

Enhanced Forms of Criminal Investigation: Analysis on Its Potential Risks to Human Rights

Molalign Asmare Jemberie

College of Law, Dire Dawa University, Dire Dawa, Ethiopia

Email: amamolasma@yahoo.com

Received 13 December 2015; accepted 28 February 2016; published 2 March 2016

Copyright © 2016 by author and Scientific Research Publishing Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

Criminal investigation is the bedrock in fact inquiry for the criminal justice system. In the contemporary world, countries use technologically enhanced criminal investigation techniques for the alleged crime or for the probable crimes. The current trends show that those enhanced forms of criminal investigation techniques have been used in more extended manner. Such extended applications of those techniques have become the threats to individual rights such as right to privacy, freedom of expression, the right to freedom of association and assembly, the right to freedom of movement and the due process rights. This paper analyzes the available justifications, compatibility and ethical sides of these enhanced forms of investigating techniques by police or investigative organs. Moreover, it also critically analyzes the potential threats and implications of these enhanced forms of criminal investigations on the certain basic individual human rights. Under the umbrella of enhanced criminal investigation techniques, there are various special techniques. The scope of this paper is not to deal with the specific nature of each technique, rather it is limited only to the general behavior or characteristics, their underlying rationales and the possible threats on the rights of individuals.

Keywords

Enhanced Criminal Investigation, Rationales, Right to Privacy, Freedom of Expression, the Right to Freedom of Association and Assembly, the Right to Freedom of Movement and the Due Process Rights

1. Introduction

Criminal investigation is the bedrock in fact inquiry for the criminal justice system. Determining which investi-

gation tools to be used depends on a variety of factors, including the nature of the alleged violations, the type of investigation to be conducted and the available resources.

The advances of technology have played a great role in changing the techniques and tactics of criminal investigation. Criminal investigation can be reactive if it is triggered after a certain criminal wrong is committed or it can be also proactive, which is concerned much more in preventing the commission of crimes in advance with the help of sophisticated technology (Tong et al., 2009). Nowadays, the advancement of technology and the sophistication of crimes oblige many countries to use special investigative techniques in their investigation process of crime.

The most remarkable fields of technologies that have been usually applied and played a prominent role in criminal investigations are, *inter alia*, “information science”; “molecular biology”; and “social science research”¹ (U.S. Congress, 1988). These technologies, obviously, are undisputable in enhancing law enforcement agents’ ability to identify offenders and capture suspects (U.S. Congress, 1988). Put differently, in investigating crimes, identifying suspects, and gathering evidence, special technologies address the quest for easy solutions for law enforcement works and criminal investigations.

The process of criminal investigations, however, has a high potential area for abuse of procedure (Harfield, 2010). In the contemporary world, countries use technologically enhanced criminal investigation techniques for the alleged crime or for the probable crimes. These advances of technology have its pros and cons to the administration of justice, mainly in crime investigation. The current trends show that those enhanced forms of criminal investigation techniques have been used in more extended manner. Such extended applications of those techniques have become the threats to other rights. However, the scopes of applications of these techniques are required to be clear and legally limited. Furthermore, it is necessary to make a clear demarcation as to which crimes or potential threats should be investigated by such kinds of investigative techniques.

Most of the time, countries engaged in special criminal investigation techniques such as various forms of surveillance, eavesdropping, undercover agents, biometrics and the like. These enhanced forms pave the way for silent and invisible intrusions on the privacy of the individuals (Scheb, 2011; Cavoukian, 2008). Such secret and invisible nature limits the individuals to show before the court that they are under some kind of surveillance so as to get judicial remedies in case of violations of due process rights (Scheimin, 2009). The required check and balance that is the bedrock for the separation of power principle would be eroded.

The practice has caught a great attention and trigger a hot forms of debate in making use of these special investigative techniques and their ethical concerns (Mullikin & Rahman, 2010). There are countries where their law enforcement officials have proposed the prohibition to utilization of communication technologies that are more difficult to intercept (Mullikin & Rahman, 2010).

Thus, this paper analyzes the available justifications, compatibility and ethical sides of these enhanced forms of investigating techniques by police or investigative organs. Moreover, it also gives an emphasis as to the potential threats and implications of these enhanced forms of criminal investigations on the certain basic human rights such as right to private life, right to freedom of expressions and other related rights as well.

Under the umbrella of enhanced or special investigation techniques, one may get various techniques of surveillance, biometrics, undercover agents and the like. The scope of this paper is not to deal with the specific nature of each techniques, rather it is limited only to the general behavior or characteristics of the selected techniques especially their underlying rationales and the possible threats on the rights of individuals.

2. Enhanced Forms of Criminal Investigation

2.1. Introduction

Today, crime is being committed in more sophisticated methods and in a more organized form. In addition, new types of crime are continuously occurring. Criminal investigation is, essentially, the process of answering questions as to how, where, when, why, and by whom a crime has been committed. For these purpose, investigative law enforcement officers are required to collect information from various sources and arrive at a certain coherent

¹“Information science”—is innovation of advanced information technology such as “broad array” computers and telecommunication technologies including surveillance technology and played great role in enhancing criminal investigation through accumulation and sharing of necessary information to investigative officers. “Molecular biology”— is the result of new biology innovation, basically studying the chemical and genetic basis of human nature or behavior or mental set up or functioning for identification, testing and screening, using body fluids or tissue for criminal investigation process.

conclusion on a given event (Ask, 2006). To effectively deal with such situations, investigative organizations are also getting systematized and scientific in terms of organization and investigation methods.

In addition to conventional and enhanced, criminal investigation can be also classified as reactive or proactive investigation. Until recently, the highly dominant model of criminal investigation was a reactive kind of investigations. This kind of criminal investigation is always relies on the past history so that it has been highly criticized by its retrospective nature (Tong et al., 2009). Whereas proactive criminal investigation mostly used when the law enforcement agents predict a crime is going to be committed, detect and prevent the community from the effects of crime proactively (Tong et al., 2009). This investigative technique is highly assisted by advanced technologies. However, one should note that though reactive criminal investigation presupposes the commission of crime, it does not mean that enhanced investigative techniques are inapplicable. What makes it different is, its scope of utility i.e. it utilizes less in scope of special investigative techniques as compared to proactive one.

In the contemporary world, the most commonly used special investigative techniques are, *inter alia*, technical aids (e.g. body scanners, iris-scanner, buss, probes, cameras, electronic facial ID software, Automatic Number Plate Recognitions; operational policing tools and systems; profiling techniques such as crime mapping, geographical profiling, offenders profiling, psychological and behavioral profiling); surveillance techniques (e.g. devices like CCTV, drone surveillance, phone tapping, wiretapping, human or electronic eavesdropping, communication data surveillance, pen register, trap and trace device, interception of communication; traffic data surveillance; covert operations such as directed surveillance, intrusive surveillance, electronic surveillance, and surveillance logs); and sources of information (e.g. intelligence database like Automated Fingerprint Identification System, DNA Database etc...). So according to the nature of the alleged crimes, countries may choose the relevant available investigative tools for their crime detection, prevention and investigation.

For the sake of this paper, it is helpful to see the general nature of some enhanced investigative techniques such as “surveillance”², “wiretapping”³, “eavesdropping”⁴, and the like (Caremen, 2010; Hewitt, 2008). Basically, applying these kinds of special investigative tools may increase the ability of the government to observe, control or intervene on the commission of crime; may enable the government to investigate at a distance or out of sight of both of the subject and concerned public interest groups (Herbert, 2011).

In most cases, the applications of those techniques are blurred. But the most common crimes which are subjected to such type of investigation or detection are: terrorism, organized crimes, money laundering, corruption, drug dealing, hijacking, espionage, treason, white collar crime, human trafficking and the like (Hall, 2004; Stutzer et al., 2010; Kaplan, 2012; Bloss, 2007). But it does not mean that the utilization of those techniques always limited only to those serious crimes though the substantive seriousness of crimes may vary from jurisdiction to jurisdiction. Mostly, it is highly influenced by the national security matters of a given country and the safety of community at large.

2.2. Rationales

Many of technological innovations can offer significant social benefits in general and the reduction of crime and just and equitable administration of justice in particular. Countries may put different justifications to make use of these enhanced forms of criminal investigative techniques on a given circumstance. The writer of this paper chooses as a matter of concern three basic rationales i.e. technological innovations, security, and crime prevention.

2.2.1. Technological Innovations

There are basically two types of technological innovations that can be identified as information-based technology

²Surveillance is the use of electronic devices so as to monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording any of this. This includes surveillance with the assistance of a surveillance device. This type of search and seizure may take various forms such as stationary surveillance, technical surveillance or electronic surveillance which generally includes eavesdropping, telephone tapping, “bugging”, Closed-Circuit Television (CCTV), GPS tracking, electronic tagging, and internet and computer surveillance. The most common types of electronic surveillance are aural surveillance (“bugging”) which includes telephone intercepting and listening device; and visual surveillance which can be covert, where it is carried out without the notice of the subject, or overt, where the subjects are aware that device are in use.

³Wiretapping is an intelligence gathering procedure used to obtain information without being detected. This activity involves tying into a wire or other conductor which is used to transmit some form of message. Mostly it is categorized under surveillance. Wiretapping can be classified into four, i.e. hardwired, soft, record and transmit wiretapping.

⁴Eavesdropping—It can be human person or equipments that is used to listen the conversations of individuals under walls or windows or the house so as to get the required information.

innovations (which is called as soft technology) and material-based technology (which is called as hard technology) (Byne et al., 2011).

The sophistication of crime commission and the challenge to investigate those crimes on one hand and the opportunity of hard or soft technological innovations that can ease such challenge on the other, create conducive environment for criminal investigator and forensic practitioners of a given country. Factually, traditional investigation techniques do not compete much better against sophisticated crimes.⁵ The advancements of surveillance technologies, for instance, have supplied law enforcement with numerous new investigative tools, tactics, and methods. These innovations have been the source of incredible simplifications and ease, providing investigators with time and effort saving advantages to more traditional painstaking investigative tactics. By nature, the efficacy and efficiency of these enhanced forms of investigation techniques in fighting modern crimes with modern technology would be one of among the other rationales. Thus, this advancement created the opportunity to law enforcement and intelligent agents to utilize those enhanced techniques for their careers.

2.2.2. National Security

Most countries may take different security measures in seeking to safeguard national security and community safety. In order to prevent those threats which pose on a given country, advanced technologies can be used in proactive and/or reactive investigative techniques. These techniques, for instance, can be justified on future terrorist acts and to obtain foreign counterintelligence information about the individuals' and groups engaging in, or preparing to engage in terrorist activities on a certain state (Stutzer et al., 2010).

Obviously, these days, criminal organizations are more sophisticated and dynamic than ever before. The challenges for law enforcement agents are to be prepared for this increasing sophistication in order to reduce the impact of criminal activities on a given state's communities. To this end, countries' law enforcement agencies and intelligent agencies need forward looking, assertive and comprehensive strategies to counteract the threat of multinational crime such as terrorism, money laundering, organized crime, hijacking, drug trafficking, and the like (United Nations Office on Drugs and Crime, 2011). Due to these reason, it is common to see while countries apply the required techniques, *inter alia*, electronic surveillance, electronic interception including wiretapping and Global Positioning System (GPS).

Moreover, the United Nations Convention against Transnational Organized Crime specifically endorses, where it deems appropriate, the state party to apply special investigative techniques such as electronic or other forms of surveillance and undercover operations by their competent body with in their jurisdictions (UN Conventions against Transnational Organized Crime, 2004). Therefore, national security issues are the largely used kind of justifications that states usually claim to use the available special investigative techniques as a protective and detective measures.

2.2.3. Crime Prevention

Special investigative tools, which are the result of technological advancement, can be used to prevent crime and to improve the performance of the police. The growth of crime and the emerging new technological innovations has brought with the parallel phenomenon of expansion and specialization of police forces (Isnard, 2001).

Crime prevention, in its present usage is a generic term of vaguely wide term. As the crime prevention trends of different countries shows, it refers to a variety of police actions ranging from patrolling the streets to surreptitious surveillance and under cover activities (Cohen, 1982).

Moreover, it is virtually impossible to organize a complex crime without communicating over public networks, and this is particularly true where there is an international dimension, as is increasingly the case. Interception can exploit this weakness in the criminal structure, providing law enforcement officers with an opportunity to gather intelligence on crimes as they are being planned and providing an invaluable insight into the thoughts and intentions of the criminal. In many countries, law enforcement officers and intelligent agents are highly proposed their government in order to ban the utilization of communication devices that are more difficult to intercept such as smart phones (Tong et al., 2009).

A highly enhanced intelligence functions and special investigative techniques are, thus, used as an instrument or tools at the guise of the prevention or detection of crime or to prevent public disorder. Therefore, crime prevention strategies can be taken as one of the justification to use enhanced technologies for criminal investigation among others.

⁵See Special Investigative Tools to Combat Transnational organized Crime, 116th International Training Course Reports of the Course, Resource Material Series No.58, at 228.

3. Potential Threats of Enhanced Forms of Criminal Investigations

Since human rights are interrelated and interdependent, right to privacy, in addition to a right in itself, serves as a basis for other right. Other rights, such as to freedom of expression, the right to freedom of association and assembly, the right to freedom of movement and the due process rights could be affected jointly or independently where law enforcement officials apply those special investigative techniques.

3.1. The Right to Privacy

Right to privacy is a fundamental human right that can be understood as the presumption that individuals should have an area of self-directed development, relations and liberty with or without interactions with others and free from state and other persons' interventions (Mullikin, 2010). The right to privacy is not an absolute right which is not subjected to any restrictions or limitations. Under international human rights instruments especially under Article 17 of International Convention on Civil and Political Rights (ICCPR), right to privacy is stated as: 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. Even though Article 17 of the ICCPR is a binding treaty provision at the universal level and does not catalogue permissible limitation (Sepulveda et al., 2004), one should note that there are situations where state party or countries have a legitimate power to limit the right to privacy under international human rights law. A given state, for instance, can derogate the right to privacy in accordance with Article 4 of the same convention. However, what is absolutely prohibited here is illegal or unlawful and arbitrary interference on such right to privacy of individuals.

However, at the international level, there is no thorough set of legal safeguards that deals with or that strike the balance between the use of those enhanced investigative tools for crime prevention, detection and investigation on one hand and the protection of the private life of individuals and other related rights on the other (Stutzer et al., 2010).

However, due to the threat of crimes certain serious such as terrorism, money laundering, organized crime, hijacking, and the like, states claim that their ability to prevent and investigate such crime is closely related to augmented surveillance power. Let alone the privacy right of the suspected individuals, the utilization of those special investigative techniques would affect the private life of any law-abiding individuals by exposing their private life or communications in unintended manner (Gene D. Park, 2006). In the prevention and investigation of such crimes, states utilize multiple techniques which might violate an individual's right to privacy. However, surveillance, whether electronic or otherwise; interceptions of telephonic, telegraphic and other forms of communication; wire-tapping and recording of conversations have been prohibited by the Human Rights committee General Comment (UN Human Rights Committee General Comment 16, 1988). But the current practice of states varies as to their means to measure the necessity, proportionality and reasonableness of their interference due to the absence of international guidelines on minimizing the risk to privacy. This in turn might create the differing approaches and conceptions as to the right to privacy.

States' conception of privacy is alarmingly developed from time to time. In USA, for example, as it is stated by the Supreme Court decision by the case of *Katz v. United States* (1967), which is the land mark case for the issue at hand, the decision had come up with new jurisprudence concerning protection of privacy from the *old property approach* towards the *new privacy approach* (Ferdico et al., 2009). According to the holdings of the court, any form of electronic surveillance, including wiretapping that violates "*a reasonable expectation of privacy*"⁶, constitutes a search that required warrant under the Fourth Amendment (Del Carmen, 2009). The prohibition against unreasonable search and seizure, thus, is not limited to homes, office buildings, or other enclosed space; rather it applies even in the public places where a person has a "reasonable expectation of privacy".

Therefore, if a certain application of special investigative techniques, be it various forms of enhanced investigation techniques or others, violates the reasonable expectation of privacy of the subjected individual, we can safely argue that such act is unlawful and arbitrary interference of the right to privacy. The writer of this paper believes that the reasonable expectation of privacy test would be the best solution even for future innovation of technology that can affect the private life and integrity of individuals.

⁶According to such landmark case, an individual has a reasonable expectation of privacy where he/she, by his or her conduct, has showed a subjective expectation of privacy i.e. he or she has shown that he or she seeks to preserve something as private; and such subjective expectation of privacy, objectively, is recognized by the society as reasonable and justifiable expectation.

3.2. The Right to Freedom of Expression

Under the present international conventions, there are state obligations to respect and protect the right to freedom of expression. Article 19 of both the Universal Declaration of Human Rights (UDHR) and International Covenants on Civil and Political Rights (ICCPR) establishes the freedom of opinion and expression. Most international and regional treaties enshrined the permissible limitation of the right to freedom of expression. According to Article 19 of the ICCPR, such restrictions are required to be provided by law; serve a legitimate aim i.e. in order to respect the rights and reputation of others, for the protection national security, or public order or public morals or health; and such restriction should meet a high standard of necessity.

However, the right to freedom of expression and its internationally accepted limitations could be distorted by various measures taken by the governments. One of the most barriers to the right to freedom of expression can be measures taken by law enforcement agents while investigating crimes such as electronic eavesdropping, covert surveillance or wiretapping. For example, if an individual subject to such kind of special investigation is being aware in any ways that his or her communications or acts would be listened to or recorded by the law enforcement agents, he or she is going to be restricted from expressing his or her ideas. This in turn affects the individuals' right to freedom of expression beyond the standard restriction set by international instruments. However, whether a given individual is being aware of or not, the mere act of the governments without the permitted limitations pose a risk on individuals' right to freedom of expression.

3.3. The Right to Freedom of Association and Assembly

One of the rights that can be affected by the technology dependent criminal investigation techniques is the right to freedom of association. "The right to freedom of association allows individuals to join together to pursue and further collective interests in groups such as political parties, NGOs and corporations" (Sepulveda et al., 2004, 2nd). Saving permissible restriction on the right to freedom of association and assembly, such right includes the right to form and join associations freely. Thus, in order to the full enjoyment of the right, associations must not be subjected to extreme and unnecessary intervention by the governments (Sepulveda et al., 2004).

In criminal investigation process, however, the right to freedom of association and assembly are threatened, for example, by the use of surveillance. These freedoms often require private meetings and communication to organize individuals for their respected association or assembly from the face of governments (Isnard, 2001).

Expanded use of these surveillance powers may led to abuse when the law enforcement agents or intelligent agencies have used these techniques so as to follow and monitor at a distance the internal activities, behavior, disciplines of the members of such association. The individual's right to freedom of association and assembly, thus, would be restrained by the governments' intrusive means of investigation mechanisms so that the protection of their private meetings might be eroded.

3.4. The Right to Freedom of Movement

The right to freedom of movement comprised the right and ability to move and choose one's residence freely and in safety with in the territory of the state, irrespective of the purpose of the move (UN Human Rights Committee General Comment No.27, 1999). It also includes the right to leave any country and return to one's own country. It is closely related to liberty and security of person, which guarantees freedom from any arbitrary arrest and detention. But one should note that like other rights, it is not an absolute right i.e. it is subjected to certain permissible restrictions like freedom of expression and freedom of association and assembly (Klein, 2013).

The right to freedom of movement can be highly affected by special investigative techniques. The use of secret watch list monitoring (no-fly selectee list)⁷, excessive data collections and sharing and imposition of intrusive scanning devices or biometrics all create barriers to the mobility of individual once they are listed or under surveillance.

3.5. The Due Process Right

The due process right, in the broader sense, can be understood as the right to be treated fairly, efficiently and effectively by the administration of justice. This right puts restrictions on criminal proceedings so as to safeguard

⁷Such lists, which are usually kept secret, are circulated to airlines and border security officials with instruction to detain and question any passenger with a certain name.

fundamental fairness and justice (Sepulveda, 2004).

One of the most serious threats of enhanced forms of investigation techniques such as surveillance measures is that they may encroach the due process guarantees of the individuals. The secret nature of such investigation techniques, which hindered the subjected individual to show the unlawful and arbitrary interference on his or her fundamental rights before the court, pose a great challenge on individuals access to judicial review.

So, it is hardly possible to show such unlawfulness or arbitrariness or unreasonableness of the governments intrusions on the rights of the suspect unless such search and seized information has been brought before the court. As a result, individuals may not be able to appeal to courts for remedy. Such unlawful acts of law enforcement would overrule the very idea of check and balance which is the main goal for separation of power (McCord et al., 2006). Therefore, these techniques may lead to miscarriage of justice and violate the due process rights.

4. Preconditions to Use Enhanced Forms of Investigative Tools

The basic issue of how to use those investigative techniques in line with the rule of law and respect of fundamental human rights cannot be universally addressed in a similar fashion. Rather, it will rely on the legal system, practice and culture of each country. It is necessary, therefore, to strike the balance as to what extent the privacy and other related rights of individuals can be respected while protecting safe from effects of crime.

Basically, for a given criminal justice system to use those investigative tools, with due consideration of the potential threats, it should be covered by a specific laws and empowers a given body to authorize based on the required probable cause and supervise as to the necessity and proportionality of government's measures. For utilization of those techniques to be in accordance with the law, it should be foreseeable, backed up by safeguards against misuse and controlling mechanisms should be established (Mooneh, 2010). Whatever forms of special investigative techniques is adopted, there must exist adequate and effective guarantees against abuse (Mooneh, 2010).

As it has been indicated in the previous section, the absence of the detailed pre-existing legal safeguards that regulate the conditions under which the implementation of those special investigative techniques, has been ensured by adequate legislative control. The special investigative techniques should be adequately defined in the national legislations about the circumstances under which the competent authorities are entitled to the use of those techniques (Council of Europe Recommendation 10, 2005).

Moreover, such legislative guidelines should prescribe the use of those techniques by the law enforcement to the extent of its necessity and appropriateness for efficient criminal investigation. Besides, legislation should also adopt the system of judicial or other independent body prior authorization for the sake of ensuring adequate control of the implementation of those special investigative techniques.

As the practice of some countries clearly reveals, the government must obtain authorization in good faith in connection with all offense for which the permits such special investigation. In this sense the law enforcement needs to be warranted to use such intrusive techniques. Secondly, the prosecutor or law enforcement officers who are in need of such kind of investigation techniques is required to show to the authorizing court that using such investigative techniques is something of last resort due to other investigation procedure have been tried and unable to address the problem; or they are required to prove that ordinary or conventional investigation techniques realistically appear not likely to be successful or very risky (Abramson, 2005; Pikowsky, 2002). Thirdly, the government must support such application with sufficient probable cause that necessitates such kind of investigation. Finally, the government is required to minimize its intrusion on other individuals and on irrelevant actions or communications of the person of special interest (Abramson, 2005).

For law enforcement, for instance under the European Convention on Human Right, to use those special investigative techniques, they have required to set a clear legitimate objectives or aims to restrict the fundamental rights and such restriction must be in all circumstances as necessary and proportional as possible to meet the legitimate objective which the state seeks to achieve (Taylor, 2011). Moreover, there are jurisdictions, for instance, establish the requirement of consent of the party to the conversation i.e. some jurisdictions permit recordings of their discussion with the consent of one party to the conversation and others require the consent of all parties to the conversation (Doyle, 2012).

5. Conclusion

Today, criminal investigation techniques are highly developed than ever before. Criminal investigation can be

reactive if it is triggered after a certain criminal wrong is committed or it can be also proactive, which is concerned much more in preventing the commission of crimes in advance with the help of sophisticated technology. Though reactive criminal investigation presupposes the commission of crime, it does not mean that enhanced investigative techniques are inapplicable. So according to the nature of the alleged crimes, countries may utilize the relevant available investigative tools for their crime detection, prevention and investigation.

There are different justifications for various countries to make use of these enhanced forms of criminal investigative techniques, inter alia, technological innovations, national security, and crime prevention. In the prevention and investigation of crimes, states utilize multiple techniques which might violate an individual's right to privacy. However, these techniques have an intrusive nature on the privacy on individuals and other related rights such as to freedom of expression, the right to freedom of association and assembly, the right to freedom of movement and the due process rights and even affects the principle of separation of powers. It is necessary, therefore, to strike the balance as to what extent the privacy and other related rights of individuals can be respected while protecting safe from effects of crime. Basically, for a given criminal justice system to use those investigative tools, with due consideration of the potential threats, it should be covered by a specific laws and empowers a given body to authorize and supervise as to the necessity and proportionality of government's measures.

Thus, according to its nature and impacts on the rights of individuals, special rules and regulations should be enacted at both international and national level in order to address specific issues of each special investigative technique. Moreover, there should be a clear demarcation between situations in which such special investigative techniques are applicable and situations in which those techniques are not applicable. On top of that countries should have a balanced size and scope of utilization of those special investigative techniques, the investigations should be conducted in way that judicial remedies are available. Therefore, criminal investigation by those special techniques should be utilized in the way that can be subjected to check and balance between the branches of a given government.

References

- Abramson, J. M. (2005). Challenging Federal Wiretaps, Criminal Law Newsletter. *The Colorado Lawyer*, 34, 73.
- Ask, K. (2006). *Criminal Investigations: Motivations, Emotions and Cognitions in the Process of Evidence*. Doctoral Dissertation at Department of Psychology, Goteborg: Goteborg University.
- Bloss, W. (2007). Escalating US. Police Surveillance after 9/11: An Examination of Causes and Effects. *Surveillance and Society, Special Issues on "Surveillance and Criminal Justice" Part 1*, 4, 208-228.
- Byne, J., et al. (2011). *Technological Innovations in Crime Prevention and Policing: A Review of Research on Implementation and Impact*. Voor België: Maklu-Uitgervers.
- Caremen, R. V. (2010). *Criminal Procedure: Law and Practice* (8th ed.). Boston, MA: Wadsworth, Cengage Learning.
- Cavoukian, A. (2008). Privacy and Video Surveillance in Mass Transit System: A Special Investigation Report. Information and Privacy Commissioner, p. 2.
- Cohen, S. A. (1982). Invasion of Privacy: Police and Electronic Surveillance in Canada. *McGILL Law Journal*, 27, 619-675.
- Council of Europe, Recommendation 10 of the Committee of Ministers to Member States on "Special Investigative Techniques" in Relation to Serious Crimes Including Acts of Terrorism, 2005, Para. 1.
- Del Carmen, R. V. (2009). *Criminal Procedure: Laws and Practice* (8th ed.). Belmont, CA: Wadsworth/Cengage Learning.
- Doyle, C. (2012). Wiretapping, Tape Recorders, and Legal Ethics: An Overview of Questions Posed by Attorney Involvement in Secretly Recording Conversation. Congressional Research Service, p. 1.
- Ferdico, J. N., et al. (2009). *Criminal Procedure for the Criminal Justice Professional* (10th ed.). Belmont, CA: Wadsworth/Cengage Learning.
- Hall, D. E. (2004) *Criminal Law and Procedure* (4th ed.). Thomson Delmar Learning, West Legal Studies.
- Harfield, C. (2010). *The Governance of Covert Investigation*. Melbourne University Law Review, Vol.34.
- Herbert, L. C. (2011). Challenging the (Un)Constitutionality of Governmental GPS Surveillance. American Bar Association, *Criminal Justice*, 26, 11 p.
- Hewitt, M. (2008) *Wiretapping: A Necessary for Effectively Combating Terrorism in the 21st Century*. Senior Honors Thesis, Virginia: Honors Program of Liberty University.
- Isnard, A. (2001). *Can Surveillance Cameras be Successful in Preventing and Controlling Anti-Social Behaviors?* (p. 7). Australian Institute of Criminology.

- Kaplan, H. J. (2012). The History and Law of Wiretapping, ABA Sections of Litigation 2012 Section Annual Conference April 18-20, 2012: The Lesson of the Raj Rajarantnam Trial: Be Careful Who's Listening.
- Klein, E. (2013). *Freedom of Movement: International Protection*. Max Planck Institute for Comparative Public Law, Oxford: Heidelberg and Oxford University Press.
- McCord, J. W. H., McCord, S. L., & Bailey, C. S. (2006). *Criminal Law and Procedure for the Paralegal: A Systems Approach*. New York: Thomson Delmar Learning.
- Mooneh, T. (2010). *Special Investigation Techniques*. Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights, *Pace Int'l L. Rev. Online Companion*, at 97, p. 106.
- Mullikin, A., & Rahman, S. M. (2010). The Ethical Dilemma of the U.S.A. Government Wiretapping. *International Journal of Managing Information Technology (IJMIT)*, 2, 32.
- Pikowsky, R. A. (2002). *An Overview of the Law of Electronic Surveillance Post September 11, 2001* (p. 605). Moscow: Law Library Journal, University of Idaho Law Library.
- Scheb, J. M. (2011). *Criminal Law and Procedure* (7th ed.). Boston, MA: Wadsworth, Cengage Learning.
- Scheinin, M. (2009). *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*. Human Rights Council, 13th Session, A/HRC/13/37.
- Sepulveda, M. et al. (2004). *Universal and Regional Human Rights Protection: Cases and Commentaries*. Costa Rica: University for Peace.
- Sepulveda, M. et al. (2004). *Human Rights Reference Hand Book* (3rd ed.). Costa Rica: University of Peace.
- Stutzer, A., et al. (2010). *Camera Surveillance as a Measure of Counterterrorism?* Economics of Security Working Paper 34, Berlin: Economic of Security.
- Taylor, N. (2011). A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance System. *Surveillance and Society*, 8, 455-470.
- Tong, S., Bryant, R. P., & Horvath, M. A. H. (2009). *Understanding Criminal Investigation* (pp. 1-36). Wiley Blackwell, Hoboken, NJ: John Wiley and Sons Ltd.
- U.S. Congress, Office of Technology Assessment (1988). *Criminal Justice, New Technologies and the Constitution* (p. 1). OTA-CIT-366, Washington, DC: U.S. Government Printing Office.
- United Nations Conventions against Transnational Organized Crime, New York, 2004.
- United Nations Office on Drugs and Crime (2011). *Criminal Intelligence: Manual for Analysis*. New York.