social security number, confidential client information, financial documents, medical records, passwords for websites, or really

anything you would not allow a stranger to hold on to. When such a device falls in the hands of a computer literate, the person will be tempted to verify the content of the USB key and this will entail reading the content and the rightful owner of this USB will be exposed to privacy risks, all personal information will be vulnerable and readable. Laurence Tribe[1] noted that, increase in technology has brought digital development and electronic gadgets are more efficient and outpacing privacy concerns, which requires some protection under the law.

Many people do misplace their USB keys and it is a privacy concern, because if it falls in wrong hands, its consequences may be disastrous, the point here is that, a person who is not apt to computer operations will not know the value of a USB key but a computer literate will normally invade the USB key in his possession to see the content of the device. The USB is however a good storage device, it is an increasingly common way to store digital files, flash drives are still commonly used. They can be great way to back up your data and provide a cost effective way to store your files, if you need to free up your computer. Additionally, if you need to transfer your files, flash drives certainly come in handy. Nevertheless it involves privacy concerns when misused, the wrongful holder can tap vital information from the device.

1.3 Whole Body Scanners

Whole body imaging scanners seek to address the fact that current technologies and screenings, such as walk-through metal detectors and hand searches, have deficiencies in detecting some types of threats, and that law enforcement and security staff need tools to enable them to deal with threats from explosives and non-metallic weapons at the airports and other significant events. Whole body imaging scanners, or body scanners, provide one possible means of reducing the threat from non-metallic weapons. Body scanners "produce an image of the body of a person showing whether or not objects are hidden in or under his clothes" by using x-ray backscatter or millimeter waves. Given the sensitive nature of the images produced by body scanners, critics have raised privacy concerns in relation to their mass deployment, particularly at large airports, including the revealing of individuals' naked bodies and medical conditions and the protection of individuals' data and images. These concerns largely align with Clarke's understanding of bodily privacy, privacy of behavior and action and privacy of personal data. However, these scanners generate images that we regard as part of personal data. As often seen in Cameroon international airports, like Douala and Yaoundé, we see a queue of passengers removing their belts which have metallic content and their watches, to pass through the body scanners before boarding the plane, is at times boring and tiring in addition to the intrusion of privacy, because the police check points are checking everyone, making sure all metallic content on passengers body are detected. This is for the safety and security of the passengers but it is an intrusion of privacy, because some goods are detected inside a luggage and on a passenger which is not harmful and it will be disclosed to the police officers as an obligation under the rules and regulation of safety and security.

Bodily privacy concerns raised by body scanners have mainly centered on two key issues, the revealing of individuals' naked bodies and revealing information about medical conditions. In terms of revealing naked bodies, privacy advocates argue that this loss of privacy is disproportionate to any gains in security. Academics, privacy advocates, politicians and journalists have all warned that the images resulting from the different types

of body scanners currently deployed in airports and other contexts reveal an individual's "naked body", including "the form, shape and size of genitals, buttocks and female breasts". The issue of "naked images" has also raised questions surrounding child protection laws, and the Electronic Privacy Information Center (EPIC) has argued that the capacity for viewing, storage and recall of images of children may contravene child protection laws. According to privacy advocates, the images also show details of medical conditions that may be embarrassing for individuals. "Passengers expect privacy underneath their clothing and should not be required to display highly personal details of their bodies, as a pre-requisite to boarding a plane". Despite these concerns, many authorities, such as Department for Transport for most developing and developed nations including Cameroon, has argued that, any loss of body privacy is proportionate and legitimate in relation to the security concerns that body scanners address.

Images generated from body scanners could also reveal information about behaviour such as augmentation surgeries or medical related practices.

Concerns around data protection and data privacy revolve around protection of personal data that the scanners generate, including the storage and transmission of images. Privacy International is also concerned that some employ operating scanners will experience an "irresistible pull" to store or transmit images if a "celebrity or someone with an unusual, body goes through the system". In fact, images from body imaging scanners have been posted on the Internet in a breach of the fundamental rights of thousands of people in the world. However, despite the link between body imaging scanners and privacy of personal data, the body scanners example makes clear that Clarke's conception of personal data needs to be expanded to include images as personal data. Thus, data protection laws control the unauthorized storage, transfer and disclosure of personal data, precisely the issues of concerns that are expressed in relation to the images produced by body imaging scanners.

1.4 Radio Frequency Identification -Enabled Travel Documents (RFID)

RFID-enabled travel documents include travel cards, such as oyster cards, credit cards,E - passports, which integrate RFID technology with the use of mass transportation in urban areas and RFID enabled passports, also called e-passports, which are currently being introduced in most countries. Such RFID-enabled travel documents raise privacy concerns within the categories of privacy of behaviour and action, privacy of data and image and privacy of location and space.

Privacy of behaviour and action can have a negative impact by RFID-enabled travel documents, in that, people's behaviours and travel activities are being and can be reconstructed or inferred from information generated as a result of their use of these technologies. Travel routes, frequent destinations and mode of transport can be gleaned from information available on both e-passport databases and travel card databases. Location, time and other information stored on databases can be combined, which police have used to check the whereabouts or movements of suspects' during criminal investigations. Furthermore, aggregated information can provide details that enable travelers' routines to be inferred. This can also materialize into a mistaken identity threat in that the association between an individual and a tag can be spurious or unreal for instance, if the travel card or passport is stolen or given to another person), but the initial association is difficult to break once it is made.

The relative insecurity of personal information on databases represents a threat to personal data protection. RFID systems are composed of tags, readers and back-end databases. In RFID-enabled travel cards, the unique identifier on the chip is linked with personal information for example, if a person pays for the card by credit card, the travelling agency or port of departure will have a record of all your travels and travel times. In RFID-enabled passports, the personal information stored on the chip can also be compromised by being read directly and without authorization from the chip. Unauthorized reading may take place in public space, can occur without the passport holder's knowledge, and can violate data protection principles in that, it can be used to reveal an individual's personal details, biometric information and or their citizenship. Although basic protection measures such as access codes and Faraday cages are built in to e-passports to prevent unauthorised reading**,** Gellert[2] argue that these measures do not provide adequate protection and do not possess the desired long-term security needed for e-passport applications, their validity is estimated to a maximum of 10 years. Systems that store personal data, including biometric data, in back-end databases may also be vulnerable to data protection threats such as hacking, unauthorized access or unauthorized disclosure of information. Some systems have attempted to protect individuals from this threat by separating personal information from the RFID chip in the e-passport. However, the resulting databases which store the sensitive personal information still represent a vulnerability of privacy. Finally, the unauthorized *use* of personal information also represents a privacy threat. In terms of RFID-enabled travel cards, marketing staff can target individuals based on the personal data they are required to submit in an application form and companies could aggregate these pieces of information to construct sophisticated consumer profiles. This is especially true if contactless travel cards are expanded for use as payment for other small items.

Privacy of location and space is another aspect of privacy that is potentially undermined by RFID-enabled travel documents. Both RFID-enabled travel cards and e-passports carry the potential for a location threat, whereby individuals' movements can be monitored based on the RFID signature of their documents. Langheinrich argues that once a tag is associated with a particular person, the presence of the tag implies a location disclosure. Information about where an individual has been, can also be accessed after the fact, using information on databases that store information about when and where documents have been read. While this information could be useful for the individual concerned in terms of billing or payment disputes, it may also harm individuals whose location information is revealed to third parties. Travelers may also be vulnerable to hot listing, which consists of compiling all the available information concerning an individual, so that when an identifier is detected, it can be linked to all the other information available concerning this particular individual. Consequently, authorities could be informed that a travel document connected to a particular individual, or an individual with particular characteristics, has been read in a particular place at a particular time. This generalized threat materializes into specific threats, such as stalking or unauthorized location disclosures to spouses, or other individuals. However, in most places, police or other authorities must obtain a search warrant or court order in order to be given access to the data.

Finally, the RFID signals in passports or travel cards may also be tracked, since most RFID tags are standardized and will broadcast their signal to any compatible reader. This means that an individual could read an RFID chip's unique identifier, store it and follow its signal as long as the RFID reader is within range of the RFID embedded travel card.

1.5 Unmanned Aircraft Systems or Drones

Despite a slow increase in the introduction of UASs (Unmanned Aircraft Systems) in civil applications, such as law enforcement, border patrol and other regulatory surveillance, the use of unmanned aircraft systems (UASs or drones) has generated relatively muted debate about privacy and data protection as stated by Kevin Washington[3]. Privacy is notable by its absence in many discussions about UAS devices, which may be partly explained by their current similarity to existing forms of surveillance such as CCTV surveillance or surveillance by police helicopter. However, the lack of noise and relative invisibility of UASs means that individuals do not know if they are being monitored and UAS surveillance may often occur covertly. Our discussion demonstrates that UASs raise issues of privacy of behaviour and action, privacy of data and image, privacy of location and space and privacy of association.

With surveillance-oriented drones, everyone is monitored regardless of whether their activities warrant suspicion, therefore, all behaviours are monitored and recorded. This potential for negative impacts on privacy of behaviour and action is particularly significant since UAS surveillance is much less overt than CCTV or helicopter surveillance. The potential to use surveillance covertly means that in order to protect themselves from the negative effects of intrusions, individuals must assume they are being surveyed at all times and attempt to adjust their behaviour accordingly. This could introduce anticipatory conformity a "chilling effect",where individuals alter their behaviour because they believe they may be under surveillance. Peter Zimmerman [4]argued that, the way technological advancement has outpaced privacy, it is difficult to restrict invasion of privacy rights of individuals.

UAS surveillance potentially infringes upon privacy of data and image in that it can generate images of individuals, sometimes covertly. This means that data protection principles contained in the basic human rights under privacy rights, Article 12 of the Universal Declaration of Human Rights Act, 1948, and the Data Protection Directive (as well as the proposed Data Protection Regulation) such as transparency, consent and rights of access can be undermined, because individuals may not even realize that they are subject to UAS surveillance at any given moment. Therefore, potentially covert data capture also leaves individuals with a limited ability to exercise privacy by taking "measures to keep private those activities that they do not wish to expose to public view". One particular group which could be disproportionately affected by deployments of UASs in civil air space are celebrities whom paparazzi or other media could target with drones and at the same time UAS may also target or survey terrorists spots by government forces for national security.

UAS devices can infringe upon privacy of location and space in that they can be used to track people or undermine their expectations regarding the boundaries of personal space. **Jeffrey Richardson[5]** noted that, surveillance devices can capture images of a person or a vehicle in public space, thereby placing individuals in particular places at particular times or revealing their movements through public space if more than one image is captured. UASs may also reveal information about private spaces such as back yards or, when flying low, can even transmit images of activities captured within homes, offices or other apparently private spaces. Thus, individuals who assume that their activities are not being monitored because they occur within the home or within private property may find that this assumption is false. The fact that this surveillance can be covert,

makes the capture of this information particularly problematic.

UAS devices may impact upon privacy of association through their ability to monitor individuals and crowds, again, sometimes covertly. Unmanned aircraft systems can generate information about groups or individuals with whom they associate. For example, at protests or other large gatherings of people, the number and organization of individuals can be analyzed, and group membership can be inferred. If UAS visual surveillance was combined with biometrics such as facial recognition technology, individual group membership and affiliation could be discovered. Furthermore, group activities are identified or analyzed, for example, place and time of meetings and activities at meetings.

1.6 Smartphones

Smartphones or mobile telephones are recent technologies which infringes on privacy rights. They are used for communication and the gadgets possess additional functions to intrude on privacy. Smartphones have the possibility to invade the right to privacy through the following means:

Smartphones can record messages while the parties are conversing and it can be stored for decades in the Receiver's Phones and the Receiver can divulged the conversation to another person without the consent of the person. Smartphones are used to invade the privacy of individuals in many circumstances, while conversing with someone, the person can be recording your messages with the use of mobile phones in his pocket, since the gadget is very portable.

Additionally, Smartphones are used to take photos and also to record images and events of people, both in private and public places. Individuals use smartphones to record and spy on people's private affairs. One may be sitting somewhere relaxing and a Smartphone User will just be recording your images and one will be surprise to see it over the social media.

Moreover, Smartphones are used to track and hack Users information and location**.** Besides, it is possible to know the location of a person through Google search map. It performs the activity of a computer, because when connected to the internet, the User is vulnerable to location assessment. Smartphones are used for surveillance, because it has cameras and recording devices attached to it.Sometimes an application, based on the Users current position.

App developers use orientation sensor in the Users device to detect which direction the user is facing. Proximity sensor to see how close they are to a point of interest. While this privacy risks are remarkable, we dot actually know how the public is exploiting the information. However, the perception of risks is subjective experience influenced by different individual factors.

Despite concerns associated with privacy use, the cost benefits of using these applications often outweigh the risks on varying scales. From a large scale perspective, society stands to benefit the use of this data for criminal surveillance purposes. Smartphones have many uses and it is use to manipulate and disseminate information over the social media and the social media and privacy concern will be discussed herein under.

1.7 Social Media

Social media is a collective term for websites and applications that focus on communication, community based–input, interaction, content–sharing, and collaboration. People use social media to stay in touch and interact with friends, family, and various communities. It facilitates the creation and sharing of information, ideas, interest, and other form of expression. Facebook is the largest social media in the world, with a clear advantage over other social media, though it has similar audiences, to others like twitter and Instagram. The figures for the most popular social media websites as of January 2021 are as follows: Facebook has 2.74 billion Users, YouTube has 2.29 billion users, Whattsapp has 2 billion users, and Instagram has 1.22 billion users. There were 9.15 million internet Users in Cameroon in January 2021.The number of internet Users in Cameroon increased by 1.3 million, which is about 16% between 2020 and 2021. Internet penetration in Cameroon stood at 34.0% in January 2022.The social media statistics for Cameroon indicates that, there are about 4.30 million social media Users in Cameroon in January 2022, the number of social media Users in Cameroon increased by 600 thousand between 2020 and 2021.The number of social media Users in Cameroon was equivalent to 16% of the total population in 2021.

Facebook subscription stand at 87%, followed by interest 7.6%, Instagram 2.2 %, Twitter 2.1%, Youtube 1.3%, and LinkedIn 0.0%.

The above applications are used by the internet platform and they are very important for communication between relatives and friends and also to make friendship from home and abroad. However, these tools has its promises and risks as far as privacy is concerned. These social media platforms promotes easy communication between people in the world but it is a threat to privacy. The violation of privacy rights is manifested rampantly over social media and the most notorious is on Facebook which has a very large number of Users.

1.8 Facebook

Facebook is a free, ad-supported social networking service (SNS) with just over 1 billion active users. On May 7, 2012, the company completed an initial public offering with an estimated market value of almost $100 billion, based on approximately $4 billion in annual revenues, almost all of which derives from its online advertising business. During its eight years in business, Facebook has suffered numerous privacy controversies, and Emily Steel &Jessica Vascellaro[6] argued that,it is partly as a result of how the service works, users of Facebook create online profiles, which contain a great deal of personal and sensitive information including their name, their interests, the names of their friends, photos and videos they upload, and content they add to their friends profiles by sending comments and sharing photos. Users may also “tag” their friends’ images, that is, identify them by name without prior consent from those friends and install games and other applications developed by third parties that permit access to the profile information of both the users and their friends. In short, Facebook, by its very nature, raises fundamental privacy challenges because it enables users to disclose unprecedented volumes of highly personal information, not only to friends of friends, but, depending on one’s privacy settings, to very large and unfamiliar audiences as well.

Again, Andrew Besner and colleagues [7] noted that, Facebook app is more complex, since Facebook allows users to share photos with their friends in multiple ways. Users can upload photos to an album, post photos directly to their profile, or post directly to someone else's profile. Once a photo is posted, it may be tag, which creates a link between the tagged photo and a person, page, or place, thereby revealing additional information about the identity and associations of the people depicted on the photo. Users may tag themselves or their friends, who will be notified of the tag. Tagging people also alters the potential audience who can view a photo. Users can remove the tag from the photo, which removes the explicit reference to theuser by eliminating the link to the user's profile, but the photo remains there, accessible from any friend's profiles to which it is cross-linked. Facial recognition is manifested on Facebook platforms, this technology can identify your facial features in photograph or videos. Facebook uses this technology to notify you when you should be tagged in a photo or video and Facebook identify all those who are available to be tagged.

On Facebook platforms you realize that, wedding pictures are shared, people can follow you without your knowledge. Facebook does not only have friend's lists as a way to connect with others. If your profile is set to public, you probably have a list of people following you. Some of these people you may know but others may be strangers to you. They do not even have to add you as a friend, they can follow you to access anything you post publicly. Consequently, many people who have Facebook accounts, may not have their Facebook settings secured. As a result, they probably have a list of unknown followers who can see what they post on their timeline.

Besides, on Facebook platform, pending friends have access to your posts. When a friend request stays pending, the person who sent it can see your profile posts and this is a breach of privacy.

Furthermore, third-party Apps collect information about you, your Facebook applications and games are not as innocent as you may think. Facebook allows its third party apps to collect data about your internet use and even your personal information. Since these applications typically store data on a server, separately from Facebook, data breaches can be difficult to detect.

Similarly, Facebook can control your profile after you die, in the sense that, when you pass away without selecting someone to take care of your account, your information stays with Facebook.

As Facebook tagging has taken off, so has the desire of individuals to retain control over unflattering images. Individuals are especially concerned about unintended results of tagged photos, which may cause embarrassment or humiliation if family, employers, school officials, or law enforcement officials see photos meant for different eyes. These tagging disputes are exacerbated by the fact that the tagging process involves three distinct individuals, the photographer, the tagger, and the tagged subject, who may disagree over the propriety of tagging a given photo. These issues will likely become even more prevalent given Facebook's creation of the Photo Tag Suggest feature, which uses facial recognition technology to help users tag more photos. Users can opt out from this feature and provide direct feedback about any items that friends post or share and Bernard Wood [8] stated that Facebook facilitates photo sharing and the Facebook blog can facilitate satellite photos which can be used to map the earth surface,therefore enabling the possibility of surveying the

earth surface and monitoring activities of individuals as well.

Austin Hangen[9] noted that, Photo Sharing introduces a new set of issues involving two kinds of peer-produced privacy violations,because there is sharing of photos without telling people where the actual website is coming from. The first arises due to the "shrinking perceived audience" problem, in which users indiscriminately disclose potentially embarrassing photos because they forget just how many people can view them notwithstanding their intentions to share them with a much smaller audience. The second implicates the social fallout from tagging disputes, where the photographer, the tagger, and the subject disagree over whether the photo should be untagged, made private, or even removed. As Grimmelmann[10] notes, Facebook is the catalyst of these privacy violations, not the perpetrator.

Additionally, the other social media platforms like Whatsapp, YouTube, Instagram, TikTok, Snap-chat, Pinterest, Reddit, LinkedIn, and Twitter are all social media platforms which discloses the personalities of individuals most often than not without their consent. But Facebook is the most popular social media platform which invades the privacy of individuals. It is less important to elaborate on these elements, since they all have the same functions in the dissemination of information of people.

1.9 Smart Television and the Right to Privacy Invasion

Smart televisions gather data that can be monetized and watching television feels like a benign pastime, but as all television become "smart", connected to the internet via router, they are gaining the ability to watch you too. As soon as you switch them on, Smart television made by the likes of LG, Samsung, and Sony are gathering data from the television itself, as well as from the operating systems and apps.Furthermore, there are devices one plugs in to the television, such as Google Chrome cast, Apple TV Amazon's Fire Stick. A TV is no longer a device for showing contents, it has become a two way mirror allowing you to be observed in real time by a network of advertisers and data brokers. The purpose of this is to gather as much information as possible about your behaviour, interest, preferences, and demographics, so it can be monetized, through targeted advertising.

The data collected by one's smart television, depends on the manufacturer, the brand and version. Most smart televisions are capable of collecting audio, video, and television usage data. Voice activation is one feature with the potential to gather amounts of data. Microphones and software are listening for instructions and they can capture conversations and other sounds within range. These recordings may be sent to third parties to be analyzed.

Moreover, cross-device tracking is another issue to consider. Data collected via your smart television is more valuable when combined with information from other smart devices such as mobile phones, laptops, and home automation gear. This allows individual's to be profiled in detail and geo-location history, web browsing activity, and social information can be added to TV data.

Similarly, there are the cookies and trackers. Apps and browsers on smart televisions use cookies and pixel-tracking technologies, just as websites do to track, recognize, and identify devices for user-profiling. Nevertheless, there is no clear cut answer on what exactly is done with the data, when looking at what a smart

television does on the network, it is often unclear why certain data is being harvested and where it is being sent. Manufacturers claim to use information for personalization and quality of content, but also, it is common to sell this type of data, anonymised or semi-anonymised to third parties, advertising companies, and streaming services. After this data has been sold, it is out of the manufacturer's control.

By using the streaming services on a smart television is another sure fire way to hand over lots of one's personal data.Apps such as Nefflix,Amazon Prime claim that they use data for credit checks and recommendations but this can as well include the private details of individuals like email address, browser type, and payment information.

1.10 Tech Wearables and Privacy

Smart watches and fitness trackers may offer some health benefits to their wearers, but it has a risk of privacy intrusion. When Apple launched its latest watch two years ago, the Chief Executive Officer (CEO) Tim Cook was adamant about the life changing benefits of the new device and expressed Apple's intention in entering the health and fitness industry. In a series of sleek videos promoting the company's latest products, one man described how the watch called 911 when he fell during a run, while a pregnant woman device capacity to measure her heart rate saved not only her but her baby as well. The watch heart rate sensor, Apple promises can help users and doctors identify early signs of cardiovascular problems. 'Apple Watch has powerful apps that makes it the ultimate device for a healthy life.

This belief that technology will save us is a repeated refrain whenever a new tool appears. After all, the internet and social media were supposed to bring more democracy to the world. But in 2023, it is not at all obvious that this belief is justified.

Wearables, also known as digital human-technology interfaces, are information technology devices worn by users that enable continuous recording, collection, transfer, analysis and possibly sharing of data. These devices come in many forms, everything from smart watches and other jewelry, such as rings, and necklaces, to body sensors, eyeglasses, backpacks, and even clothing that can track productivity, gestures, health, sounds, speech, and more.

Tech Wearables can be used in different environments and for a growing array of purposes. According to the Surveillance Studies Centre at Queens University, 425 wearable's are available today with fitness trackers and smart watches using body sensors leading the market. The Apple Watch can track sleep patterns, menstrual cycles, detect high and low heart rate. The Apple Watch and sensory wristbands provide therapeutic help through, for example, medication features and breathing recommendations.

Nevertheless, these devices, worn on our own persons, also enable the collection of data that can be scrutinized by others beyond ourselves as stated by Marie Lamensch,[11] our privacy is exposed online through the wearing of digital devices, which are capable to detect and read our personal or private data, which intrudes on our privacy.

In the health care space, wearables have been used for medical monitoring in post-operative settings. These digital tools are in no doubt invading the privacy of the employees, even though it is to improve workers' productivity, the fact that these companies can track the activities of their employees using digital tools signifies privacy intrusion.

The COVID -19 pandemic has only accelerated the use of digital human-tech interfaces and there is a necessity to weigh their benefits against their risks with regards to privacy intrusion. Over the past years, governments and authorities, including the Republic of Cameroon, have considered and in some cases have already used wearables to track and prevent the spread of COVID 19.South Korea used a smartphone app to monitor its citizens self –quarantining and social distancing but imposed wristbands on those people who violated quarantine. Bracelets were also used to monitor lockdowns, social distancing or quarantining in Hong Kong, Bulgaria, Lichtenstein and Belgium.

The United States of America has 23 contact –tracing apps, more than any other country in the world. Some of the wearable's using these applications monitor complex biological data, including body temperature, to detect infections before symptoms are felt.

With the emergence of COVID 19, Tech companies have seized this moment to test and market new applications for wearable's.

In time of crises, the use of tech interfaces can benefit the general public. And during crises, citizens may be willing to forfeit essential rights.Shoshana Zuboff[12] argued that, surveillance capitalism emerged in the wake of September 11, 2001, as authorities gathered much information as possible in order to protect their citizens.

The core difficulty with tech wearable's, is when it comes to privacy and human rights, because a huge amount of data users surrender to their device and therefore to the company that makes and operates it.

In The Age of Surveillance Capitalism,Zuboff stated that,every time we encounter a digital interface we make our experience available to 'datafication'thus 'rendering unto surveillance capitalism, its continuous tithe of raw –material supplies'.Similarly, American Legal Scholar Julie E.Cohen uses the term surveillance innovation complex,to describe how our bodies have a source of presumptive raw material that are there for the taking 'The perpetual sharing of information normalizes a distinctly Western democratic type of surveillance society, in which surveillance is conceptualized first and foremost as a matter of efficiency and convenience. Following the advent of mass market tech wearables for consumers, one can see surveillance capitalism approaching a new scale.

First because the consumer- tech interface can be worn constantly and is highly privacy invasive, again, because the data collected is extremely intimate, especially when it comes to personal health. There are long term implications to the 'surveillance of the human body by governments, private companies, employers and other entities who have a stake in our data. This is particularly true for devices developed by private tech companies interested in selling devices and collecting data for commercial purposes. Nevertheless, who benefits? How will the data be stored and used and by whom?

The questions keep upcoming but critically the benefits goes to private tech companies. The experience with Apple, Google, Facebook, and others is that, they are not competent enough at protecting privacy and they hide behind opaque terms of services.

A study by the Citizen Lab and Open Effect also show that, basic technical safeguards have sometimes been improperly established and that health apps manage to take the consumers private data without express consent. And send it to advertising firms and other third parties. The 2015 Google Deep Mind –Royal Free London NHS Trust scandal in the United Kingdom is one such case where patients' medical data was given away without proper consent. This example is particularly frightening since the project was a collaboration between a big tech company and the UK National Health Service. It is increasingly obvious that, more and better legal reforms are urgently needed to protect privacy invasion from new technologies.

Advancement in technologies can dramatically improve human life but the notion that it will save us from privacy is a myth.

1.11 Invasion of Privacy by Satellite Surveillance

We face a new world of technological advancements that will have lasting effects on society, industry, and the law. One such advancement is in the field of satellite, imaging. In the past, satellite images have been extremely useful in depicting important world events, such as the Persian Gulf War. Presently, satellite photos are used to map the earth's surface, to aid in ecological research. And to research areas of archeological and paleontological significance. They are used to spot potential famine areas, and even to locate dangerous insects' swarms. In addition, military "spy"satellites can detect a missile launch, military maneuvers, or a ship directional course.

Looking towards the future, higher resolution satellite imaging will play an important role in society. Since the end of the cold war the market for satellite imagery and technology has grown world-wide. In the light of world competition, both government and military satellite developers now strive to generate the highest resolution possible at affordable prices, thus increasing the possibility of satellite imagery to both government and private individuals. Theref6re the potential exist for satellite photos to help law enforcement agencies provide evidence and halt ongoing criminal activity, such as narcotic trafficking, and environmental violations, much in the same manner as aerial surveillance does today. Nevertheless, along with the benefits of satellite photography, there is a cost, the potential existence for unknown sources to scrutinize another person's activities without his knowledge or consent. No longer is the society dealing with mere inferences generated by thermal imagery, or with a simple enhanced view from an above airplane or helicopter. Tehila Schwarz[13] stated that, now, a silent, invisible intruder from space possess the capabilities, to peep in to our businesses,backyards,and even through physical structures in to our homes. Everything and everyone, both the criminal and the innocent alike, will be under monitoring and surveillance. As a result, questions concerning the constitutionality of satellite photography are likely to come up, just as they do when aerial surveillance from an air plane or helicopter takes place. The taking of photographs from a satellite, without first obtaining a warrant violates the right to privacy. It encroaches in to an individual's right to privacy.

Furthermore, gone are those days when trespass Doctrine controlled and a simple physical intrusion constitute an unreasonable search. Krysten Kelly[14] stated "that advanced technology has made physical intrusion unnecessary and therefore one need not trespass to violate an individual's right to privacy". Sophisticated devices are now available that can hear and see what human ears and eyes cannot. At present, many types of artificial satellite orbit the earth, relaying valuable information to its inhabitants. Uses broadly range from communications and environmental survey. However, one of the most important uses of artificial satellite is in the area of pictorial imaging.

1.12 Global positioning System (GPS) and Privacy Concerns

GPS is based on a network of at least 24 satellites that continuously send out radio signals transmitting their locations. A GPS receiver back on Earth can then triangulate its three dimensional position using the information received from at least four of the satellites. The system is accurate everywhere on Earth to within 100feet.

This device is originally developed by the Department of Defense as a means of navigating submarines and guiding missiles, GPS is today used in numerous creative commercial applications. Many municipalities and businesses now use the system for vehicle fleet management, and millions of personal cars nowadays do have GPS navigation system. GPS is even used to track the migration pattern of animals. GPS is capable to track the movement of individuals and the direction of their cars and determine their exact location. The device is implanted in vehicles, and can be used by car renters to track their vehicles location, this a threat to privacy, especially in cases where the Client is unaware or not consented thereof. This device is a privacy intruder when one is not aware or consented of it use. They are used to track the location of goods on transit, thereby capable of tracking the position of the person who is travelling with the good.

2. Results

The result of this study is to the effect that, users of new technologies are on the rise. As of now, about 6.92 billion people are using smartphones and mobile phone users stood at 7.33 billion of the population in the world. These gadgets are used to have access to other online transactions like the social media, using of the global positioning system and using of the cameras to videotape events. The use of new technologies is on the rise and the use of it is a threat to privacy rights, though it has its own merits to humanity and the society at large.

2.1 Limitation of the Study

The study had some limitations like time constraints which was an impediment to the undertaking of this study, time was limited to search for more facts pertaining to some aspects of the study. Similarly, access to findings was at times difficult because to obtain an accurate data, one needs to meet participants and conduct interviews relating to the study, but it was not all that easy, because some participants are uncooperative and unwelcoming, some are apathetic to respond to questions. Again not all the new technologies have been highlighted and elaborated upon, just the pertinent ones have been discussed herein.

3. Conclusions

Based on the literature review and survey of the implications of new technologies on the rights to privacy, the advancement in technology has fostered the development of digital instruments for the benefit of the User's, because it has improved the living standard of most people, since people can now communicate easily around the universe, modern instruments are being used in hospitals, nevertheless, all these modern instruments involved privacy concerns, in that, most often than not, they are being misused by the owners,actually,the problem is not the development of these digital tools, but the problem is the manner that they are being managed by the user's to invade the privacy rights of others and the design of the instruments invade the right of privacy, at times without the intention of the Users. The above digital tools discussed above are all necessary for the improvement of our living standard in the society. In as much as we are embracing them with excitement, they also invade our privacy. These digital tools are beneficial to our daily lives, for it has ease communication in the society, facilitate good medical health care, and people cannot more live without them, but the problem is to use it responsibly and know our limitations and boundaries, in order not to invade the privacy of individuals.

Acknowledgements

The complétion of this article could not have been possible without the participation and assistance of some people. Their contribution is immensely appreciated and gratefully acknowledged. I would like to express my deep appréciation and indebtedness to the following persons: Professor Mbifi Richard who is my academic Mentor, Professor Fombe Lawrence, my friend Dr.Jinkeng Asong, my wife and children, without forgetting my brothers and sister.

References

[1]. Laurence Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic
[2]. Frontier, (1991) Raphael Gellert,Legal Construction of Privacy,(2013)
[3]. Kevin Washington, Locator System Draws Bead on Better Accuracy, May 8, (2000).
[4]. . Peter Zimmelman, Photos from Space: Why Restriction Won't Work, June (1998).
[5]. Jeffrey Richardson, The Future of Space Reconnaissance, (1991)
[6]. Emily Steel & Jessica E Vascellaro, Facebook My Space Confront Privacy Loophole, WALL STR.J.Online, May21, 2010).
[7]. Andrew Besmer et al; Social Applications: Exposing a more secure Framework,(2009)
[8]. Bernard Wood, A Remote Sense for Fossils, January 30,(1992),
[9]. Austin Haugen, Answers to Your Questions on Personalized Web Tools, (Apr 26, 2010).
[10]. Grimmelmann, A Catalyst of Privacy Violation (Undated)
[11]. Marie Lamensch, Putting Our Privacy Online, August 11, (2021).
[12]. Shoshanna Zuboff, The Age of Surveillance Capitalism, (2018).
[13]. Tehila Schwarz, Privacy in a Digital World, (2019).
[14]. Krysten C .Kelly, Warrantless Satellite Surveillance, (1995).