Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking

Chika Ebere Odoemelam

Abstract—**The concept of surveillance has received immense attention especially since September 11, 2001 terrorist attack in the USA. Surveillance could be defined as watching over something, secretly monitoring the lives and movements of others with a view to either stopping a crime from taken place or for the purpose of national security. New models of technologies have changed not only the practices of surveillance but also its very nature and as a result have extremely diminished individuals' privacy rights. For instance, surveillance as it occurs in social media has been increased in these environments because everybody is watching everybody. This paper will look at the various forms of surveillance such as e-mailing, telephone and movement tracking, and electronic monitoring bracelets for prisoners, etc. The study will finally discuss society and surveillance adaptation, as well as the issue of privacy violations and wrap up with a conclusion.**

Index Terms—**Privacy, social network-ing, surveillance, technological.**

I. Introduction

There is no doubt that surveillance is very crucial in the investigation of organized and other serious crimes. It gives law enforcement agencies all over the globe the opportunity to speed up the process of evidence gathering and the prosecution of offenders. In the developed world, electronic surveillance is a common phenomenon used in solving crime. Electronic surveillance is a common phenomenon these days with invisible, visible, semi-concealed cameras and sensors embedded everywhere in all corners of society. There also exist laws around how cameras can be utilized in public spaces. However, surveillance is also used in homes, offices, and other public places, as a way of exerting control by parents over their children, community members over their neighbours, managers over their employees and the government over its citizens.

Since the September 11, 2001 terrorist attack in the US, many countries have introduced a significant amount of technology focused on the detection of personal information of those within and outside of their borders. There is no doubt that despite all the advantages of the use of surveillance technology, it has eroded our privacy in a number of ways. For instance, we reveal our information and personal data through participation in social networking sites such as Facebook, Twitter, blogs, and job application websites, Smartphone usage, e-commerce transactions and Foursquare. Whether privacy will be protected, the degree to which anonymity will be allowed, and the extent to which restrictions to access to personal data will be guaranteed, will all depend on the extent to which the general public re-examines their accepting attitude towards privacy issues, especially in this era of digital technology.

Besides, even though a lot of benefits exist as a result of the use of electronic surveillance in crime investigation, the question should be, how do we strike a balance between electronic surveillance and the protection of citizens' fundamental human rights and privacy? Thus, the purpose of this research is to define the meaning of surveillance and privacy issues. According to Anabel Quan-Haase (2013) [1], “the term surveillance originates in the French language and means “watching over”. Observing the lives of other people and their behaviours, appearances and social relationships in a naturally occurring social process”. Also Foucault (1977) [2] saw surveillance as a “shameful act” of supervising and imposing discipline on a subject through a hierarchized system of policing”. This means that Foucault believed that surveillance act as a mechanism of control for those who hold political and economic authority. This research will also look at the various forms of surveillance such as e-mailing, telephone and movement tracking, and electronic monitoring bracelets for prisoners, etc. The study will finally discuss society and surveillance adaptation, as well as the issue of privacy violations and wrap up with a conclusion.

II. Literature Review

Surveillance cameras are seen everywhere in developed cities across the world with the aim of monitoring the activities of people and for security purposes. Such cameras are a ubiquitous commodity of the 21st century, especially since after the September 11, 2001 terrorist attacks in the United States.

According to an article by the United Nations Office on Drugs and Crime, (2009) [3], “Surveillance is the collection or monitoring of information about a person or persons through the use of technology”. Thus, from the above definition, one can see that surveillance involves a wide range of technology and practices aimed at monitoring the activities of people possibly without their knowledge and permission. For instance, there is audio surveillance which involves phone-tapping and listening devices, visual surveillance which involves in-car video devices, hidden video surveillance, and closed-circuit television camera (CCTV), tracking surveillance which includes global positioning systems (GPS) and mobile phones and data surveillance which involves computer, internet and keystroke monitoring. The majority of the above devices are constantly

Manuscript received March 3, 2014; revised May 2, 2014.

Chika Ebere Odoemelam is with University of Western Ontario, London, Ontario, Canada (e-mail: ochikaebere@yahoo.ca).

DOI: 10.7763/IJSSH.2015.V5.520

used to monitor people without their prior permission.

Furthermore, surveillance according to David Lyon (2007) [4] is “the focused, systematic and routine attention to personal details for the purposes of influence, management, protection or direction”. The above definition shows that surveillance is an instrument used by the authorities for the monitoring and management of the activities of its citizenry. Thus, to achieve this objective, nations use electronic communication technologies such as wiretapping telephone conversations, tracking people with biometric data and using infrared cameras. In the same vein, marketing firms sometimes use social media technologies such as Facebook, Twitter, blogs and instant messaging devices to collect data about individual users, and in most cases, end up in violating the privacy of the users.

Privacy according to Woo Jisuk (2006) [5], refers to “how one's own personal data and information about others are handled in social contexts, particularly more public setting. The “private” is that which is shared only with close, trusted, face-to-face relations”. The above definition explains that privacy has to do with the protection of sensitive data and information, such as medical and financial records, as well as personal relations from unauthorized access or view. One should also note that the emergence of social and new digital media such as Twitter, blogs, Facebook, Smartphones and instant messaging systems, that allow for the sharing of personal information in the public domain are making privacy issues more problematic for the members of the public.

Also according to Encyclopedia.com (2008) [6], school bus cameras both “improve behaviour and overall safety” and “offer reassurance to youngsters and their parents” who are worried about bullying and abusive behaviour”. From this definition, one can see that surveillance encompasses all forms of monitoring whether at home, at the office, at school or even on public transportation. Hence, while all kinds of surveillance devices are designed by the government and other security experts as a way of ensuring the safety of everyone, they also directly or indirectly violate the fundamental rights of citizens. For instance, the recent claims that US intelligence agencies have been monitoring the mobile phone conversations of German Chancellor, Angela Merkel and Argentine president, Cristina Fernandez is a typical case of breach of one's privacy and fundamental human right. Also, it is worthwhile, to note at this juncture that our governments and communities are more conscious about safety because of broader economic, social, political and cultural changes and conceptions of freedom and constraint.

The concise Oxford Dictionary defines surveillance as “close observation”, especially of a suspected person”. From the above definition, one can deduce that surveillance is supposed to apply to “a suspected person”. But the big question is , is that the case in our today's world? Electronic surveillance has become a common phenomenon especially in the developed world as a way of monitoring the activities of every member of the society irrespective of whether or not they are a suspect. Again, in our present day world filled with all kinds of modern technology, surveillance could be carried out from afar instead of only from “close observation”, as the dictionary meaning suggests. Satellite images and remote monitoring of communications via high-powered infra-red technologies can be used for long distance surveillance activities. Thus, governments and big corporations have made surveillance part of everyday life, in that it includes, but is not limited to, hidden cameras in an ATM machines, data bases of all employees in a particular company, scanners that picks mobile phone communications, computer programs that monitor keystrokes, or key words and video cameras that parents can use, to monitor, their children at a day care centre.

Still contributing in the definition of surveillance, Gary T. Marx, (2002) [7], adds to the definition of surveillance by describing it as “The use of technical means to extract or create personal data. This may be taken from individuals or contexts”. The above definition suggests that those that have the power or authority, such as police and other members of law enforcement agencies, can carry out surveillance activities beyond what individuals disclose to them and without their prior notice or permission. Hence, to carry out such operations in the context, law enforcement agents look at patterns and settings of relationships while using surveillance technologies, such as data profiling of individuals.

Anthony Giddens (1984) [8], provided a definition of surveillance based on administration, explaining that “surveillance as the mobilising of administrative power-through the storage of and control of information-is the primary means of the concentration of authoritative resources involved in the formation of nation-state”. Through the above definition, Giddens explains that the modern state uses surveillance and information gathering mechanisms such as those related to births, marriages, deaths and other demographic figures, as a means of exerting its authority, power and influence on the society as the only instrument of enforcing control on its citizens. As a result, surveillance has become a universal phenomenon that exists in every sphere of all human endeavours.

Also surveillance according to Ogura Toshimaru (2006) [9], “surveillance refers to an activity which enables the nation state, or capitalist formations like corporations, to manage a population”. The above definition entails a way of monitoring employee performance by employers of labour for their own selfish purposes and maximum benefit. It is a form of control imposed by the owners of the means of production as a way of further enslaving their employees for their own benefit and profit.

III. Research Questions

The following questions will be examined in this research:

1) Why have people adapted to surveillance as a way of life?
2) Why is surveillance an important tool for government and societal safety?
3) What instruments are involved with surveillance?
4) When, and at what stage of surveillance is a person's privacy violated?

IV. Research Problem

Over the last decade, the issue of surveillance and privacy has become a great concern to the majority of members of the society. One of the reasons for this is the rise in modern technology that is easily accessible by the vast majority of the society. Another reason is the over-dependence on technology by both governments, corporations and the general public in the execution of their day to day activities. Modern technology has become part and parcel of our everyday life to the extent that life is now meaningless without technology. We live in the age of digital world and technology. Everyone is trying to catch up in one way or the other irrespective of the consequences.

Moreover, detailed personal information is often times requested by governments or organizations before simple or complex transactions can be completed. People are asked to fill out forms, produce identification, or undergo fingerprinting, DNA tests, or urine tests, depending on the type of help they need from the government or an organization. In the developed world, everyday life is anchored on record keeping, monitoring, and supervision by many different agencies and organizations. Thus, the ways and means through which these personal details are collected, stored, processed and retrieved are further evidence that the whole world now depends on technology irrespective of its negative implications.

Our privacy and personal information are being constantly eroded, as a result of this high level of dependence on technology. However, individuals sometimes complain and make noise whenever their personal information or data are compromised by corporations, governments or the business world. They will threaten such organizations with law suits and boycott their products. But after a certain number of months the anxiety will disappear. The same members of the society will continue their patronage of such businesses and organizations as if nothing had happened in the first place. This very scenario motivated the researcher to venture into this project.

It is on the basis of the above, that this research has become necessary. Reasons abound as to why society is so dependent on technology. Such reasons include; quick communication networks across continents with the help of the internet, for business purposes such as, marketing, advertising, e-commerce and other forms of electronic transactions for business purposes, electronic e-mailing via the use of Twitter, Facebook, and blogs, and electronic surveillance by various governments all over the world for national security and public safety. Based on the above, this research, when completed, will contribute in no small measure to the wealth of data and materials that already exists in the field of surveillance and privacy. It will also help scholars, academics and other researchers who might look at this aspect of research in the near future.

V. Types of Surveillance

The advent of advanced forms of technology has made our lives more prone to public scrutiny today, in the 21st century. The concept of a surveillance society whereby our everyday private lives are being monitored and recorded by the authorities is no longer news. Since the September 2001 terrorists attack in the United States, the assault on our privacy by security agents using sophisticated surveillance programs or privacy-invading devices has been a constant presence in the news media. The availability of wireless communications, computers, cameras, sensors, GPS, biometrics, and other technologies is growing silently in our midst.

According Christopher Parsons (2011) [10], “When we send messages to one another online, when we browse web pages and send e-mail, our communications are typically unencrypted, that is, they are in a form that can be easily read”. Because our communications are unencrypted, everyone who uses online technology or other forms of communications is vulnerable to surveillance. Our online and offline communications are constantly being monitored and are under surveillance by the “appropriate” authorities. As a result, it is possible for our privacy to be violated without our consent because of our reliance on technology. There is a huge privacy issue in relation to digital and other forms of communications all over the globe, especially when telecommunications companies install equipment that could be used for covert surveillance and even modification of our communications.

Moreover, various forms of surveillance abound that could be blamed for bringing our lives out of the private domain and into the public sphere. These forms of surveillance include.

A. *E-mail Surveillance*

This is related to the monitoring of both encrypted and unencrypted electronic messages or communications of individuals by government agencies. The government does this by ordering Internet Service Providers (ISP) to inspect their user's communications data, both encrypted and unencrypted. According to the *New York Times* (June 16, 2009) [11] article, “The National Security Agency is facing renewed scrutiny over the extent of its domestic surveillance program, with critics in Congress saying its recent intercepts of the private telephone calls and e-mail messages of Americans are broader than previously acknowledged, current and former officials said”. The above statement suggests that we are living in a surveillance society, and that the challenges society will face in adapting it as a way of life are enormous and potentially overwhelming.

B. *Telephone Tracking Surveillance*

The recent claims that US intelligence agencies have been monitoring the mobile phone conversations of German Chancellor, Angela Merkel, as well as those of over seventy million French citizens, is a strong example of telephone surveillance.

According to an article, *Der Spiegel* (2013) [12] reporting on information obtained from former NSA worker Edward Snowden, “Merkel's mobile number had been listed by the NSA's Special Collection Service (SCS) since 2002 and may have been monitored for more than 10 years”. This information makes it obvious that the surveillance business observes no boundaries and a respects no individual. In surveillance, everybody is a suspect irrespective of one's position in the society. Surveillance is sometimes carried out by tapping the targets' communications with high-tech surveillance equipment, thus threatening their right to privacy as guaranteed by the International Covenant on Civil and Political Rights. Disclosures of this nature will continue to raise fundamental questions around the world about how to effectively protect our privacy and our personal data from unauthorized surveillance. For instance, if companies are handing over customer data or access to their equipment without authorization, those businesses may well have broken the law by violating the privacy of their customers.

C. Other Forms of Surveillance

According to Christian Fuschs (2010) [13], other forms of surveillance include:

1) Scanning the fingerprints of visitors entering the United States.
2) The use of speed cameras for identifying speeders which involves state power.
3) Electronic monitoring bracelets for prisoners in an open prison system.
4) Scanning of Internet and phone data by secret services.
5) Usage of full body scanners at airports.
6) Biometric passports containing digital fingerprints.
7) CCTV cameras in public places for the prevention of crime and terrorism.
8) Assessment of customer shopping behaviour with the help of loyalty cards.
9) Data collection in marketing research.
10) Assessment of personal images and videos of applicants on Facebook by employers prior to a job interview.
11) Passenger Name Record (PNR) data transfer in the aviation industry.
12) Corporations spying on employees, or union members.

VI. Society and Surveillance Adaptation

The continuing assault on our privacy as a result of technology is no longer news. People have consciously and unconsciously adapted to surveillance and invasion of privacy as a way of life. Surveillance technologies have been embedded into our existing norms and practices as additional forms of communication. As numerous forms of technology are introduced into the market, individuals have increasingly lost control over who has access to their personal information, why others want that access, and when others access their personal information. It is obvious that people have lost this control because of the ubiquitous nature of surveillance technologies in every nook and cranny of society.

The introduction of social networking sites such as Facebook, Twitter, Instagram, MySpace, has also contributed to opening up many of the previously shielded aspects of human life to the public realm. Social networking site users therefore view surveillance as a issue of trade-off: the individual provides his or her personal information, and will receive something in exchange.

Besides, reasons why individuals and society in general, adapt to surveillance abound. In one of his articles, Gary T. Marx (2002) identifies three approaches that describe the changes in surveillance as a result of the information revolution and its associated technologies:

A. Functional View

In order to operate effectively, societies require some element of security and safety.

B. Revolutionary View

The introduction of new technologies have led to a radical transformation in the very nature of surveillance, placing basic privacy rights in jeopardy.

C. Cultural View

Social and cultural factors moderate how information technology impacts sur-veillance.

For the purpose of this essay, the revolutionary view will be considered, as it supports the notion that the advent of new and advanced technologies has led to increased violation of the privacy of individuals. In this global age of digital technology, nothing is private or sacred anymore. People adapt to surveillance as the only way they can protect themselves from being under constant surveillance. This means that people let go their privacy as a way of saying, “this is me, I have nothing to hide”.

Another reason people adapt to surveillance is the introduction of “self-imposed surveillance” as result of the increasing popularity of social networking sites like Facebook, Twitter, and MySpace. In the case of Facebook, account owners decide on what to post and what not to post. Users willingly allow themselves to be monitored by the simple act of registering on these sites with their personal information, without being forced by anyone. Most people who use Facebook, Twitter, and other social networking sites are happy to be part of the digital world irrespective of privacy issues or concerns.

Convenience is another reason why the society adapts to the increase in surveillance. This means that most people are fully aware of the consequences of sharing their personal information online, but continuously engage in it because they do not have a choice. People have decided to give out their personal information online because of over- reliance on technology that is omnipresent and almost unavoidable.

Furthermore, people adapt to surveillance because they are trying to ensure that their friends, family members, and colleagues can easily find them when the need arises. Based on this, they are willing to release their e-mail address, phone numbers, first and last name, pictures, home address, date of birth, sexual orientation and even relationships status online without any trepidation.

VII. Privacy

The emergence of advanced new technologies has exposed our private lives to the public domain to such an extent that everyone is a target. Social networking sites such as Facebook, Twitter, and Instagram have become major surveillance centres, storing the personal information of millions of users. These sites continuously redefine what is legally considered as “private”. As a result, our personal data are often violated without our consent. Privacy violation entails looking into the personal data of another individual without their consent or authorization. Violation of privacy also occurs when recipients of our personal information, which we intentionally shared with them or which we lost through an invasion of privacy, disclose our information to others. Hence, technology has directly collided with our societal definition of public life, semi-public life, and private life, creating very serious negative consequences for all of us.

According to Margulis (2003b) [14], there are two domain views of privacy: the socio-political and the psychological perspectives. From a socio-political perspective, "privacy refers to a core of fundamental rights and freedoms afforded individuals in a liberal democratic society, including freedom of expression, freedom of thought, freedom from unwarranted police and government interference, and freedom for political expression and criticism".

For A. F. Westin (1967) [15], privacy from a psychological perspective protects personal autonomy, which is important for the development and maintenance of the self and individuality. "It provides individuals with opportunities for self-reflection/ evaluation and experimentation; it supports emotional release outside of the public sphere, thereby allowing individuals to vent, make unfair or frivolous comments without public scrutiny; and, it enables individuals to decide for themselves when, to whom and to what extent personal information should be revealed to others".

Besides, individuals are sometimes aware of the privacy concerns they face online, but they may not know how to protect themselves from unauthorized interference. Users of technology often exhibit only vague knowledge with regard to protect themselves and their personal information from getting into the hands of unauthorized persons.

It is worthy of note that in some cases, most people does not even know how to differentiate between information that will jeopardise their privacy and those that will not. Our personal information is constantly under the purview of the public sphere. The vast majority of Internet users are not careful about what they post online, leaving their information accessible to anyone at any point in time.

VIII. Methods

This study is primarily meant to discover how and why people adapt to surveillance in this era of technology and social networking. To achieve this, the study adopts the content analysis approach, by reviewing the related literature in the field of surveillance and privacy.

Content analysis was adopted as the main tool of data generation. Subsequently, content categories were developed to analyze the data collected.

This study further developed some content classifications to determine and analyze the definitions of such terms as surveillance, and privacy, and to examine and differentiate between the different forms of surveillance.

IX. Conclusion

In this paper, I provided a wide-ranging account of the various literatures on surveillance and privacy issues. The main purpose of this paper was to argue that people adapt to surveillance in this digital age due to a number of reasons including convenience, the increased use of social networking sites, etc. The paper also focused on the different forms of surveillance that exists which in the long run, have contributed to the further violation of our privacy. Social networking sites such as Facebook, Twitter, MySpace and Instagram have not helped protect the personal information of users. Thus, it is my opinion that advances in technology have tremendously increased the power of the state to carry out surveillance upon its citizens without any form of restraint. This situation has inevitably exposed members of the society to constant surveillance by security agents.

References

[1] A. Q. Haase, *Technology and Society: Social Networks, Power, and Inequality*, 1st ed Oxford University Press Canada, 2013, ch. 10, p.192.

[2] F. Michel, "Discipline and punishment: The birth of the prison," *Trans. Alan Sheridan*, New York: Vintage Books, September 1977.

[3] United Nations Office on Drugs and Crimes: Current Practices in Electronic Surveillance in the Investigation of Serious and Organized crime. (June 2009). New York. [Online]. p. 5. Available: http//www.unodc.org/document/organizedcrime/lawenforc-ement/electronic surveillance.pdf

[4] D. Lyon, *Surveillance Studies: An Overview*, Cambridge, UK, 2007, pp.12-14.

[5] W. Jisuk, "The right not to be identified: Privacy and anonymity in the interactive media environment," *New Media and Society*, vol. 8 no. 6, pp. 949-967, July 2006.

[6] Free Online Encyclopedia. (2008). [Online]. Available: http://www. Encyclopedia.com

[7] G. T. Marx, "What's new about the 'new surveillance'?" *Classifying for Change and Continuity*, Massachusetts, USA, 2002.

[8] A. Giddens, *A Contemporary Critique of Historical Materialism*, the Nation-State and Violence, Cambridge, UK, ch. 2.

[9] O. Toshimaru, "Electronic govern-ment and surveillance-oriented society," in *Theorizing Surveillance: The Panopticon and Beyond*, ed. David Lyon, Cullompton, UK: William, pp. 270-295.

[10] C. Parsons, "Security, surveillance and sovereignty: The internet tree: The state of telecom policy in Canada," *Canadian Centre for Policy Alternatives*, vol. 3, pp. 83, March, 2011.

[11] *New York Times Publication*, June 16, 2009

[12] *Der Spiegel: NSA's Secret Spy Hub in Berlin*, October 27, 2013

[13] C. Fuschs, "Theoretical foundations of defining the participatory, co-operative, sustainable information society," *Information, Communication and Society*, vol. 13, no. 1, pp. 23-47, June 2010.

[14] S. T. Margulis, "Privacy as a social issue and behavioural concept," *Journal of Social Issues*, vol. 59, no. 2, pp. 243-261, March 2003.

[15] A. F. Westin, *Privacy and Freedom*, New York, Antheneum, 1967.

Chika Ebere Odoemelam was born in Ehime-Mbano, Imo State Nigeria. He obtained higher national diploma in mass communication of the Institute of Management And Technology (IMT), Enugu 1997 and a diploma in computer science and information technology from Goon Institute (St. Clement University, United Kingdom) in 2002. In 2005, he earned a master of arts degree in Media Studies of the University of Malaya, Kuala Lumpur, Malaysia and another master of arts degree in Media Studies of the University of Western Ontario, London Ontario, Canada.

He was a visiting research postgraduate scholar Lehigh University, Pennsylvania State, USA from 2002-2003, and a guest lecturer at the department of Journalism, University of Toronto in 2010. Before coming to Malaysia and Canada, Mr. Odoemelam worked as a public relations officer, Nigeria Telecommunications Limited (NITEL), as a journalist with Ondo State Television (ODTV), Akure, Ondo State, and also with the National Post Newspaper, Owerri, Imo State. He joined University of western ontario as a graduate teaching assistant in 2012 and has been there till date. He has also completed his Ph.D degree in Media studies at the University of Malaya, Kuala Lumpur, Malaysia and awaiting for his graduation ceremony. His research interests are political communication, environmental journalism, communication theories, crisis communication, communication/dialogue and conflict resolution, and public relations.

Mr. Odoemelam is currently a member of the Canadian communication association, national communication association, society of environmental journalists, international federation of environmental journalists and the Nigerian institute of public relations. He has received several awards such as certificate of merit as the best anti-drug reporter by the National Drug Law Enforcement Agency (NDLEA), Ondo State Chapter, 1999, certificate of honour as an active participant at an international conference on the management of information pertaining to health crisis, Kuala Lumpur, Malaysia, 2007, certificate of honour as a presenter/author at an international conference at Carnegie Mellon University, Pittsburgh Pennsylvania State, USA, 2004, certificate of honour as a presenter/author at an international conference on Environmental Journalism, Putrajaya, Malaysia, 2003, certificate of honour as a presenter/author at an international conference on journalism and sustainable development, Singapore, 2002.