(2014) 18 JUUM 9 - 26

Admissibility of Covert Surveillance Evidence: A Prolegomenon

(Kebolehterimaan Keterangan 'Covert Surveillance': Satu Pengenalan Umum)

MD. ABDUL JALIL
ABU HENA MOSTOFA KAMAL

ABSTRACT

This article presents the epistemology of a new but mostly neglected subject 'admissibility of surveillance evidence.' It addresses the complex issues around 'the proper limits of covert surveillance' and 'whether evidence obtained by the public authority in breach of statutory provision should be ruled inadmissible.' Further, it analyses issues that have a profound relationship with 'individual's right of privacy' and 'public authority's duties of conducting surveillance.' In this research much emphasis is placed on case laws as persuasive precedents as there are no adequate statutory laws in some countries like Bangladesh and Malaysia which deal with this subject. It is hoped that the results of this research would attract the attention of policy-makers of some interested countries. It is also hoped that reasonable ethical and legal safeguards should be implemented to protect the rights of the people from future abuse.

Keywords: Surveillance and interception; admissibility of surveillance evidence; right of privacy; intrusion of privacy

ABSTRAK

Artikel ini mengutarakan suatu isu baru tetapi telah lama diabaikan berkaitan kebolehterimaan 'keterangan pemantauan' atau 'surveillance evidence' serta asas, skop dan kesahannya. Ianya menyingkap isu kompleks berkaitan 'had pemantauan rahsia yang dibenarkan' serta 'persoalan samada keterangan sedemikian yang diperolehi oleh pihak berkuasa dengan cara yang menyalahi peruntukan statut harus ditolak.' Artikel ini seterusnya menganalisis isu hubung kait dan perimbangan antara 'hak privasi individu' dan 'tanggungjawab pihak berkuasa untuk melaksanakan tugas-tugas pemantauan.' Dalam kajian ini, penekanan banyak diberikan kepada kes-kes yang persuasif disebabkan ketiadaan peruntukan undang-undang yang mencukupi di negara-negara seperti Bangladesh dan Malaysia yang yang menangani isu ini. Adalah diharapkan agar hasil kajian ini akan menarik perhatian pembuat polisi di negara lain. Adalah diharapkan juga agar perlindungan yang munasabah yang beretika serta mematuhi undang-undang dapat diimplementasikan untuk melindungi hak orang awam daripada dicerobohi.

Kata kunci: Pemantauan dan pengintipan maklumat; kebolehterimaan keterangan pemantauan; hak privasi; pencerobohan privasi

INTRODUCTION

According to Warren and Brandeis, 'Numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops.'[1] This prediction became reality as technology has developed at an unprecedented rate in recent years. In parallel with the rapid and prodigious development of electronics, the surveillance and interception technologies have also improved tremendously. Public authorities, like law enforcement agencies and national security wings are using sophisticated modern equipment for surveillance and interception to eradicate terrorism and hideous crime. Innovative technologies have enhanced their ability not only to track people through their computerised record trail, but also to see through walls, overhear conversations and follow the movement of wrong doers. Satellite photographs, massive millimeter wave detectors or millivision,[2] tubular and parabolic microphones,[3] van eck monitoring device,[4] wiretapping, thermal imaging, mobile phone tracking are examples of some modern surveillance technologies. Nowadays surveillance technologies are increasingly used for detecting and investigating offences. Courts are acknowledging the fact that electronic evidence gathering has significant advantages over more conventional means of obtaining information, such as providing a direct and contemporaneous account of an event, which may avoid many of the threshold evidentiary issues.[5] But many fears that the abrupt use of surveillance technologies could lead to a serious loss of autonomy, endangering people's right of privacy and freedom. It should be mentioned that the development of effective legal and practical safeguards for individual privacy has lagged far behind the pace of technological developments and the uptake of surveillance technologies by both the public and private sector.[6]

Thus the use of modern technologies in performing surveillance and interception tasks are quite vulnerable to the legal dispute. Courts often face difficulties in understanding how the surveillance evidence was derived, processed, and presented when it performs the task of 'weighing the probative value of the information against its potential value' in order to determine admissibility. Here, one has to bear in mind that 'despite the tremendous opportunity for technologies to offer more informed and cost-effective evidence against a crime, the issues of credibility, admissibility, and other evidentiary hurdles are impending the integration of these technologies into the judicial process.'[7] Until scientists and attorneys work together 'to educate tiers of fact to develop protocols for general acceptance, courts will be reluctant to work through the associated complex science and mathematics necessary to assign evidentiary value to the information.'[8]

The word surveillance derived from the French word 'surveiller' which literally means watching over. But, in real life the term is often used for all forms of observation or monitoring, not just visual observation. It is commonly used to describe observation from a distance by means of electronic equipment or other technological means. In a broad sense surveillance is a legal investigative process entailing a close observing or listening to a person in an effort to gather evidentiary information about the commission of a crime, or lesser improper behaviour.[9] In the narrow sense, surveillance is the systematic monitoring of enemy forces using a variety of electronic and optical means as well as other intelligence assets.[10] In modern time, no one denies the essentiality of surveillance in protecting a state's interest. However, its improper use may damage individual's privacy. Therefore, a logical parameter of state surveillance must be determined to protect individuals from 'state authorised' intrusion. Sometimes public authorities' step beyond their powers in performing surveillance which may cause irreparable damage of reputation if the surveillance evidence is inadvertently exposed to others. Courts remain only as a source of justice in these types of cases.

Despite repeated statutory attempts to regulate police and security service interception activity, controversy still persists with regard to admissibility of surveillance evidence. In this article we are going to discuss three basic legal issues which have a profound connection with the admissibility of surveillance evidence. They are as follows:

1. Are the directed and intrusive surveillance activities justified?
2. Are the data or evidence collected and conserved by surveillance and interception gadgets admissible in the court room?
3. Are there any limits that can be placed on the power of technology for protecting individual's right of privacy?

ARE THE DIRECTED AND INTRUSIVE SURVEILLANCE ACTIVITIES JUSTIFIED?

Jane Austen opined that "I am afraid my inquiry has been impertinent, but I had not supposed any secrecy intended…. "[11] Similarly, Blackstone long ago wrote that "Eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance," punishable at common law.[12] But this is not always true. Law enforcement authorities often perform surveillance and interception tasks to eradicate terrorism and hideous crime which could be to some extent interpreted as 'intrusion of privacy' of individuals. Many jurists promote the view that it is essential to use surveillance or interception devices 'in cases vitally affecting the domestic security.'[13] They advocate that law enforcement authorities should be given the power to approve the installation of surveillance devices when required in the interest of internal security or national safety. But privacy is citizens' fundamental right and any intrusion upon it cannot be justified easily.

As a consequence, there is a public policy dilemma as public authorities and lawmakers seek a balance between the public interest in the prevention of crime and the need for constraints on state power to intrude into the individual's life. In an attempt to find a balance between the interests of the individual and the interest of the state, 'Proportionality' becomes a vital factor.[14] Now the question arises what is proportionate, and what is not? The European Court defines proportionality as 'if a measure, which restricts a right, does so in such a way as to impair the very essence of the right it will almost certainly be disproportionate.'[15] Furthermore, the need to have relevant and sufficient reasons provided in support of the particular measure has been emphasised in *Jersild v Denmark* as: "The Court will look at the interference complained of in light of the case as a whole and determine whether the reasons adduced by the national authorities to justify it are relevant and sufficient and whether the means employed were proportionate to the legitimate aim pursued."[16]

To make proportionate measure the public authority must ensure that there is no less restrictive alternative available. It is unlikely that a measure could be considered to be proportionate where a less restrictive alternative was available. As stated by Harris et al. "action for the prevention of crime may be directed against homicide or parking offences: the weight of each compared with the right sought to be limited is not the same."[17] Thus a balancing exercise takes place that requires a consideration of whether the interference with the right is greater than is necessary to achieve the aim.[18] In *Campbell v United Kingdom*[19] a blanket rule on the opening of prisoners' mail was found to be a disproportionate response to the problem identified and thus was in breach of Article.8 of European Charter of Human Right. The argument

put forward by the Government that the interference was necessary to ensure that prohibited material was not contained in the mail was rejected on the grounds that the same policy objective could have been met by opening the mail in the presence of the prisoner without actually reading it.[20]

A further factor in the proportionality equation is "to assess the adequacy of procedural fairness in the decision making process. Where a public body has exercised a discretion that restricts an individual's rights, the rights of the affected individual should have been taken into account."[21] Proportionality can be more easily established where it could be shown that there are sufficient safeguards against abuse in place. This was expressed clearly in *Klass v Germany*:[22] "One of the fundamental principles of a democratic society is the rule of law ... [which] implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to an effective control ..."[23] Given that "most policing actions will have a basis in law and will invariably satisfy the requirement of being in pursuit of a legitimate objective the crux of a case will often be the proportionality of the action under scrutiny."[24]

In the light of the above discussion, we may conclude that public authorities should act with prudence and be cautious about the fact that any unscrupulous conduct could cause severe intrusion upon one's privacy. It should be mentioned that if a measure, which restricts the right of an individual, and does so in such a way as to impair the very essence of the right, it will almost certainly be disproportionate.[25] Furthermore, whatever system of surveillance is adopted, there must be adequate and effective guarantees against abuse. It was decided in *Klass v Germany* [26] admissibility of surveillance depends on the following facts:

1. the nature, scope and duration of the possible measures,
2. the grounds required for ordering such measures,
3. the authorities are competent to permit, carry out and supervise such measures, and
4. the kind of remedy provided by national law.[27]

In *Klass v Germany* [28] the Court further acknowledged the significance of the technical advances made in surveillance as well as the development of terrorism, and recognised that the state must be entitled to counter terrorism with secret surveillance of mail, post and telecommunications. But such measures must be taken in exceptional circumstances and the state does not have the right to adopt whatever measures it thinks appropriate in the name of counteracting espionage, terrorism or serious crime.[29]

Further, in this case, the Court provided the following general guidance as to the application of Article 8 of ECHR[30] to the prevailing German legislation that authorises surveillance:

1. The legislation must be designed to ensure that surveillance is not ordered haphazardly, irregularly or without due and proper care;
2. Surveillance must be reviewed and must be accompanied by procedures which guarantee individual rights;
3. It is in principle desirable to entrust the supervisory control to a judge in accordance with the rule of law, but other safeguards might suffice if they are independent and vested with sufficient powers to exercise an effective and continuous control;
4. If the surveillance is justified under Article 8(2) the failure to inform the individual under surveillance of this fact afterwards is, in principle, justified.[31]

Recently in *Tessling*,[32] the Canadian Supreme Court considered whether, in the absence of prior judicial authorisation, the surveillance conducted by Royal Canadian Mounted Police for detecting cannabis growing facilities owned by the respondent from the airspace using an infra-red camera, breached the right against unreasonable search and seizure guaranteed by section 8 of the Canadian Charter of Rights and Fundamental Freedoms. In this case the court reaffirmed the value of privacy and stated that "few things are as important to our way of life as the amount of power allowed the police to invade the homes, privacy and even the bodily integrity of members of Canadian society without judicial authorization."[33] The court further noted that "privacy of the person perhaps has the strongest claim to constitutional shelter because it protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters which we wish to conceal."[34] The court reiterated that section 8 of the Charter protects 'people, not places' and that the original notion of territorial privacy had "developed into a more nuanced hierarchy protecting privacy in the home, being the place where our most intimate and private activities are most likely to take place."[35] The court acknowledged that informational privacy was a 'thorny issue' concerning "how much information about ourselves and activities we are entitled to shield from the curious eyes of the State."[36] In this case the court adopted a 'totality of the circumstances' test that was evolved in *R v Edwards*.[37] The tests are as follows:

1. Did the Respondent Have a Reasonable Expectation of Privacy?
    a. What was the subject-matter of the infra-red image?
    b. Did the respondent have a direct interest in the subject-matter of the image?
    c. Did the respondent have a subjective expectation of privacy in the subject-matter of the image?
    d. If so, was the expectation objectively reasonable? In determining this it was necessary to have regard to:

i. whether the subject matter was in public view;
ii. whether the subject matter had been abandoned;
iii. whether the information was already in the hands of third parties and if so, whether it was subject to an obligation of confidentiality;
iv. whether the police technique was intrusive in relation to the privacy interest;
v. whether the use of surveillance technology was itself objectively unreasonable;
vi. whether the infrared image exposed any intimate details of the respondent's lifestyle, or information of a biographical nature.

2. If There Was a Reasonable Expectation of Privacy, Was It Violated by The Police Conduct?

On the facts, no violation of the respondent's rights under section 8 of the Charter was found in *Tessling*. It should be suggested that Tessling test provides a clear guidance in determining the periphery of the right of privacy in cases where privacy of an individual is subject to intrusion.

The European Court adopted the most acceptable approach and provided proper guidelines to determine whether an interception is ultra vires or not. In a 1998 report, JUSTICE[38] summarises those as comprising:

a. Legitimacy: Public authorities should not step beyond their jurisdiction and act legitimately. Proper disclosure should be maintained so that citizens are aware of the circumstances under which surveillance may be undertaken or communications intercepted.
b. Essentiality: The interference should be essential.
c. Proportionality: The intrusive measures should be proportional to the seriousness of the offence, bearing in mind the rights not only of the individual but also those of others likely to be affected.
d. Accountability: There must be proper controls and adequate and effective remedies against abuse.

But when the public authorities become the intruders, the consequences are apt to prove more than a mere nuisance. For example, the UK allows the interception of telephone calls, emails, letters and faxes by authorisation of the Home Secretary rather than by a judge. In America, there exists a similar system of warrantless surveillance operated by the National Security Agency. Bangladesh and the UK's system of interception without prior judicial authorisation or American system of warrantless surveillance is a threat to the privacy of an individual.[39] Section 97(a) Bangladesh Telecommunication Act 2001 empowers Minister or Home Minister to order the public authority to approve tapping of any telephone, or recording of the intercepted message without prior authorisation of the judiciary. Further, section 97(a) of this Act states that any information obtained under section 97(a) shall be considered as an admissible evidence in all circumstances, even if it conflicts with the Evidence Act 1872 (Bangladesh) or other statuary provisions. It means if surveillance evidence is obtained illegally or if a public authority acts beyond its jurisdiction in procuring surveillance evidence, that evidence should not be treated as inadmissible in the court. This is a pure inclusionary rule that undermines the individual's right of privacy. Moreover, the investigatory activities authorised by the Telecommunication Act 2001 (Bangladesh) inevitably make an impact on the privacy of the affected individual. In most instances, it is clear that this impact constitutes an interference with the right to respect for private and family life, home and correspondence, as protected by our constitution.[40] We must admit that law of Bangladesh has failed to keep pace with the ever more sophisticated surveillance techniques available not just to eager law enforcement agencies but also to possibly unscrupulous private persons. The Telecommunication Act 2001 (Bangladesh) falls far short of an effective Parliamentary response. It is unfortunate that law of Bangladesh still does not offer a single legal regulatory system to deal with the surveillance and the interception technology. Thus the law remains weak in terms of the imposition of regulation and the protection for privacy in electronic communications.

In Malaysia, no person or authority can offer multimedia service to the people without first obtaining licence from the Government. Media law in Malaysia is governed by the Communications and Multimedia Act 1998 (CMA 1998) and Printing Presses and Publications Act 1984. Under CMA 1998 "communications" means any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms. The CMA 1998 came into effect on 1 April 1999 and repealed the Telecommunications Act 1950 and the Broadcasting Act 1988 (Malaysia). The CMA 1998 provides a regulatory framework for the convergence of the telecommunications, broadcasting and computing industries. It creates a licensing mechanism and states the roles and responsibilities of those providing communication and multimedia services.

Under the CMA 1998 "The Minister may determine that a licensee or class of licensees shall implement the capability to allow authorised interception of communications."[41] This section provides wide power to the relevant Minister to intercept communication of information and no safeguard has been provided against this section. The CMA 1998 also provides that "On the occurrence of any public emergency or in the interest of

public safety, the Yang di-Pertuan Agong (the Central King of Malaysia) or the Minister authorised by him in that behalf may intercept any communication through the network."[42]

Therefore, the CMA 1998 authorises the Government of Malaysia to intercept of communication through the internet or other electronic media on the ground of the occurrence of any public emergency or in the interest of public safety. However, the Government should make sure that people's privacy right is not violated unreasonably while exercising this interception power under section 266 of the CMA 1998. In other words, when there is no emergency situation exists or public safety is not an issue, the Malaysian Government should not invoke the statutory provision provided in section 266. If this statutory provision is violated, the government might be liable for misuse of the statutory provision.

In *Mohd. Abdul Aziz Ibrahim v PP*,[43] the High Court in Kuala Lumpur, Malaysia ruled that CCTV footage would be inadmissible if not accompanied with a certificate or at least oral testimony to back it. This was a murder case and the prosecution failed to prove the case with a CCTV footage certificate or oral testimony.

Now the question is how far this covert video surveillance evidence gathered by the help of modern and sophisticated video surveillance devices is admissible as evidence in the court. There is no so far any hard and fast rule on this issue and the court decides on a case by case basis, taking into account the importance of protecting the security of the State and its people on the one side and the personal privacy issue of people on the other side.[44]

As we know, covert surveillance involves an invasion of people's privacy. Therefore, avoid acting unlawfully; it is necessary that the investigatory activities be justified under a new act with sufficient safeguard. This requires that the activity is both necessary for one of the specified aims, which include the interests of national security and the prevention of crime, and in accordance with the law. Unfortunately, most of countries do not have healthy regulation of conducting surveillance. We have so far studied the statutes of 23 countries that authorised domestic surveillance, the details of which included in the table: 1, placed in the Appendix. Unfortunately, most of the statues that the authorised surveillance are designed to undermine individual's right of privacy and they severely lacked the democratic characteristics. In this case, the court remains the main source of justice. In this circumstance the courts must assess the validity of public authority's action against a set of coherent standards. These include consideration of whether the action in question satisfies a legitimate ground for interference with the right, and, equally, whether such action is necessary and proportionate.[45]

ARE THE DATA OR EVIDENCE COLLECTED AND CONSERVED BY MODERN-DAY SURVEILLANCE AND INTERCEPTION GADGETS ADMISSIBLE IN THE COURT?

Public authorities concerned with law enforcement and national security, have been engaged in surveillance and interception activities for many years. To a significant extent, these forms of investigation were "historically unregulated. However, as the prevalence and technological capabilities of surveillance developed, so too did the awareness of the threat to privacy and the demands for regulation."[46] The enactments of various regulations regarding surveillance were a response to both areas of development. On the one hand, these regulations "facilitated the use of diverse investigatory activities, while on the other, they provided a comprehensive regulatory framework, designed to respect individual's right of privacy."[47] In so doing, it maintained a frail balance between the competing demands of privacy and surveillance. The balance between respect for privacy and the facilitation of investigatory activities is indeed a fragile one and a difficult task to maintain. If the public authority fails to act properly, judiciary intervenes to provide an appropriate remedy to the aggrieved party. And it is in large extent true that whatever potentiality the surveillance evidence possesses for the enforcement agencies, court will not recognise its full prospect due to the lack of reliability. Courts always challenge the admissibility of evidence procured from surveillance and interception gadgets on the basis of the following grounds:

1. Surveillance techniques are untrustworthy as there remain chances of manipulation. A manipulated datum or photograph or information is not admissible as evidence.
2. Sometimes public authorities act beyond their jurisdiction and obtain evidence illegally, which may make the evidence inadmissible.

SURVEILLANCE TECHNIQUES ARE UNTRUSTWORTHY AS THERE REMAIN CHANCES OF MANIPULATION: A MANIPULATED DATUM OR PHOTOGRAPH OR INFORMATION IS NOT ADMISSIBLE AS EVIDENCE

Courts have a tendency to question about the authenticity and reliability of an information that derived from high-tech surveillance gadgets. The standards that are essential for determining the admissibility of digital evidence derived from surveillance gadgets are as follows:

1. *Relevance*: Courts admit only relevant evidence. So, evidence must be logically connected to the dispute and must have probative value.
2. *Authenticity*: Once evidence is found to be relevant, it must be authenticated. It means there must be a guarantee of trustworthiness attached to the evidence.[48] Authentication standards are meant 'to

ensure that the evidence is what it purports to be, and how rigorous a foundation is needed to make this finding depends on the existence of something that can be tested in order to prove a relationship between the evidence and an individual and control against the perpetration of fraud.'[49]

3. *Reliability*: Another evidentiary lynchpin is that evidence must be original. This rule is known as the 'Best Evidence Rule'. As per American law an 'original' of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.[50] A similar approach was discovered in Ohio v. Morris.[51] In this case the government's forensic analyst copied the hard drive of the Defendant's computer and returned it to the police department that seized it. However, prior to returning the computer, the analyst erased all the data on the drive. The evidence in question was actually presented at trial in the form of a copy of the hard drive. The Defendant argued that his due process rights were violated because he could not examine the original hard drive to determine whether it contained exculpatory evidence. The appellate court held that testimony about the imaging techniques of the software used to create a copy of the original drive was sufficient to show that the duplicate was admissible. This case suggests that exact replication of the original digital evidence derived from surveillance carries the same value equivalent to the original.

To determine reliability, the Court suggested five criteria in *Daubert v Merrell Dow Pharmaceuticals, Inc*.[52] These are as follows:

1. Whether the information is derived by the scientific method,
2. Whether the information has been subjected to peer review or publication,
3. Whether the relevant scientific community 'generally accepts' the information,
4. Consideration of the actual or potential rate of error of the scientific technique, and
5. Whether standards for controlling the technique's operation exist.

These five criteria are very crucial to determine reliability of digital evidence. Therefore, almost all digital surveillance evidence is subject to this rule. Furthermore, the International Organization on Computer Evidence (IOCE) provided the following guidelines that can also be used for ensuring reliability of digital evidence:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his/her possession.
6. Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.[53]

A further clear guideline can be found in the U.S statute 'Title - Ill of the Omnibus Crime Control and Safe Streets Act of 1968'. In this statute, it is mentioned that 'intercepted communications are required to be recorded in a way that will protect the recording from editing or alterations. Interceptions are required to be conducted in such a way as to minimize the interception of communications not otherwise subject to interception. This included unrelated, irrelevant, and non-criminal communications of the subjects and of others not named in the order. Upon expiration of the intercept order, or as soon as practicable, the recordings are presented to the court of jurisdiction and are sealed. Within a reasonable time period after interception, the subjects must be furnished with an inventory of the recordings, and upon motion, a judge may direct that portion of the recordings be made available to the subject for inspection. Should the law enforcement agency err in conducting the electronic surveillance as authorized in the court order, the intercept may be challenged, and if found to have been illegally conducted, the evidence in the intercept may be suppressed.'

SOMETIMES PUBLIC AUTHORITIES ACT BEYOND THEIR JURISDICTION AND OBTAIN EVIDENCE ILLEGALLY, WHICH MAY MAKE THE EVIDENCE INADMISSIBLE

Sometimes evidence can be excluded for its illegal nature where public authorities act beyond their jurisdiction. In the United States, the courts hold any evidence as inadmissible, if it is established that the means of gathering the evidence was unconstitutional or otherwise unlawful.[54] In *Hudson v Michigan*[55] the US Supreme Court stressed that 'the exclusionary rule should only be applied where its deterrence benefits outweigh its substantial social costs.'[56] This exclusionary rule rests upon the prohibition of unreasonable searches and seizures contained in the Fourth Amendment of the USA's constitution.[57] This approach was recently adopted by American Court in *Kyllo III* [58] in determining the question "whether the warrantless use of a thermal imaging device to detect heat sources within a home constitutes an unreasonable search and seizure under the Fourth Amendment to the

United States constitution." In this case enforcement authorities used a thermal imaging device to identify indoor cultivation of marijuana plant belonged to Kyllo from outdoors without securing a warrant. The survey revealed unusually high amounts of heat emanating from the walls of Kyllo's residence. Then a warrant was issued and a raid uncovered the presence of an extensive indoor marijuana growing facility. Kyllo was convicted of drug manufacturing and sentenced to 63 months in prison. Kyllo then appealed by saying the warrantless use of the thermal imager was unconstitutional.[59]

It should be mentioned that the indoor marijuana cultivation process requires extensive use of artificial lighting. These lights generate enormous amounts of heat that is emanated outdoors either naturally or through a ventilation system installed by the cultivator. A thermal imager, placed outside the residence, can be used to measure and record the magnitude of these heat emissions. In Kyllo I ,[60] the Supreme Court held that "the use of a thermal imager to detect heat emissions from a home is not authorised under the Fourth Amendment and is therefore presumptively unreasonable without a warrant." But later in the Kyllo III ,[61] a panel of the Ninth Circuit held that the government's warrantless use of a thermal imager was not an unreasonable act and thus the evidence is admissible. The court reasoned that as the technology merely measured 'wasted or depleted heat' and did not reveal any 'intimate details' inside Kyllo's home, therefore, it was constitutionally legitimate. Accordingly, the court also concluded that one's home is not safeguarded from such outside, non-intrusive government observation.

A similar approach was found in *United States v Knotts*,[62] the defendant challenged the government's use of a beeper to monitor the transportation of a can of chemicals that the police suspected would be used for manufacturing lethal drugs. The police used the beeper and visual surveillance to track the movement of the chemicals in a suspect's car, and eventually found that the signal, once stationary, came from an area near Knotts' cabin. The officers secured a warrant and searched the cabin, where they found equipment and chemicals capable of producing fourteen pounds of pure amphetamine. The Court found no Fourth Amendment violation since the movements of the automobile with the can across public roads to the 'open fields' outside Knotts' cabin could have been observed by the naked eye.

From the above two cases, it is very evident that the U.S.'s judiciary only accept evidence which was not procured from an intrusion of privacy of an individual. And in *Kyllo* and *Knotts*, they successfully redefined the parameter of the individual's privacy.

Until 1982, the Canadian courts adopted 'inclusionary approach' to deal with illegally or unfairly obtained evidence which has a profound connection with surveillance. For example, in *R v Wray*,[63] the Court held that a trial judge had no discretion to exclude evidence of substantial probative value because it was illegally or unfairly obtained. Any discretion to exclude admissible evidence was "limited to evidence gravely prejudicial to the accused, the admission of which is tenuous and whose probative force in relation to the main issue before the court is trifling."[64] As a result, illegally or unfairly obtained evidence could only be excluded when its prejudicial effect outweighed its probative value or where it was either irrelevant or unreliable.[65] But, the position changed significantly after the enactment of the Charter of Rights and Freedoms in 1982 (Canada).[66] Section 24(2) of the Charter of Rights and Freedoms provides that "If a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded, and if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."[67]

In Australia, courts enjoy absolute discretion to exclude unlawfully or improperly obtained evidence. This is commonly referred to as the public policy discretion. The High Court of Australia held that when unlawful means are used to procure evidence, the judge has discretion to reject it.[68] Here Barwick CJ must be quoted. In *R v Ireland*, Barwick CJ said: "Evidence of relevant facts or things ascertained or procured by means of unlawful or unfair acts is not, for that reason alone, inadmissible. This is so, in my opinion, whether the unlawfulness derives from the common law or statute. But it may be that acts in breach of a statute would more readily warrant the rejection of the evidence as a matter of discretion or the statute may on its proper construction itself impliedly forbid the use of facts or things obtained or procured in breach of its terms."

On the other hand evidence of facts or things so ascertained or procured is not necessarily to be admitted, ignoring the unlawful or unfair quality of the acts by which the facts sought to be evidenced were ascertained or procured. Whenever such unlawfulness or unfairness appears, the judge has discretion to reject the evidence. He must consider its exercise. In the exercise of it, the competing public requirements must be considered and weighed against each other. On the one hand there is the public interest in the protection of the individual from unlawful and unfair treatment. Convictions obtained by the aid of unlawful or unfair acts may be obtained at too high a price.[69]

The basis for the public policy discretion to exclude evidence has further been expressed by Stephen and Aickin JJ in *Bunning v Cross*. In this case they said: "Were there to occur wholesale and deliberate disregard of these (procedural safeguards for the individual) its toleration by the courts would result in the effective abrogation of the legislature's safeguards of individual liberties, subordinating it to the executive arm. This would not be excusable however desirable be the end in view, that of convicting the guilty. In appropriate cases it may be 'a

less evil that some criminals should escape than that, the Government should play an ignoble part."[70]

But in the United Kingdom the court adopts a different approach in deciding the admissibility of surveillance evidence. In case *R v Khan*,[71] the House of Lords decided that an illegal covert recording of a conversation was admissible, even though obtaining the recording involved trespass and damage to property from the part of public authority. In this case Lord Nolan commented that it would be a 'strange reflection on the law' if a person who had admitted involvement in an offence could have the conviction set aside because his privacy had been invaded.[72] In this case, the Court conceded that the installation of the listening device had involved a civil trespass. But the Court accepted that without the tape recording there would be no case to answer. The trial judge, therefore, declined to exclude the taped conversations under the prevailing law of the UK. Khan was sentenced to three years' imprisonment. He made an appeal to the House of Lords. The House took the view that the trial judge had been justified in not excluding the evidence. Another appeal was made to ECJ. Despite finding unanimously that Khan's right to privacy had been violated, the European Court held that Khan had received a fair trial.[73]

This view was further supported in *R. v X*.[74] In this case, defendants were charged with offences related to possessing and misusing drugs, and convicted. They appealed by saying that evidence of intercepted telephone conversations that had been obtained in a foreign jurisdiction was inadmissible and should be excluded under the regulations of the UK. Dismissing the appeal the House of Lords held that the telephone interceptions had been undertaken lawfully outside the UK with the aim of bringing about a criminal prosecution, and as such evidence had not been used for any other purpose nor held for longer than was necessary, there had been no illegality and the surveillance evidence was admissible. It should be mentioned that on balance, the current English case law favours the admission of illegal or improper surveillance evidence 'in the absence of blatant bad faith or oppression on the part of the investigators.'[75]

In summary, it should be noted that once an enforcement authority succeeds to maintain 'Proportionality' and 'Essentiality' remaining in their jurisdiction and if the intercepted evidence is free from manipulation and inaccuracy, courts are bound to accept that evidence. But the problem arises when public authorities procure surveillance evidence illegally. In this case, judiciary becomes the saviour. I do agree that the constant need surveillance to maintain law and order in a state, and the right of privacy stands in two different directions. The first recommends the use of desperate methods for maintaining peace inside a state, and the other prescribes ultimate caution must be maintained to safeguard the individual's right of privacy.

Therefore a balance must be upheld in all the circumstances. It should be remembered "... in respect of national security as in respect of other purposes, there has to be at least a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is ... evidently problematic."[76] Further, where a court believes that surveillance evidence is possibly manipulated, it may ask for supporting evidence. For example, if X, an enforcement agent, produces a satellite image to the court to prove that Y is using his company trucks to carry illegal equipment and chemicals, court may ask the question - whether the satellite had been working properly at the time it shot the image, so further proof of correct functioning, reliability and accuracy from an expert witness might be necessary in this case.[77] The Daubert standards will be applicable here and satellite data must be presented through expert testimony. In doing so one must remember the fact that the satellite evidence must have an adequate foundation; it must be accurate and reliable.[78] If accuracy cannot be confirmed, courts will not admit the evidence.[79]

JUDICIAL PRECEDENT AND SURVEILLANCE EVIDENCE

SATELLITE PHOTOGRAPHY

There are many cases in which courts have admitted satellite photographs as evidence. For example, In *I&M Rail Link v Northstar Navigation*,[80] satellite photos were used to determine whether a barge accident occurred in Illinois or Iowa. In *Inre Vernon Sand & Gravel, Inc.*,[81] aerial photographs were used in settling a land acreage discrepancy. In *Scruggs v United States*,[82] an F-16 military aircraft and the plaintiff's civilian plane almost collided in mid-air. The plaintiff testified that a cloud prevented him from flying at a higher altitude. The court ruled for the government because the satellite data showed that the area was free of clouds. In *Cobb v United States*,[83] the plaintiff claimed that a 'freak' wave injured him when he was a guest on a Navy destroyer. As satellite data indicated that no storms were in the area at that time, the court ruled for the defendant. Furthermore, satellite and aerial photographs have also played a vital role in International Court of Justice in *Burkina Faso v Republic of Mali*[84] and *Namibia v Botswana*.[85] It must be mentioned that satellite and aerial photographs always explore the aerial view of an exposed object; therefore, its admissibility cannot be challenged on the ground of intrusion of privacy. This view was supported in *Florida v Riley* [86] and *Dow Chemical Co. v United States*.[87]

TAPPING TELEPHONES

The use of court authorised electronic surveillance became increasingly important as the telephone system became a part of everyday life. In the case of *Olmstead v United States*,[88] the Court found that tapping a telephone did not violate the Fourth Amendment. In Olmstead, defendants were convicted for conspiring to violate the National Prohibition Act (41 Stat. 305) by illegally possessing, transporting, importing and selling intoxicating liquors. Four federal prohibition officers discovered the information of the conspiracy by intercepting the telephones of the conspirators. Wires were placed along the ordinary telephone wires from the homes and offices of the defendants. The insertion of the wires was made without trespassing the defendants' property. The defendants were convicted of a conspiracy to violate the National Prohibition Act. Later they appealed on the grounds that the prosecution's case relied exclusively on evidence gathered through a wiretap of the defendant's telephone lines in violation of the Fourth Amendment, which says, "The right of the people to be secured in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[89]

The Supreme Court held that messages passing over telephone wires were not within the protection against unreasonable searches and seizures. The eavesdropper had to have physically trespassed in order for evidence procured by wiretapping to be regarded as having been obtained unconstitutionally. The Court reasoned that, since there was no entry of the homes or offices of the defendants, there was no physical trespass. It must be stretched out that the Olmstead case was overruled; the physical trespass doctrine of Olmstead was abandoned. Under current law, in order for electronic surveillance to be constitutionally permissible, it must be done, in most cases, pursuant to the prior authorisation by a court.[90]

In *Malone v Commissioner for the Metropolitan Police (no. 2)*,[91] the plaintiff was tried at the UK's Crown Court for handling stolen property. During the trial the prosecution counsel stated that the plaintiff's telephone was intercepted by the police on the authority of a warrant. The warrant was sent to the Post Office and the Post Office then made a recording of conversations for the police. After being acquitted of the criminal charges, the plaintiff brought a civil action against the police claiming that the police interception of his phone calls had been unlawful as it constituted a breach of confidence, a trespass, and an unlawful interference with his privacy.

The Court held that telephone services provided by the Post Office to subscribers were not supplied under a contract and it was therefore impossible to imply a term that telephone conversations should remain confidential and free from tapping. Moreover, the Court indicated that 'on the principle everything was permitted in law except that which was expressly forbidden, telephone tapping was not unlawful since telephone tapping by the Post Office at the request of the police could be carried out without any breach of the law, and it did not require any statutory or common law power to justify it. Furthermore, although there was no statute which expressly authorised telephone tapping, where the tapping was done under warrant, statutory recognition of the lawfulness of the tapping was afforded by s 80 b of the Post Office Act 1969. Moreover, telephone tapping was not in other respects illegal.' The Plaintiff took his case to the European Court of Human Rights under article 8 which is concerned with privacy against state interference in international law. The European Court of Human Rights held that the English practice of interception was insufficiently grounded in law to allow it to be justified under Article 8(2). As a reaction to this judgment and other pending cases, legislation was later passed in the form of the Interception of Communications Act 1985 and the Police Act 1997 Part III.

BUGGING DEVICE

In *Goldman v United States*,[92] the Court held that federal agents acted within constitutional guidelines when they planted a Dictaphone recording device in a wall to listen to conversations taking place inside the next room. In *On Lee v United States*, an undercover agent wearing a concealed microphone entered a retail store to investigate narcotics violations while another agent listened in from a location outside the building.[93] No constitutional violation was found, since the use of electronic equipment substantially resembled the permissible use of bifocals, field glasses, or telescopes.[94] It was not until the late 1960s, in the case of *Silverman v United States*,[95] where the Court found evidence of an actual trespass by law enforcement agents conducting the surveillance activity, invading the defendant's physical space was declared to be a violation of the Fourth Amendment.[96]

In *Berger v New York*,[97] the Court was faced with determining the constitutionality of evidence seized through the use of a bugging device planted in a business office. In *Berger*, state agents were investigating allegations that an individual was accepting bribes in exchange for issuing liquor licenses. Although an eavesdropping order was obtained, the majority concluded that the provisions authorising the order did not satisfy constitutional requirements. Furthermore, the length of time eavesdropping permitted was too extensive, extensions were granted even without proof that the surveillance served the public interest.[98] In the view of the majority, the Court recognised an intrusion on privacy.[99]

EMAIL

Email is the most popular mode of Internet communication. Private messages that once would have been communicated via postal mail nowadays occur through email. Private

letters, photos, personal financial documents, trade secrets, privileged legal and medical information all exchanged over email, and stored with email providers after they are sent or received. These numerous private uses of email demonstrate society's expectation that the personal emails sent and received over the Internet and stored with email providers are as private as a sealed letter. The U.S. Court of Appeals in *United States v Long,*[100] and *United States v Maxwell*[101] supported this view. These cases ruled that email account holders have a reasonable expectation of privacy in their stored email. Further, the U.S. Supreme Court's decision in *Smith v Maryland* [102] reaffirms that the Fourth Amendment protects the contents of stored email messages just as it protects the contents of phone calls and sealed letters.

Moreover, under the reasoning of *Katz v United States*[103], email users have a constitutionally protected 'reasonable expectation of privacy' in their stored email.[104] In *Katz*[105], Harlan, J., concurred that Fourth Amendment protections apply where "a person [has] exhibited an actual (subjective) expectation of privacy… that society is prepared to recognize as [objectively] 'reasonable'. The reasonableness of such 'an expectation of privacy in the contents of stored emails is made plain by analogy to society's expectations of privacy in the contents of phone calls, the contents of rental residences like apartments and hotel rooms, and the contents of sealed postal mail."[106] Since *Katz*, the U.S Supreme Court has regularly looked to societal expectations in judging Fourth Amendment problems, particularly where new technologies are concerned.[107] It is equally plain that society expects privacy in stored email because email users often store their personal messages with the provider rather than downloading them onto their own computers after sending or receiving an email.[108]

It should be mentioned that the email providers have the technical ability to access the email account stored on their servers without violating the right of privacy of a user. Katz and Smith also supported this view. This is why Stewart, J., dissented in Smith by saying that "A telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment."[109] This means the court recognises telephone providers' potential and actual power to intercept phone calls. But this right is achieved at the cost of 'no delegable duty' which should be performed by the telephone company or e-mail service provider. In this case, the U.S. Supreme Court further held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world"[110] If this rule is applicable to email then an email provider may be able to enjoy the privilege to access the individual's email account but can not have the right to broadcast the information to anyone.

GPS EVIDENCE

Nowadays Global Positioning System (GPS)[111] has become the technology of choice for tracking and locating parolees, and sex-offenders. At least twenty-three states in the United States are using GPS for tracking convicted sex-offenders and some states are even using GPS for tracking low-risk offenders.[112] Usually worn as an anklet or bracelet by the parolee, GPS tracking has proven to be a powerful tool in monitoring of high-risk offenders.[113]

With regards to admissibility of GPS data as evidence courts have regarded GPS technology to be 'generally accepted and fundamentally valid and waived any doubts about its credibility.'[114] The *United States vs Garcia* is a more recent case which directly involves the use of GPS data for tracking suspected criminals. In this case the 7th Circuit Court of Appeals concluded that the installation of the GPS tracking device in the defendant's car neither constituted a seizure nor search because the device did not interfere with the driving qualities of the vehicle and was analogous to a police officer following the vehicle.

In the *Peterson* trial Judge Alfred Delucchi ruled that the satellite tracking devices used by the police to track Scott Peterson in the days after his wife disappeared would be allowed as evidence.[115] Further, in 2 BvR 581/01,[116] Germany's Federal Constitutional Court (FCC) held that the law enforcement agencies have the right to use the Global Positioning System (GPS) to track the movements of suspects. In this case, the petitioner was a member of a terrorist group. Several government agencies investigated the petitioner and his co-defendant for past and ongoing terrorist offences. During the course of these investigations, the security agencies installed a GPS tracking device in the petitioner's vehicle. The device recorded a vehicle's location, movements, and speeds along with the corresponding dates and times. In this way, it permitted the investigators to construct a complete picture of the car's past and present movements.

In this case, the federal investigators not only used GPS technology, but also conducted visual surveillance and monitored his telephone and his mail. These together permit a fairly detailed reconstruction of a target's daily activities. The petitioner appealed against his attempted murder convictions for carrying out a series of terrorist bombings. His petition challenged the state's use of GPS technology to monitor his movements. The petitioner argued that the accumulation of different modes of surveillance exposed too much personal information to the government. The petitioner further claimed the evidence obtained through the Global Positioning System could not have been used to convict him without infringing his right to a fair trial. In upholding the use of GPS technology, the Supreme Court rejected the petitioner's claims.

ARE THERE ANY LIMITS THAT CAN BE PLACED ON THE POWER OF TECHNOLOGY FOR PROTECTING INDIVIDUAL'S RIGHT OF PRIVACY?

"The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his forces dare not cross the threshold of the ruined tenement."

- Sir William Pitt [117]

Electronic surveillance is an essential part of modern policing, but we cannot rely on the courts to ensure that public authorities do not infringe fundamental liberties of the individuals. Thus, there is indeed a need for a proper legislative framework to cover the whole range of espionage operations. But unfortunately, most states are reluctant to confront fundamental issues relating to policing and privacy. They have consistently failed to determine the extent of privacy and impose adequate controls on surveillance and interception activities of their public authorities. For example, in the U.S the Fourth Amendment states that 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.'[118] But this statutory provision failed to answer the question: how much privacy should one enjoy? or how much privacy should be left for individual enjoyment from the intrusion of law enforcement authority?

In the landmark decision of *Katz v United States*,[119] the U.S. Supreme Court analysed the Fourth Amendment violations and determined its periphery by rejecting the notion of constitutionally protected areas and adopting a new emphasis on the individual expectation of privacy.[120] In *Katz v United States*,[121] Katz was convicted under an indictment charging him with transmitting wagering information by telephone across state lines in violation of 18 U.S.C. 1084. Katz's conversations were intercepted by FBI agents who had attached an electronic listening and recording device to the outside of the telephone booth from which Katz made calls. The recorded conversations are introduced at the trial as evidence. In the Court of Appeals, Katz has phrased the following questions:

1. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth?
2. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution?

The Court of Appeals affirmed the conviction, finding that there was no Fourth Amendment violation since there was no physical entry into the telephone booth from where Katz made the call. Furthermore, later the Supreme Court rejected the longstanding view that a Fourth Amendment violation must be coupled with a physical intrusion into "a constitutionally protected area."[122] In the Court's view, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," it became clear that "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[123] The decision expressly overruled Olmstead[124] and Goldman[125], asserting that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[126] In this case Justice Harlan articulated his celebrated 'expectation of privacy' test for defining legitimate warrantless surveillance by electronic devices.[127] According to Justice Harlan, the application of Fourth Amendment protection is predicated upon a twofold test. These are as follows:

Firstly, a person have exhibited an actual (subjective) expectation of privacy and,

Secondly, the expectation should be one that society is prepared to recognize as reasonable.

But Harlan's test is not free from criticism as it failed to provide appropriate remedies in many circumstances. The famous jurist Wayne R. LaFave & Jerold H. Israel said, "as the case law developed, it became clear that when interpreting the subjective prong of Harlan's test, it is not sufficient that [the expectation] be merely reasonable; something in addition is required."[128] With an illustration I can make the problem easier for readers to understand: If two notorious drug dealers, X and Y were to rely on the privacy of an isolated corner of Romna Park in the middle of the night to carry out an illegal transaction. It would be a reasonable for both of them to expect privacy as there would be virtually no risk of discovery. But fortunately if Z, a policeman present at the park at the same time and sheds light on the crime spot with his flashlight, it would be foolish for the criminals to suppress the officer's testimony as a violation of their rights.

The hypothetical criminals in the given scenario "rationally considered their transaction to involve little risk of discovery. Rather, the expectation of privacy is intended to be a basis of differentiating those expectations which are merely reasonable from those expectations which are to be constitutionally enforced due to other social considerations."[129] Thus, the emergent framework established that "expectations of privacy that society is prepared to recognise as legitimate have, at least in theory, the greatest protection; diminished expectations of privacy are more easily invaded; and subjective expectations of privacy that society is not prepared to recognize as legitimate have no protection."[130] A literal interpretation of Justice Harlan's test requires that the defendant have an actual (subjective) expectation of privacy to invoke constitutional protections. The Court's

further expounding of the doctrine has clarified that the standard strictly depends upon the expectations of privacy that society deems reasonable.[131] The Supreme Court in Katz rejected Olmstead's strictly property-based conception of the Fourth Amendment, holding instead that 'the Fourth Amendment protects, people, not places.'[132] Therefore, even though Katz's telephone conversations were intangible and not literally his 'houses, papers, [or] effects' and even though they were transmitted via the phone company's property, they were protected by the Fourth Amendment against search or seizure by the government. It was recognized in Katz case that the Fourth Amendment protects society's shared expectations about what is private, and applied Fourth Amendment protections based on the telephone's vital societal role as a medium for private communication.[133]

In *Florida v Riley*,[134] a county sheriff's office hired a helicopter, and flew over the defendant's property at an altitude of roughly four-hundred feet for tracking a marijuana-growing field. Through aerial naked-eye observations, the law enforcement officer discovered a marijuana field in the defendant's backyard greenhouse. Based upon this information, a search warrant was issued to enter the premises, and the defendant was charged with possession of an illegal substance under state law. The defendant filed a motion to suppress the evidence, claiming that the warrantless aerial surveillance constituted a violation of his reasonable expectation of privacy against unreasonable searches under the Fourth Amendment. The trial court granted the defendant's motion, and on appeal, the Florida Supreme Court held that the helicopter surveillance from four-hundred feet established a search for which a warrant was required. In the view of Florida's highest court, such conduct must be assessed in light of society's standards of reasonableness in order to be considered an unacceptable intrusion into the privacy of the home.[135] However the United States Supreme Court reversed this decision. In the majority opinion by Justice White, the Court reasoned that although the defendant no doubt intended and expected that his greenhouse would not be open to public inspection, by leaving the sides and roof of the structure partially open to the aerial view, the contents of the greenhouse were subject to viewing from the air. Thus, the defendant "could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter … flying within the navigable airspace for fixed-wing aircraft." The majority concluded that helicopter flights at four-hundred feet are not "sufficiently rare in this country to lend substance to [the defendant's] claim that he reasonably anticipated that his greenhouse would not be subject to [aerial] observation." Accordingly, in the Court's view, the defendant could not possess any reasonable expectation of privacy by societal standards under the Katz search test.

In *Dow Chemical Co. v United States*,[136] Dow Chemical operates a 2,000-acre facility manufacturing chemicals at Midland, Michigan. The facility consists of numerous covered buildings, with manufacturing equipment and piping conduits located between the various buildings exposed to visual observation from the air. Dow Chemical maintained elaborate security around the perimeter of the complex, barring ground-level public views of these areas. The Environmental Protection Agency (EPA) failed to get permission for an on-site inspection of the plant, employed a commercial aerial photographer to take aerial photographs of the facility remaining within lawful navigable airspace without seeking on a search warrant. The photographer used a standard precision aerial mapping camera for this purpose. Being aware of the aerial photography, Dow Chemical brought suit in Federal District Court, alleging that EPA's action violated the Fourth Amendment and was carried out beyond its statutory investigative authority. The District Court granted summary judgment for the petitioner, but the Court of Appeals reversed, holding that EPA's aerial observation did not exceed its investigatory authority and that the aerial photography of the petitioner's plant complex without a warrant was not a search prohibited by the Fourth Amendment.

The Court found that though commercial areas receive constitutional privacy protection, this protection does not extend to the outdoor areas of industrial complexes. The Court also found that homes and their outside areas receive a higher level of protection than commercial areas. In dicta the Court stated, "Surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[137] Further it was mentioned, 'The open areas of an industrial plant complex such as petitioner's are not analogous to the curtilage of a dwelling, which is entitled to protection as a place where the occupants have a reasonable and legitimate expectation of privacy that society is prepared to accept (citation omitted). The intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant. For purposes of aerial surveillance, the open areas of an industrial complex are more comparable to an open field in which an individual may not legitimately demand privacy.[138]

Here, EPA did not employ some unique sensory device which was not available to the public, but rather employed a conventional, albeit precise, commercial camera commonly used in map-making. The photographs were not so revealing of intimate details as to raise constitutional concerns. The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.'[139] In this case Burger C.J., said "We emphasized that, unlike a homeowner's interest in his dwelling, '[t]he interest of the owner of commercial property is not one in being free from any inspections (citation omitted).'And with

regard to regulatory inspections, we have held that 'what is observable by the public is observable, without a warrant, by the Government inspector as well."[140] The Court feared that technology providing information not available to the naked eye would reveal intimate details, for example, imaging that could reveal actions occurring inside a building.[141] Despite this concern, the Court noted that photos enhancing human vision were still admissible, provided that they do not reveal such intimate details.[142]

A contrary decision was found in *DuPont v Christopher*.[143] In this case, an unknown party hired the defendants to take aerial photographs of new construction at a DuPont chemical plant in Beaumont, Texas. DuPont had developed a secret process for producing methanol, which gave it a competitive advantage over other manufacturers. DuPont alleged that the defendants were engaged in industrial espionage, and that their deliberate over-flights violated its trade secret rights and industrial privacy. The defendants responded that they had every right to fly over the plant and were not trespassing. They claimed that anyone could legitimately fly through that airspace and aim a camera at the ground.

Therefore, DuPont could not claim protection over such aerial evidence any more than over what a passer-by could see in plain view by walking outside the plant on a public road. The court rejected this argument. It held that aerial photography was "an improper means of obtaining another's trade secret," because it was a form of espionage that "could not have been reasonably anticipated or prevented" by DuPont. *Dow Chemical Co. v United States* can be distinguished from *DuPont v Christopher*. Dow Chemical discussed the issues of illegal government search and DuPont was concerned with the issues of trade secret infringement. But at a conceptual level, both cases raised the same question: if aerial photography of a location was a reasonably expected phenomenon, or an improper intrusion? These two cases provided two different approaches in determining the parameter of privacy. But one common thing they established that aerial and satellite data is admissible if it is properly conducted.

Last of all I would like to discuss another case to shed light on the particular point. In *Barbra Streisand v Kenneth Adelman*, the plaintiff filed a lawsuit in Los Angeles Superior Court, seeking an injunction for barring the defendant from continuing to distribute aerial images of her home, as the photos provide a 'road map into her residence' and 'clearly identify those routes that could be used to enter her property.' The defendant operates the California Coastal Records Project, which specialises in aerial photographs of the California coast, images intended for use by scientists and researchers. He has posted more than 12,000 high-resolution digital aerial images of the coastline on a website, where they are freely available for download. The plaintiffs sued the defendant for invasion of privacy and violation of California's anti-paparazzi law. The judge rejected plaintiff's claim, finding that "Aerial views are a common part of daily living, and that there is nothing offensive about the manner in which they occur, nor in the manner in which this particular view was obtained."[144] This decision was given in the light of the Dow case. I hope in future we will receive further guidance from the U.S judiciary which will help us to know the exact parameters of the right of privacy.

In the final analysis, we may conclude that the extent of guaranteed privacy of an individual is still uncharted area for the modern law; therefore it is for the judiciary to assess the validity of police action against a set of coherent standards (Test of essentiality and proportionality). It should also be noted that court should not rely on any surveillance evidence when its procedural safeguards are infringed. Further it must be mentioned that the use of legitimated electronic intrusion only acceptable for protecting citizens from lawlessness or to preserve domestic tranquillity otherwise not.

CONCLUSION

Nowadays the state is one of the countless numbers of surveilling entities that have a legal authority to gather information regarding anything or any person. Most states have a legal framework authorising surveillance activities but they do not provide sturdy shield against any intrusion. Limited scope of prevailing legal regulations left much surveillance practice beyond authorisation, and information gathered from surveillance must not be disclosed in normal circumstances. Stringent legal rules are required with regard to disclosure of information, rather than restricting access to it. It is true, after 9/11 technology-driven loss of privacy inevitably became a negative development rather than something to be cherished as law enforcement agencies are doing more than they are authorised to do. As a result, an intrusion of privacy is not always considered as usurpation of the individual's right by the concerned authorities.

Sturdy rules are therefore, required for regulating law enforcement agencies surveillance activities, which is not an easy matter to accomplish. On the one hand the law makers have to give the public authorities unprecedented power to conduct surveillance to safeguard the interest of a state, on the other hand they must empower the judiciary to grant an immediate remedy if anyone acts beyond their power conferred by statutes and intrudes others privacy. Most developed countries have successfully invented a mechanism to protect the right of privacy of an individual by empowering the judiciary to provide guidelines to the government agencies for conducting surveillance for the interest of the nation. Side by side, they gave the judiciary an absolute authority to use its discretion to accept or reject evidence procured from surveillance.

In some countries, for example Bangladesh, there is no adequate legislation and precedents on the admissibility of covert surveillance evidence. It is

recommended that these countries may follow the above mentioned precedents related to the covert surveillance evidence. The Evidence Act 1872 (Bangladesh) does not have provision of covert surveillance evidence nor the admissibility of digital message communicated through the internet. Unlike the evidence law of Bangladesh, the Indian Evidence Act 1872 has been amended by the Indian Information Technology Act 2000 to elaborately deal with the issues of admissibility of electronic records.[145] However, Bangladesh has enacted Information and Communication Technology Act 2006 (ICT Act 2006) which has clear provision to recognize the digital message and to use digital message in the court as evidence. Similarly, the Evidence Act 1950 (Malaysia) provides that digital information can be used as evidence in the court.[146]

In the absence of clear laws on the admissibility of covert surveillance evidence, concern countries' law makers may shed light on this particular topic and successfully fill the gap between 'individual's right to leading a peaceful life' and the 'right to retain the privacy'. For this purpose a fair and up to date state policy must be adopted. The policy should contain a clear definition of what is (and is not) acceptable use of surveillance evidence, leaving the citizens in as little doubt as possible as to where the boundaries lie. A 'zero tolerance' policy must not be adopted, as it may have drawbacks in terms of preventing the nourishment of an individual's right that could ultimately lead to a paradoxical situation. A more balanced policy might be adopted to limit the power of public authorities that authorises espionage and judiciary must be equipped properly to handle cases related to surveillance evidence. This can only be achieved if a draconian power is conferred on the judiciary, which will enable them to use 'the discretionary rule of admissibility of evidence' freely along with exclusionary rule. For doing so 'due diligence' must be practiced to ensure: (a) accountability of public authorities; (b) maintaining the proportionality and essentiality remaining in their jurisdiction; (c) maintaining proper disclosure when cases will face judicial action, (d) maintaining the strength of the judiciary to shape the occupational and professional culture of the enforcement agencies. Vigilant citizens will not have any objection in accepting any intrusion which legitimately limits the individual's right of privacy if the mentioned criteria are followed.

NOTES

1 S D Warren and L D Brandeis (1990), the Right to Privacy, 4 Harvard Law Review 193 at 195.

2 Massive millimetre wave detectors use a form of radar to scan beneath clothing. By monitoring the millimetre wave portion of the electromagnetic spectrum emitted by the human body, the system can detect items such as guns and drugs from a range of 12 feet or more. It can also look through building walls and detect activity. In simple words, it is a device that can detect guns through people's clothing by measuring electromagnetic radiation and producing an image of the body of the person being viewed.

3 A microphone that has a dish like that of a satellite dish which is placed behind the microphone, usually hypercardioid, to focus its sensitivity to an extremely narrow range. A parabolic microphone uses a parabolic reflector to collect and focus sound waves onto a receiver, in much the same way that a parabolic antenna does with radio waves. Typical uses of this microphone, which has unusually focused front sensitivity and can pick up sounds from many meters away, include nature recording, field audio for sports broadcasting, eavesdropping, law enforcement, and even espionage. Source: http://en.wikipedia.org/wiki/Parabolic_microphone.

4 A new eavesdropping technique can be used to read cathode-ray tube (CRT) displays at a distance. The intensity of the light emitted by a raster-scan screen as a function of time corresponds to the video signal convolved with the impulse response of the phosphors. Experiments with a typical personal computer colour monitor show that enough high-frequency content remains in the emitted light to permit the reconstruction of readable text by deconvolving the signal received with a fast photo sensor. These optical compromising emanations can be received even after diffuse reflection from a wall. Shot noise from background light is the critical performance factor. In a sufficiently dark environment and with a large enough sensor aperture, practically significant reception distances are possible. Source: http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf.

5 The Australian High Court has acknowledged the importance of recorded evidence, particularly where confessions and admissions in criminal trials are concerned in the case *McKinney v The Queen* (1991) 171 CLR 468 at 473-474.

6 The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their relationship with the State, House of Lords Constitution Committee, June 2007.

7 Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J. L. & TECH. 161, 229-30 (2000).

8 Kenneth J. Markowitz, *Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence*, 12 Duke Environmental Law & Policy Forum, 220 (2002).

9 http://www.yourdictionary.com/surveillance.

10 http://www.army-technology.com/glossary/surveillance.html, Retrieved from the internet on July 2007.

11 Jane Austen, *Sense and Sensibility*, Penguin Classics, (1811), 116.

12 Abu Hena Mostofa Kamal, *Admissibility of covert surveillance evidence,Law and Our Rights*, Daily Star, Issue No: 227 February 25, 2006, http://archive.thedailystar.net/law/2006/02/03/advocacy.htm

13 D.J. Harris, M. O'Boyle, and C. Warbrick, Law of the European Convention on Human Rights (Butterworths, London, 1995) at p. 298.

14 Richard C. Turkington, *Legal Protection for Conversational and Communication Privacy in Family, Marriage and Domestic Disputes: An Examination of Federal and State Wiretap and Stored Communications Acts and the Common Law Privacy Intrusion Tort*, 82 *Nebraska Law Review* 3,

(2004). Villanova University School of Law, Public Law and Legal Theory, Working Paper No. 2003-10, September 2003.

15 *Rees v United Kingdom* (1987) 9 E.H.R.R. 56.

16 *Jersild v Denmark* (1995) 19 E.H.R.R. 1 at para.31.

17 D.J. Harris, M. O'Boyle, and C. Warbrick, Law of the European Convention on Human Rights (Butterworths, London, 1995) at p. 297.

18 *Jersild v Denmark* (1995) 19 E.H.R.R. 1 at para. 31.

19 *Campbell v United Kingdom* (1993) 15 E.H.R.R. 137.

20 Richard C. Turkington, *Legal Protection for Conversational and Communication Privacy in Family, Marriage* and *Domestic Disputes: An Examination of Federal and State Wiretap and Stored Communications Acts and the Common Law Privacy Intrusion Tort*, 82 *Nebraska Law Review* 3, (2004). Villanova University School of Law, Public Law and Legal Theory, Working Paper No. 2003-10, September 2003.

21 *W v United Kingdom* (1988) 10 E.H.R.R. 29.

22 *Klass v Germany* (1979-80) 2 E.H.R.R. 214.

23 *Klass v Germany* (1979-80) 2 E.H.R.R. 214 at para. 55.

24 Fred Galves, Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, 13 HARV. J. L. & TECH. 161, 229-30 (2000).

25 *Rees v United Kingdom* (1987) 9 E.H.R.R. 56.

26 *Klass v Germany*, (1979) 2 E.H.R.R.

27 The European Court stated in Klass v Germany, (1979) 2 E.H.R.R. 214 at para.50.

28 *Klass v Germany*, (1978) 2 E.H.R.R. 214.

29 *Ludi v. Switzerland* A 238 (1992)

30 Article 8 provides a right to respect for private and family life, subject to the qualification in Art. 8(2) that interference may occur where it is 'in accordance with the law and is necessary in a democratic society in the interests of', inter alia, the prevention of disorder or crime. The interrelationship between Arts. 8(1) and (2) is not one of balancing the legitimate interferences against the right; the Art. 8(2) qualifications clearly represent exceptions to Art. 8(1). This substantive hierarchy is reflected in the process of evaluating the Art. 8 protection in any given case. The court determines whether surveillance interfered with privacy rights as broadly interpreted in Art. 8(1) before assessing the Art. 8(2) elements in turn.

31 *Klass v. Germany* (1978) 2 E.H.R.R. 214.

32 Tessling [2004] S.C.C. 7

33 Tessling [2004] S.C.C. 7, para 13.

34 Tessling [2004] S.C.C. 7, para 21.

35 Tessling [2004] S.C.C. 7, para 22.

36 Tessling [2004] S.C.C. 7, para 23.

37 *R v Edwards* [1996] 1 S.C.R. 128, http://casebrief.me/casebriefs/r-v-edwards/

38 Justice under Surveillance: *Covert Policing and Human Rights Standards* (1998). Retrieved from internet on September 2007, see, http://www.cils.org/WSIS/TechnologySurveillance/03sin.pdf

39 *American Civil Liberties Union v National Security Agency, US District Court*, 18 August 2006 (Case no. 06-CV-10204).

40 Article 48(b).

41 See, section 265 of the Communication and Multimedia Act 1998 (Malaysia).

42 See, section 266 of the Communication and Multimedia Act 1998 (Malaysia).

43 Available online http://www.thestar.com.my/News/Nation/2013/06/07/*Vagrant-acquitted-of-murder-after-court-rules-CCTV-footage-of-attack-inadmissible*/, retrieved on 10.11.2014.

44 Ralph D. Thomas, *The History And Evolution of Covert Video Surveillance Evidence Gathering*, (2008). See online: http://www.pimall.com/nais/videohistory.html.

45 T. John, Covert and Deceptive Policing in England and Wales: Issues in Regulation and Practice, 4 European Journal of Crime, Criminal Law and Criminal Justice 316 (1996).

46 T. John, Covert and Deceptive Policing in England and Wales: Issues in Regulation and Practice, 4 European Journal of Crime, Criminal Law and Criminal Justice 316 (1996).

47 Deirdre K. Mulligan, Reasonable Expectations of Privacy in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1569 (2004).

48 Edward Imwinkelried, *The Debate in the DNA Cases Over the Foundation for the Admission of Scientific Evidence: The Importance of Human Error as a Cause of Forensic Misanalysis*, 69 WASH. U. L. Q. 19 (1991).

49 Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J. L. & TECH. 161, 229-30 (2000).

50 Fed. R. Evid. 1001. Variations of this rule have been adopted by nearly every state in the United States.

51 *Ohio v Morris*, 2005 Ohio 599, (Ohio Ct. App. Wayne County, Feb. 16, 2005).

52 509 U.S. 579 (1993).

53 International Organization on Computer Evidence (IOCE) First Responders Guide Template (Dec. 14, 2000), available online at: http://ncfs.org/documents/ioce2000/reports/firstResponders.pdf

54 *State v Fisher* 686 P2d 750 (1984); *People v Hamilton* 666 P2d 152 (1983); *State v Johnson* 716 P2d 1288 (1986); *Thompson v Carthage School Dist* 87 F3d 979 (1996); *US v Kennedy* (1995) 61 F3d 494; *US v Medina Reyes* 877 F Supp 468 (1995).

55 *Hudson v. Michigan*, 126 S. Ct. 2159, 2168 (2006).

56 *Hudson v. Michigan*, 126 S. Ct. 2159, 2168 (2006), at 2165 (using a balancing test to determine when the exclusionary rule may be appropriately applied).

57 *Olmstead v United States* 277 US 438 (1928); *US v Nichols* 979 F2d 402 (1992); *US v Eastland* 989 F2d 760 (1993); *US v Kennedy* (1995) 61 F3d 494.

58 *United States v Kyllo* (Kyllo III), 190 F.3d 1041 (9th Cir. 1999).

59 *United States v Kyllo*, 809 F.Supp. 787 (D. Or. 1992).

60 *United States v Kyllo* (Kyllo I), 37 F.3d 526 (9th Cir. 1994).

61 *United States v Kyllo* (Kyllo III), 190 F.3d 1041 (9th Cir. 1999).

62 *United States v Knotts*, 460 U.S. 276 (1983).

63 *R v Wray* (1970) 11 DLR (3d) 673.

64 *R v Wray* (1970) 11 DLR (3d) 673 at 690-691.

65 A. Kenneth Pye, *The Rights of Persons Accused of Crime under the Canadian Constitution: A Comparative Perspective, Law and Contemporary Problems*, 45(4) Canadian Constitution 221-248 (Autumn, 1982).

[66] The Canadian Charter of Rights and Freedoms was enacted by the Canada Act 1982 (Eng).
[67] A. Kenneth Pye, The Rights of Persons Accused of Crime under the Canadian Constitution: A Comparative Perspective, Law and Contemporary Problems, 45(4) Canadian Constitution 221-248 (Autumn, 1982).
[68] *R v Ireland* (1970) 126 CLR 321 at 335 (Barwick J); See also *Bunning v Cross* (1978) 141 CLR 54 at 72 (Stephen and Aickin JJ); *Cleland v The Queen* (1982) 151 CLR 1 at 19-20 (Deane J); *Ridgeway v The Queen* (1995) 184 CLR 19 at 30-36 (Mason, Deane and Dawson JJ).
[69] Barwick CJ in *R v Ireland* (1970) 126 CLR 321 at 334-335. See online at http://www.hrlrc.org.au/files/JU8G8I75WP/Amnesty%20final%20submissions.pdf
[70] Stephen and Aickin JJ in *Bunning v Cross* (1978) 141 CLR 54 at 77-8.
[71] *R v Khan* [1996] 3 WLR 162.
[72] *R v Khan* [1996] 3 WLR 162 at 175.
[73] *Khan v United Kingdom* (2001) 31 E.H.R.R. 45.
[74] Telephone Intercepts: Admissibility of Evidence, 145 S.J.L.B. 28 (2001).
[75] S. Sharpe "*Electronic Eavesdropping: A Chance for Accountability*?" (1996) 146 New Law Journal 1088 at 1091.
[76] Judge Wildhaber in *Rotaru v Romania* (8 B.H.R.C. 449).
[77] Ray Purdy & Richard Macrory, Satellite photograph 21st Century evidence by, New Law Journal, (March 7, 2003).
[78] *Zagaroli v Pollock*, 379 S.E.2d 653, 656 (N.C. App. 1989).
[79] *T.R. Miller Mill Co. v Ralls*, 192 So. 2d 706, 714 (Ala. 1966).
[80] *I&M Rail Link v Northstar Navigation*, 21 F. Supp. 2d 849, 855 (N.D. Ill. 1998).
[81] *In re Vernon Sand & Gravel, Inc*., 93 B.R. 580, 583 (Bankr. N.D. Ohio 1988).
[82] *Scruggs v United States*, 959 F. Supp. 1537, 1541 (S.D. Fla. 1997).
[83] *Cobb v United States*, 471 F. Supp. 102, 103 (M.D. Fla. 1979).
[84] Frontier Dispute (*Burkina Faso v Republic of Mali*), 1986 I.C.J. (Dec. 22).
[85] Kasikili/Sedudu Island (*Namibia v Botswana*), 1999, I.C.J. (Dec. 13).
[86] *Florida v Riley* 488 U.S. 445 (1989).
[87] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986).
[88] *Olmstead v United States*, 48 S. Ct. 564, 277 U.S. 438.
[89] *US Government Guide: Olmstead v United States*
[90] Title III of the Crime Control and Safe Streets Act of 1968.
[91] *Malone v Commissioner for the Metropolitan Police* (no.2) [1979] 2 All ER 620.
[92] *Goldman v United States* 316 U.S. 129 (1942), overruled in part by Katz v United States, 389 U.S. 347 (1967).
[93] *On Lee v United States* 343 U.S. 747 (1952).
[94] *On Lee v United States* 343 U.S. 747 (1952) at 754.
[95] *Silverman v United States* 365 U.S. 505 (1961).
[96] *Silverman v United States* 365 U.S. 505 (1961). At 511.
[97] *Berger v. New York* 388 U.S. 41, 45 (1967).
[98] Stephen A. Saltzburg & Daniel J. Capra, *American Criminal Procedure: Cases and Commentary* 373 (5th ed. 1996).
[99] *Berger v New York*, 388 U.S. 41, 64 (1967) at 54.
[100] *United States v Long* 64 M.J. 57 (C.A.A.F. 2006).
[101] *United States v Maxwell* 45 M.J. 406 (C.A.A.F. 1996).
[102] *Smith v Maryland* 442 U.S. 735 (1979).
[103] *Katz v United States*, 389 U.S. 347, 359 (1967).
[104] 389 U.S. at 360-61.
[105] *Katz v. United States*, 389 U.S. 347, 359 (1967).
[106] Deirdre K. Mulligan, Reasonable Expectations of Privacy in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1569 (2004).
[107] *Kyllo v United States*, 533 U.S. 27, 34 (2001) and Georgia v. Randolph, U.S., 126 S.Ct. 1515, 1526 (2006).
[108] Deirdre K. Mulligan, Reasonable Expectations of Privacy in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1569 (2004).
[109] Smith, 442 U.S. at 746.
[110] Smith, 442 U.S. at 746-47, quoting Katz, 389 U.S. at 352.
[111] The Global Positioning System (GPS) is a space-based radio-navigation system using a constellation of satellites and provides precise position, velocity and timing information to receivers on the ground that can obtain the signals of four or more satellites simultaneously. Primarily designed for military applications, it has recently seen widespread adoption by the civilian community with an explosive growth in the number of users and applications of this technology. GPS devices have become pocket-sized, battery operated and commercially available at nominal costs. They are also being embedded into mobile phones, digital cameras, Personal Digital Assistants (PDAs) and watches. This ubiquity of location-determination devices enables tracking and monitoring of individuals by governmental entities, private entities and individuals which raises profound ethical, policy and legal issues for the society. Source: Iqbal, M.U., & LIM, S. (2007). Privacy implications of automated GPS tracking and profiling. Second Workshop on Social Implications of National Security: From Dataveillance to Uberveillance, Wollongong, Australia, 29 October 2007.
[112] Mohan, S. (2006). *Technology: GPS Keeps Parolees on a Short, Smart Leash*. Ziff Davis Media Inc. Source:http://findarticles.com/p/articles/mi_zdcis/is_200609.
[113] Newschannel.com (2007). *Parolees Monitored by GPS Tracking*. Source: http://www. newschannel9.com/onset?id=963605&template=article.html, Retrieved: March 2008.
[114] Fox News (2004). *GPS Expert Testifies in Peterson Trial*. Source:http://www.foxnews.com/ story/0,2933,132197,00.htm, Retrieved: February 2008.
[115] Jason Dearen, *Judge will allow GPS evidence in Peterson trial Oakland*, Tribune, Feb 18, 2004.
[116] 2 BvR 581/01; *the decision is available online in* German at: www.bverfg.de/entscheidungen/20050412_2bvr058101.html, The information was retrieved from the internet on April 2008.
[117] *Miller v United States*, 357 U.S. 301, 307 (1958) (quoting the Oxford Dictionary of Quotations).
[118] U.S. Const. Amend. IV.
[119] *Katz v United States*, 389 U.S. 347, 359 (1967).
[120] Sharon L. Davies and Anna B. Scanlon, Katz in the *Age of Hudson v Michigan: Some Thoughts on "Suppression as a Last Resort*", 41 UC Davis Law Review 1035, (2005).
[121] *Katz v United States*, 389 U.S. 347, 359 (1967).
[122] *Silverman v United States*, 365 U.S. 505, 512 (1961).
[123] *Katz v United States*, 389 U.S. 347, 359 (1967) at 351-52.

[124] *Olmstead v United States*, 277 U.S. 438 (1928).
[125] *Goldman v United States*, 316 U.S. 129 (1942).
[126] *Katz v United States*, 389 U.S. 347, 359 (1967) at 3513.
[127] *Katz v United States*, 389 U.S. 347, 359 (1967) at 361-62 (Harlan, J., concurring).
[128] Wayne R. LaFave & Jerold H. Israel, Criminal Procedure 125 (2d ed. 1992) supra note 183, at 126.
[129] Wayne R. LaFave & Jerold H. Israel, 1992: 126.
[130] Thomas K. Clancy, What Does the Fourth Amendment Protect: Property, Privacy, or Security?, 33 Wake Forest L. Rev. 307, 312 (1998).
[131] Wayne R. LaFave & Jerold H. Israel, Criminal Procedure 125 (2d ed. 1992) supra note 183, at 126.
[132] *Katz v United States*, 389 U.S. 347, 359 (1967) at 351.
[133] Anthony G. Amsterdam(1998), Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 403 (1974).
[134] *Florida v Riley* 488 U.S. 445 (1989).
[135] *Riley v State*, 511 So. 2d 282, 288 (Fla. 1987).
[136] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986).
[137] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986).at 238.
[138] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986) at 235.
[139] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986) at 234-239.
[140] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986) at 476.
[141] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986). At 139.
[142] *Dow Chem. Co. v United States*, 476 U.S. 227 (1986). At 138.
[143] *DuPont v Christopher* 431 F.2d 1012 (1970).
[144] Paul Rogers, *Judge Says Aerial Photos of Streisand's Mansion Not Invasion of Privacy*, San Jose Mercury News, (2004); Jane Kirtley, Bashful Barbra, Amer. Journalism Rev 62, (Feb/March 2004).
[145] Section 65B of Evidence Act 1872 (India).
[146] Section 90A of the Evidence Act 1950 (Malaysia).

REFERENCES

Alaaron, 'Illegal surveillance evidence used to prosecute JW's in Russia', Now Public News Coverage, February 11, 2011. http://www.nowpublic.com/ health/illegal-surveillance-evidence-used-prosecute-jws-russia.

American Civil Liberties Union v National Security Agency, US District Court, 18 August 2006 (Case no. 06-CV-10204)

Austen, J. 1811. *Sense and Sensibility*. Penguin Classics.

Barwick CJ in R v Ireland (1970) 126 CLR 321 at 334-335. See online at http://www.hrlrc.org.au/files/JU8G8I75WP/Amnesty%20final%20submissions.pdf

Bunning v Cross (1978) 141 CLR 54 at 72 (Stephen and Aickin JJ)

Campbell v United Kingdom (1993) 15 E.H.R.R. 137.

Cleland v The Queen (1982) 151 CLR 1 at 19-20 (Deane J)

Communication and Multimedia Act 1998 (Malaysia).

Dearen, J. 2004. Judge will allow GPS evidence in Peterson trial. *Oakland Tribune*, Feb 18.

Edwards [1996] 1 S.C.R. 12.

Evidence Act 1872 (India).

Fox News 2004. GPS Expert Testifies in Peterson Trial. http://www.foxnews.com/story/0,2933,132197,00.htm, Retrieved: February 2008.

Galves, F. 2000. Where the not-so-wild things are: computers in the courtroom, the federal rules of evidence, and the need for institutional reform and more judicial acceptance. 13 *HARV. J. L. & TECH*. 161: 229-330.

Harris, D. J., O'Boyle, M. and Warbrick, C. 1995. *Law of the European Convention on Human Rights*. London: Butterworths.

Hudson v. Michigan, 126 S. Ct. 2159, 2168 (2006).

Imwinkelried, E. 1991. The Debate in the DNA Cases Over the Foundation for the Admission of Scientific Evidence: The Importance of Human Error as a Cause of Forensic Misanalysis, 69 WASH. U. L. Q. 19 (1991).

International Organization on Computer Evidence (IOCE) First Responders Guide Template (Dec. 14, 2000). http://ncfs.org/documents/ioce2000/reports/ firstResponders.pdf

Jersild v Denmark (1995) 19 E.H.R.R. 1 at para.31.

John, T. 1996. Covert and deceptive policing in England and Wales: Issues in regulation and practice. *4 European Journal of Crime, Criminal Law and Criminal Justice* 316.

Justice under Surveillance: Covert Policing and Human Rights Standards (1998). Retrieved from internet on September 2007. http://www.cils.org/WSIS/ TechnologySurveillance/03sin.pdf.

Khan v United Kingdom (2001) 31 E.H.R.R. 45.

Klass v Germany (1979-80) 2 E.H.R.R. 214.

Ludi v. Switzerland A 238 (1992).

Markowitz, K. J. 2002. Legal challenges and market rewards to the use and acceptance of remote sensing and digital information as evidence. 12 *Duke Environmental Law & Policy Forum*: 220.

McKinney v The Queen (1991) 171 CLR 468 at 473-474.

Media Inc. http://findarticles.com/p/articles/mi_zdcis/is_200609

Mohan, S. 2006. Technology: GPS keeps parolees on a short, smart leash. Ziff Davi.s

Mulligan, D. K. 2004. Reasonable expectations of privacy in electronic communications: A critical perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1569.

Newschannel.com. 2007. Parolees Monitored by GPS Tracking. Source: http://www. newschannel9.com/onset?id=963605&template=article.html.

Ohio v. Morris, 2005 Ohio 599, (Ohio Ct. App. Wayne County, Feb. 16, 2005).

Olmstead v United States 277 US 438 (1928).

People v Hamilton 666 P2d 152 (1983).

Pye, A. K. 1982. The rights of persons accused of crime under the Canadian constitution: A comparative perspective, law and contemporary problems. *Canadian Constitution* 45(4): 221-248.

Purdy, R. & Macrory, R. 2003. Satellite photograph 21st Century evidence. *New Law Journal* (March).

R v Ireland (1970) 126 CLR 321 at 335 (Barwick J).

R v Khan [1996] 3 WLR 162.

R v Wray (1970) 11 DLR (3d) 673.

Rees v United Kingdom (1987) 9 E.H.R.R. 56.

Rees v United Kingdom (1987) 9 E.H.R.R. 56.

Ridgeway v The Queen (1995) 184 CLR 19 at 30-36 (Mason, Deane and Dawson JJ).
Sharpe, S. 1996. Electronic eavesdropping: A Chance for accountability? *146 New Law Journal* 1088-1091.
State v Fisher 686 P2d 750 (1984).
State v Johnson 716 P2d 1288 (1986).
Tessling [2004] S.C.C. 7.
The Canadian Charter of Rights and Freedoms was enacted by the Canada Act 1982 (Eng).
Thomas, R. D. 2008. The history and evolution of covert video surveillance evidence gathering. http://www.pimall.com/nais/ videohistory.html.
Thompson v Carthage School Dist 87 F3d 979 (1996).
Turkington, R. C. 2004. Legal protection for conversational and communication privacy in family, marriage and domestic disputes: An examination of federal and state wiretap and stored communications acts and the common law privacy intrusion tort. 82. *Nebraska Law Review* 3.
United States v Knotts, 460 U.S. 276 (1983).
United States v Kyllo (Kyllo I), 37 F.3d 526 (9th Cir. 1994).
United States v Kyllo (Kyllo III), 190 F.3d 1041 (9th Cir. 1999).
United States v. Kyllo, 809 F.Supp. 787 (D. Or. 1992).
US v Eastland 989 F2d 760 (1993).
US v Kennedy (1995) 61 F3d 494.
US v Kennedy (1995) 61 F3d 494.
US v Medina Reyes 877 F Supp 468 (1995).
US v Nichols 979 F2d 402 (1992).
W v United Kingdom (1988) 10 E.H.R.R. 29.
Warren, S. D. and Brandeis, L. D. 1990. The right to privacy. *4 Harvard Law Review*: 193-195.

Dr. Md. Abdul Jalil
Associate Professor
International Islamic University Malaysia
Jalan Gombak, 53100 Kuala Lumpur.
Email: abd_jalil2@yahoo.com

Abu Hena Mostofa Kamal
Assistant Professor
ASA University Bangladesh,
Shamoli, Dhaka, Bangladesh.