

E-Surveillance Vis-à-Vis Digital Privacy Rights under the Information and Communication Technology (ICT) Act- 2006: Inquesting of New Hope or Hype?

Md. Zubair Kasem Khan ¹
Dilruba Parvin²

Abstract

The sophistication of science and technologies has profoundly altered the way of social life. This also led to a paradigm shift in the methodology of taking preventive measures for conforming security, both nationally and transnationally throughout the world. The newly adopted Information and Communication Technology (ICT) Act- 2006 [Act No. 39 of 2006] has raised new controversies relating to constitutional and privacy issues in Bangladesh by allowing the law enforcement agents to impose electronic monitoring as well as other types of technologically-aided surveillance software for the purpose of intruding conversations of the citizens of Bangladesh on the whole. This processing of personal information by dint of wiretapping by the security officers intersects with a very basic notion of individuals' data privacy, 'protection of home and correspondence' and 'Protection of right to life and personal liberty' which were protected by the Constitution of Bangladesh to some extent. With latest legislative and judicial supports thrown on the right to data privacy of individuals, questions now emerge on whether this support to privacy right will be short-lived by the newly-passed ICT law, which legally introduce the power of electronic surveillance in Bangladesh? This paper seeks to initially explore this intersection and to outline the roadmap for better legal development in Bangladesh.

Keywords: *Electronic Surveillance, Right to Privacy, Security, Law Enforcement.*

-
1. Lecturer, Department of Law, International Islamic University Chittagong (IIUC), Bangladesh. Former Graduate Research Assistant, Ahmad Ibrahim Kulliyah of Laws (AIKOL), International Islamic University Malaysia (IIUM), Malaysia. Tel: +88017 1717 2254, Email: zubair.rumi505@gmail.com
 2. Lecturer, Department of Law, International Islamic University Chittagong (IIUC), Bangladesh. Email: deepalawdu@yahoo.com

1. Introduction

*“...The world isn't run by weapons anymore, or energy or money. It is run by little ones and zeros, little bits of data, it's all just electrons. There's a war out there old friend, a world war. And it's not about who's got the most bullets, it's about who controls the information, what we see and hear, how we work, how we think. It's all about the information...”*³

This twenty-twenty vision film-noir prediction that was expressed twenty-three years back in ‘*Sneakers*’ movie becomes spot-on nowadays, owing to the proliferation of the use of internet in the globe. In addition, making connection with millions of computer-networks, undoubtedly metamorphose the wide notion of “world” what we understood twenty years back in subjective. Rather, it becomes a ‘global village’ where no one is disembodied from this cyber network.

In this era of globalization, a substantive endeavour has been taken by the technologist to develop science and to innovate smart high-tech gadgets. This amelioration of technologies have contributed in security paradigm and correspondingly have given the governments as well as law enforcement agents of both domestic (by the police) and international (by the Interpol) levels, a remarkable opportunity to conduct surveillance over ordinary citizens or suspected criminals. Even some unpleasant controversies have been occurred owing to conducting surveillance privately over senior officials in national level.⁴

“E-Surveillance” or “Electronic Surveillance” predominantly connotes any kinds of secret close observation over a particular location or person by using electronic apparatus for the purpose of monitoring or gathering evidence.⁵ This could be conducted in several electronic forms like- radio surveillance, radar surveillance, infrared surveillance, visual surveillance, aerial surveillance, ultraviolet surveillance etc.⁶ Correspondingly, various kinds of techniques have been invented over time only to ensure national security and to control social felonies.⁷ Moreover, one can easily be under the surveillance of national security agent by tracing his

3 Lask, Lawrence., Parkes, Walter F., (Producer) & Robinson, Phil. A., (Director), *Sneakers*, [Videotape], United States: Universal Studios, 1992.

4 Ahmed, B. Nazir., “The recent Skype scandal and its impact on the Apex Judiciary of Bangladesh”, retrieved on January 03, 2013 from <http://newsfrombangladesh.net/new/highlights/5977-the-recent-skype-scandal-and-its-impact-on-the-apex-judiciary-of-bangladesh>

5 Garner, Bryan A., *Black's Law Dictionary*, Eighth Edition, St. Paul: Thomson, 2004 at 1486.

6 Peterson, Julie K., *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications*, New York: CRC Press, 2001 at 1-11.

7 Khan, Md. Zubair Kasem., “Privacy Issues in Electronic Surveillance in Malaysia: A Comparative Analysis between Common Law and the Sharīah” (MCL dissertation, International Islamic University Malaysia, 2015).

cellular phone-calls even about his whereabouts.⁸ In particular, the epidemic government surveillance by way of wiretapping (or by mobile tracking) and other forms of digital communications (like: video conferencing through Skype-casting) without court-approved warrants has now become one of the blistering cross-border issues in mass-media, especially, the evidentiary documents on American digital surveillance, that was leaked out by former contractor of the American National Security Agency, *Edward J. Snowden*. Scenarios have undergone by far awful when it affects the diplomatic relationship between Berlin-Washington as reflected in the New York Times.⁹

Therefore, the modern technology facilitates the security agents of any country to use considerable number of diurnal electronic devices as a surveillance instrument that we are attached with. Thus, Anthony Amsterdam legitimately described how damaging is the widespread use of electronic surveillance in this contemporary society when he said that:

*“...The insidious, far-reaching and indiscriminate nature of electronic surveillance - and, most important, its capacity to choke off free human discourse that is the hallmark of an open society - makes it almost, although not quite, as destructive of liberty as “the kicked-in door”...”*¹⁰

2. Provisions of Conducting E-Surveillance in Bangladesh

In perspective of Bangladesh, the Government of Bangladesh enacted the *Information and Communication Technology (ICT) Act- 2006* [Act No. 39 of 2006] in 2006 as a key instrument for supporting the development of information and communication technologies in Bangladesh. It is intended to facilitate the application of information and communication technologies for building information society. Furthermore, the cardinal objective behind the adoption of this statute is to bolster the advisable use of information technology and to assure its sustainability in overall social system, in line with international regulations.¹¹

8 Tatum, Christine., “Navigators Hit Road in Digital Quest”, *The Chicago Tribune*, 29 July, 2002 at <http://articles.chicagotribune.com/2002-07-29/business/0207290009_1_mapquest-charles-dolan-digital-maps>

9 Smale, Alison., “Surveillance Revelations Shake U.S.-German Ties”, *The New York Times*, 25 August, 2013. Viewed from http://www.nytimes.com/2013/08/26/world/europe/surveillance-revelations-shake-us-german-ties.html?_r=0

10 Amsterdam, Anthony G., “Perspectives on the Fourth Amendment”, Vol. 58, (1974), *Minnesota Law Review*, at 349, 400. See also: Gray, David., and Citron, Danielle., “The Right to Quantitative Privacy”, Vol. 98 No. 62, (2013) *Minnesota Law Review*, at 12.

11 Hassan, M. Mahdy., “Violation Of Right To Digital Privacy”, Retrieved on November 20, 2015 from <http://archive.thedailystar.net/beta2/news/violation-of-right-to-digital-privacy/>

Under the ICT Act- 2006, provision has been inserted under Sec. 9 to provide a guideline of the retention of electronic records. Here, "Electronic Record"¹² denotes: E-mail, picture, image or sound recording (conversations either through cellular or by Skype-casting), SMS etc. Moreover, Sec. 29 confers power to the Controller to investigate himself about the contravention of the provisions of this Act, or give authorization, in written, to a Deputy Controller, Assistant Controller or any other officer (under Sec. 28) to do so. Sec. 30 of the said Act- 2006 dedicates the Controller or any officer authorized by him, the power to Access to computers and data. Furthermore, under Sec. 46¹³ of the ICT Act- 2006, a Controller has the power to give authorization to any government agency to intercept any information to be transmitted through any computer resource in the ground for the interest of the sovereignty, integrity, or security of Bangladesh etc.

In other words, in a situation, where information is transmitted through computer, computer network or by any other means of transmission via internet and as a consequence, national peace, security and tranquility could be disrupted, then the Controller can have the power to direct any agency of the government to investigate, intercept or cease that information transmitted through internet or any computer resources.¹⁴ All these provisions undoubtedly signifies that, the controller or any law enforcement agent authorized by the controller can intercept, retain and store information of any citizen in the ground of national security, integrity and secure of sovereignty of the nation.

3. Domestic Protection of Privacy Rights in Bangladesh

Forthrightly speaking, the provision of 'right to privacy' has neither been inserted directly under the Constitution of the People's Republic of Bangladesh nor have any separate legislation in Bangladesh. However, it does not mean that, Bangladesh Constitution is

12 See: Sec. 2(7) of the Information and Communication Technology (ICT) Act- 2006 [Act No. 39 of 2006] which reads- "...*electronic record*" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche..."

13 According to Sec. 46 of the ICT Act 2006:

"(1)...If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information to be transmitted through any computer resource.

(2) The subscriber or any person in charge of a computer resource shall, when called upon by any agency to which direction has been issued under sub-section (1) of this section, extend all facilities and technical assistance to decrypt the information...."

14 Alam, A. M. Jahangir, "*Understanding Cyber Law In Bangladesh*", Dhaka: University Publications, 2013 at 136.

reluctant to recognize the importance of privacy rights over its citizens. Furthermore, it can instead be interpreted as a subset to a stupendous fundamental right.¹⁵

More specifically, the constitutional provision of the “*protection of home and correspondence*” as stated in Article 43¹⁶ of Bangladesh Constitution can also be treated as a legal protection for privacy right. Another constitutional provision recognised as fundamental rights such as: ‘*Protection of right to life and personal liberty*’¹⁷ which has been inserted under Articles 32 of the Bangladesh Constitution, could have similar values of right to privacy in Bangladesh. In fact, this kind of constitutional provisions have already got similar values of right to privacy in many other countries.¹⁸ To illustrate this, in India, the right to life and liberty as stated under Art. 21¹⁹ of the Constitution of India (*Bharatiya Samvidhaan*) 1949, has taken into account as similar effect for the ‘right to privacy’ of every individual and this had been proven in the case of *Kharak Singh vs. State of Uttar Pradesh* [1963] AIR SC 1295, where the learned Judge *Subba Rao* held that:

*“...If physical restraints on a person’s movements affect his personal liberty, physical encroachments on his private life would affect it in a larger degree. Indeed, nothing is more deleterious to a man’s physical happiness and health than a calculated interference with his privacy. We would, therefore, define the right of personal liberty in art. 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions to encroachments are directly imposed or indirectly brought about by calculated measures...”*²⁰

15 Zulhuda, Sonny., “Right to privacy: Development, Cases and Commentaries” in *Constitutional Law and Human Rights in Malaysia- Topical Issues and Perspectives*, edited by Mokhtar, Khairil Azmin., (Malaysia: Sweet & Maxwell Asia, 2013) at 459.

16 Article 43 of the Constitution of the People’s Republic of Bangladesh states as-
 “...Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health-
 (a) to be secured in his home against entry, search and seizure; and to the privacy of his correspondence and other means of communication....”

17 Article 32 of the Constitution of the People’s Republic of Bangladesh states as: “...No person shall be deprived of life or personal liberty save in accordance with law....”

18 Khan, Md. Zubair Kasem., “Privacy Issues In Electronic Surveillance In Malaysia: A Comparative Analysis Between Common Law And The Shaī’ah” (MCL dissertation, International Islamic University Malaysia, 2015).

19 See: The Constitution of India (*Bharatiya Samvidhaan*) 1949, Article 21 reads: “No person shall be deprived of his life or personal liberty except according to procedure established by law.”

20 *Kharak Singh v. State of Uttar Pradesh*, [1963] AIR SC 1295.

Moreover, this notion of right to privacy has got further constitutional recognition under the rubric of right to life and liberty in the case of *Gobind vs. State of Madhya Pradesh* [1975] AIR SC 1378 and *R. Rajagopal vs. State of Tamil Nadu* [1995] AIR SC 264. Furthermore, in the recent case of *R. Rajagopal* where the Supreme Court Judge, *B.P. Jeevan Reddy* expounded this concept of privacy right by saying that: certain privacy related rights such as ‘individual privacy rights’, ‘privacy of his family’, ‘child bearing’, ‘marriage’, ‘procreation’, ‘motherhood and education’ should be ensured and the violation of these rights could be claimed under Art. 21 of the Constitution Of India 1949. In addition, in *Gobind*²¹ case, the learned judge of the Supreme Court *Mathew, J.* implicitly accepted the existence of privacy rights guaranteed under the rubric of Art. 21 of the Constitution of India.

As we have mentioned earlier, unlike some developed countries like- the United States, the United Kingdom or the European Union, Bangladesh could not reach up to that á la level of standardized statute for data protection and digital privacy comprehensively. However, the words: ‘confidentiality’ and ‘privacy’ have been inserted under the Information & Communication Technology (ICT) Act- 2006 [Act No. 39 of the year 2006] to provide legal protection of data and electronic records. In fact, these terms are used to give protection of data confidentiality and privacy by shielding unlawful intrusion or interference over any electronic record, book, register, correspondence, information, document or other material of an individual. To illustrate, Sec. 12(d) of the ICT Act- 2006 confers authority of the government to make effective rules to control processes and procedures of digital signatures for the sake of assuring integrity, security and confidentiality of electronic records and payments and notified this either by ‘official gazette’ or ‘electronic gazette’. Sec. 12(d) of the ICT Act- 2006 says that:

“... The Government may, by notification in the Official Gazette and in additionally optionally in the Electronic Gazette, make the following rules (all or any of them) to prescribe for the purposes of this Act—

... ..
(d) the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records and payments; ... ”

21 *Gobind vs. State of Madhya Pradesh* [1975] AIR SC 1378. Here the learned Supreme Court Judge Mathew, J. Held that: *“...The Right to Privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right...”*

Correspondingly, Sec. 63 has been inserted under the said Act-2006, as tool to save the right to digital privacy; which discuss specifically, the punishment for disclosure of confidentiality and privacy. According to Sec. 63 of the ICT Act 2006:

“...Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence....”

4. Implication of E-Surveillance VS. Conservation of Digital Privacy Rights in Bangladesh: In Reality (?)

However, the practical enforcement scenario of this ICT Act- 2006 in Bangladesh is pretty awful and controversial due to the random violation of some constitutional as well statutory rights that ensured under this enactment. To illustrate, the government has purchased surveillance software²² from a private European company which allows the country's intelligence and law enforcement bodies to remotely intercept audio, video and written communications from privately owned computers.²³ Not only that, the country's leading six mobile phone companies have paid for a multi-million dollar 'upgrade'²⁴ to the government's mobile phone surveillance system which allows intelligence and law enforcement authorities to directly record thousands of ongoing mobile phone conversations. In fact, the current mobile phone surveillance system, which has been operational for over five years, was purchased from 'Nokia Siemens Network' and this system provides the government's

22 The main 'surveillance malware' software license that Bangladesh authorities have purchased from the German company (FinFisher) is called 'FinSpy'. According to the surveillance expert- 'FinSpy', once installed, can take control of a targeted computer, and through 'control and command servers' allows agent to intercept and record skype conversations, instant messaging, emails, and 'silently' extract files even if they are encrypted.

23 David Bergman., "Surveillance In Bangladesh - Govt Purchased Tk 8.2cr Software To Spy On Private Computers", retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-govt.html>.

24 The upgrade, which will also allow greater access to mobile phone messages sent through e-mails and social networking sites, is being provided by the German company, 'Trovicor', one of the world's leading suppliers of high end surveillance equipment and monitoring centers. See: David Bergman., "Surveillance In Bangladesh - Phone Operators Pay For Govt's Surveillance System Upgrade", retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-phone.html>

‘National Monitoring Centre’ the capacity to record as many as 20,000 mobile phone conversations at any one time.

It is also important to note that, mobile phone operators are required (according to the terms of retaining operating license) to keep copies of all SMS messages sent by their subscribers for at least six months so that, they can be easily accessed by intelligence and law enforcement agencies.²⁵ In addition, the operators keep all ‘Call Related Information’, which includes details of all calls to and from a mobile phone, including the geo-location of the phone when the conversation took place.²⁶ It is gruesome to mention that, any one of nine state agencies (such as: the Police, the Rapid Action Battalion (RAB), the National Security Intelligence *et-cetera*) can contact phone operators and ask for SMS’s and other call related information involving any mobile phone number, and the operators are required to provide the information without seeking information on the purpose of the request.²⁷

It is also worthy to signify that, the figure of budget for purchasing these high-tech softwares, installation and upgrading thereto is pretty astounding. In particular, in case of purchasing ‘*FinSpy*’, this cost amounting to € 831,060 (equivalent to Tk 8.2 crore) from German company *FinFisher*. Not only that, approximately € 20.1 million (equivalent to Tk18.5 crore) has been spent by Bangladesh government (since December 2012) and the leading mobile phone operators respectively only to upgrade surveillance software from another German company *Trovicor*.²⁸ Furthermore, the Rapid Action Battalion (RAB) is seeking to purchase a powerful mobile spy tool, known as an ‘*IMSI catcher*’²⁹ which can obtain details of all mobile phone numbers operating in a particular locality.

Based on the above-mentioned synopsis of attempts taken by the government as well as law enforcement agents, it is pertinent to opine that, the connotation digital privacy rights has got less preference than conducting e-surveillance over her citizens, when it comes to the question of national security. It becomes by far gruesome, when some constitutional

25 David Bergman., “Surveillance In Bangladesh - Telecom Operators Retain 6 Months Of SMS, Other Info, For Law Enforcers”, retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-telecom.html>.

26 Ibid.,

27 Ibid.,

28 Ibid., David Bergman., “Surveillance In Bangladesh - Govt Purchased Tk 8.2cr Software...”

29 The term ‘IMSI catcher’ stands for ‘*International Mobile Subscriber Information*’ which allows [law enforcement authorities] to indiscriminately gather data from thousands of mobile phones in a specific area and at public events such as political demonstrations and so on. See also: David Bergman., “Surveillance In Bangladesh - RAB Seeking Purchase Of Mobile Phone Spy Tool”, retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-rab-seeking.html>.

protections under the rubric of fundamental rights (such as ‘right to life’, ‘right to liberty’, ‘freedom of movements’ and ‘protection of home and correspondence’) have been curtailed owing to the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement. At this point of departure it is undeniable that, this statutory development made recently raises a legitimate concern that, by overruling the supreme constitutional rights of ‘Personal Liberty’, ‘Freedom of Movement’ and ‘Protection of Home And Correspondence’ by the provisions under the Information & Communication Technology (ICT) Act- 2006 [Act No. 39 of the year 2006], the concept of ‘privacy rights’ becomes a fanciful and mythological illusion for the citizens of Bangladesh.

5. Proposal for Policy Recommendations

Paying attention to the present context of Bangladesh, it is indubitable that the concept of individual privacy right is not carefully ensured before the latest legislation development (such as: the Information & Communication Technology (ICT) Act- 2006 [Act No. 39] of the year 2006) and the decisions of the courts. Therefore, an attempt to lay down such a comprehensive guideline is timely and necessary.

At this juncture, this paper suggests several points of concern arising especially from the Security Offences (Special Measures) Act 2012 and the Prevention of Crime (Amendment and Extension) Act 2014, that can be taken to mitigate the problem between executing electronic surveillance and upholding privacy rights:

- i. *Firstly***, it is pertinent to point out that unnecessary collection of any information over an individual by any authority (either public or private) could lead to contravene individual’s privacy right. To illustrate, to buy a new car from car-showroom, it may be relevant for the seller to take note about the name and personal addresses including the tax-related documents of his prospective clients, however, it is absurd to ask about his client’s marital status, employment description, criminal records or physical conditions because it does not really have any practical effect for the car-showroom proprietor, unless there is a clear justification under certain statutes. Same goes to any mobile operator for the purpose of SIM card registration.
- ii. *Secondly***, the law enforcement agents of Bangladesh have purchased surveillance software (with the approbation of the Government) from developed countries which allows them to remotely intercept audio, video and written communications from privately owned computers. This creates some controversy in the ground of the protection of privacy rights. However, it is astounding that, there is no such guideline stated under

the ICT Act 2006, as to what extent and to whom it shall apply. Therefore, there is an urgency of adopting a specific legislation through parliament for the protection of personal data/information of the citizen of Bangladesh. This kind of legislations has already been adopted by a number of countries, like: “*The Data Protection Act- 1998*” in the UK and “*The Personal Data Protection Act- 2010*” in Malaysia.

- iii. **Thirdly**, an individual enactment to be known as “Privacy Act” should be adopted in Bangladesh under which individual privacy rights should be shielded. This kind of legislation has already been embraced by a number of countries like: *Privacy Amendment (Private Sector) Act 2000* (Act No. 155) in Australia; *Privacy Act* (R.S.C., 1985, c. P-21) in Canada; *Privacy Act 1993* (Public Act 1993 No 28) in New Zealand; *The Privacy Act of 1974* (5 U.S.C. § 552a) in the United States and so on. Even though, Bangladesh has already adopted *Information and Communication Technology (ICT) Act- 2006*, it mostly regulates the legal recognition and procedure for implementation of rules of relevant subject of Information and Communication Technology. Undoubtedly, this ICT Act could not fulfill the demand of individual privacy rights for the citizen of Bangladesh exhaustively. Therefore, there is a dearth of having an individual instrument for the protection of privacy rights in Bangladesh.
- iv. **Last but not least**, the government should avail a standard and acceptable roadmap for reconciling privacy rights under the rubric of the provisions of human rights protection in line with the conventions of ICCPR and the UDHR in Bangladesh.

6. Conclusion

The research hypothesizes that there is an urgent need for the government as well as the legislative body to think carefully and take necessary steps to adopt such inalienable principles that is proposed by the international human rights agent for the protection of privacy rights of every individual regardless of race, sex, colour, religion within Bangladesh. It is also important to note that, there is no such guideline specifically for the protection of data privacy for the citizens of Bangladesh at this moment, whereas this kind of legislations is available most of the developed countries in this world. Therefore, there is an immediate necessity to evaluate the newly adopted ICT Act- 2006 and brought into a reconciliation so that, implementation of electronic surveillance for the purpose of national security will not necessarily defeat the individual privacy rights.

References:

- Ahmed, B. Nazir. (2013). The recent Skype scandal and its impact on the Apex Judiciary of Bangladesh. Retrieved on January 03, 2013, from <http://newsfrombangladesh.net/new/highlights/5977-the-recent-skype-scandal-and-its-impact-on-the-apex-judiciary-of-bangladesh>.
- Alam, A. M. Jahangir. (2013). *Understanding Cyber Law in Bangladesh*. Dhaka: University Publications.
- Amsterdam, Anthony G. (1974). Perspectives on the Fourth Amendment. *Minnesota Law Review*. Vol. 58.
- David, Bergman. (2015). Surveillance In Bangladesh - Govt Purchased Tk 8.2cr Software To Spy On Private Computers. Retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-govt.html>.
- David, Bergman. (2015). Surveillance In Bangladesh - Phone Operators Pay For Govt's Surveillance System Upgrade. Retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-phone.html>
- David, Bergman. (2015). Surveillance In Bangladesh - RAB Seeking Purchase Of Mobile Phone Spy Tool. Retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-rab-seeking.html>.
- David, Bergman. (2015). Surveillance In Bangladesh - Telecom Operators Retain 6 Months Of SMS, Other Info, For Law Enforcers. Retrieved on 15 July, 2015 from <http://bangladeshpolitico.blogspot.com/2015/02/surveillance-in-bangladesh-telecom.html>
- Garner, Bryan A. (2009). *Black's Law Dictionary (9th ed.)*. WEST Publishers.
- Gray, David. & Citron, Danielle. (2013). The Right to Quantitative Privacy. *Minnesota Law Review*. Vol. 98(62).
- Hassan, M. Mahdy. (2015). Violation of Right to Digital Privacy. Retrieved on November 20, 2015 from <http://archive.thedailystar.net/beta2/news/violation-of-right-to-digital-privacy/>.
- Khan, Md. Zubair Kasem. (2015). Privacy Issues in Electronic Surveillance in Malaysia: A Comparative Analysis between Common Law and the *Shari'ah*. Unpublished MCL dissertation, International Islamic University Malaysia.
- Lask, Lawrence. & Parkes, Walter F. (Producer), & Robinson, Phil. A. (Director). (1992). *Sneakers* [Videotape]. United States: Universal Studios.

- Peterson, Julie K. (2001). *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications*. The United States of America: CRC Press.
- Smale, Alison. (2013). Surveillance Revelations Shake U.S. *The New York Times*. Retrieved on August 25, 2013 from http://www.nytimes.com/2013/08/26/world/europe/surveillance-revelations-shake-us-german-ties.html?_r=0.
- Tatum, Christine. (July, 2002). Navigators Hit Road in Digital Quest. *The Chicago Tribune*. Retrieved on February 10, 2014 from http://articles.chicagotribune.com/2002-07-29/business/0207290009_1_mapquest-charles-dolan-digital-maps.
- Zulhuda, Sonny. (2013). Right to Privacy: Development Cases and Commentaries. In Khairil Azmin Mokhtar (eds.), *Constitutional Law and Human Rights in Malaysia- Topical Issues and Perspectives*. Selangor: Thomson Reuters Malaysia Sdn. Bhd.