UNODC
United Nations Office on Drugs and Crime

Current practices in electronic surveillance

in the investigation of serious and organized crime

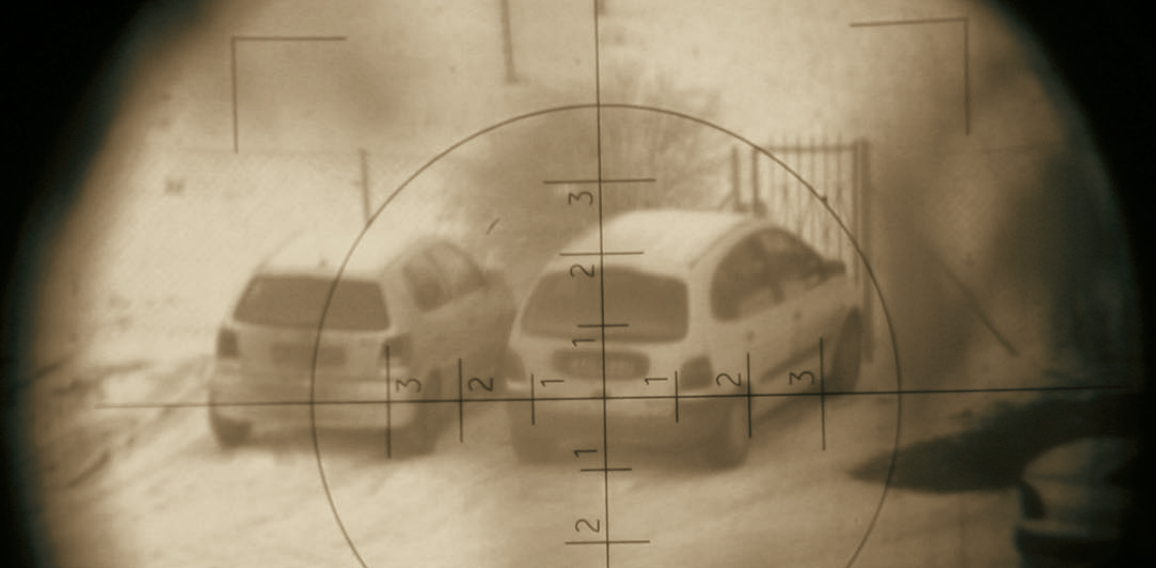
UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Current practices in electronic surveillance in the investigation of serious and organized crime

UNITED NATIONS
New York, 2009

UNITED NATIONS PUBLICATION
Sales No. E.09.XI.19
ISBN 978-92-1-148246-1

Contents



1. INTRODUCTION

1.1. The issue

The value of employing electronic surveillance in the investigation of some forms of serious crime, in particular organized crime, is unquestionable. It allows the gathering of information unattainable through other means. Some countries have utilized surreptitious electronic surveillance for nearly a century. For others it is a more recent phenomenon, and for some it is not yet utilized at all.

The use by law enforcement of electronic surveillance should not be an investigative tool of first resort, instead its use should be considered when other less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence. Even when electronic surveillance is appropriate, it will generally need to be used in conjunction with other investigation methods in order to be most effective.

For those jurisdictions without any regulation, or with legislation which is lacking in some respect, the challenge is to develop a balanced system for the use of electronic evidence gathering. The balance which needs to be struck is that between the effective use of electronic evidence gathering and the protection of citizens' rights. This includes balancing the cost of utilizing these methods against the ultimate public benefit gained from a conviction. These considerations should be weighed carefully by legislators, prosecutors, law enforcement and the like.

It should also be noted that in some countries the existence of a federal system of governance means that electronic surveillance can be regulated at both a local and at a national level. Federal law will often apply where the investigation is into crime that crosses borders, however, organized crime is of course also investigated by local law enforcement. It is not possible for this document to comprehensively consider regulation of individual states, regions or provinces within countries, although their mention will occur where valuable examples arise.

1.2 Electronic surveillance

The term "electronic surveillance" covers an array of capabilities and practices. To better understand what is meant by electronic surveillance, it is useful to break it down into parts. Surveillance has previously been defined on the basis of covert/overt distinctions, or determined according to the level of contact with the target, whether remote or direct. These distinctions might, arguably, create a false dichotomy, particularly in the context of modern surveillance technologies, where overt/covert lines are not as easy to draw. Thus, a framework based on function is perhaps more useful. The table below provides some examples. Although this too is flawed in that modern surveillance technologies will often have multiple capabilities (see below discussion at section 5.2 on regulating technologies with multiple capabilities).

Audio surveillance	*Visual surveillance*	*Tracking surveillance*	*Data surveillance*
Phone-tapping.	Hidden video surveillance devices.	Global positioning systems (GPS)/transponders.	Computer/internet (spyware/cookies).
Voice over internet protocol (VOIP).	In-car video systems.	Mobile phones.	Blackberries/mobile phones.
Listening devices (room bugging).	Body-worn video devices.	Radio frequency identification devices (RFID).	Keystroke monitoring.
	Thermal imaging/forward looking infrared.	Biometric information technology (retina scans at airports etc).	
	CCTV.		

This document confines its consideration of surveillance practices to electronic surveillance and not other forms of surveillance such as the use of covert operatives. Thus, for the purposes of this document, the terms "surveillance" and "electronic surveillance" are synonymous and used interchangeably.

1.3 The process

In December 2007 the United Nations Office on Drugs and Crime (UNODC) commenced the first of a series of meetings with expert representatives from law enforcement and prosecutorial and judicial authorities of Member States. The first informal expert group meeting on electronic evidence gathering was held from 3-5 December 2007 at the Vienna International Centre. A second regional expert group meeting for South-East Asian countries was held 17-18 March 2009 at the Digital Forensic Centre in Seoul. The meetings each brought together a small group of law enforcement officials and legal experts from different countries and regions. It is anticipated that more regular expert group meetings are to follow.

The initial goal of these meetings was to utilize participants' expertise and experiences to develop a training manual for electronic surveillance. However, due to the complexity of

this issue, it was decided that as a first step it would be useful to draft a comparative study of surveillance regulation and practices, drawing primarily upon the expert group meetings but also by completing more general research in the area. The document will broadly outline the use of and challenges faced by law enforcement and investigative authorities in a range of jurisdictions in the collection, use and storage of electronic evidence through surveillance.

1.4 Objectives

The purpose of conducting a comparative study of electronic evidence gathering is to outline current practices that will serve as an important reference tool for Member States in the regulation and use of electronic evidence gathering in the investigation of serious crime. Essentially, this document aims to:

- Contribute to an improved understanding of the global practical and legal issues presented by the use of electronic surveillance in evidence gathering, handling and use.
- Provide an account of the challenges faced by law enforcement and investigative authorities in the use of electronic evidence gathering in the investigation of serious crime.
- Provide some guidance, options and ideas for countries developing policy or regulation of electronic evidence gathering in the investigation of crime.

This document aims to assist legislative drafters, policymakers, legal practitioners, law enforcement and other investigative authorities involved in or considering electronic evidence gathering. It hopes to provide a comprehensive outline of measures and options which may be considered for incorporation into respective legal systems and operational procedures subject to the particular social, political and economic circumstances of their countries.

1.5 Scope

Countries with greater resources for policing and investigative techniques tend to have a longer history of both regulation and use of special investigative techniques. This will be reflected somewhat in the research, however, this does not represent any kind of bias, but merely an unavoidable limitation reflective of modern and historical economic realities.

Despite these limitations, the preparation of this document involved broad research across a range of regions, despite a scarcity of information in some. Thus a variety of jurisdictions and approaches are considered. Further national examples will be added and expanded upon as they are provided by participants in ongoing regional expert group meetings.

In this document, UNODC is concerned only with electronic surveillance for the investigations of serious crime. Although, it is acknowledged that electronic evidence gathering techniques may be appropriate for use in the investigation of less serious offences.

1.6 Structure

This document begins by outlining the multilateral and international framework within which electronic evidence gathering takes place in section two. Following this the focus shifts to national regimes in section three which pays particularly attention to the process and regulation of the authorization of electronic surveillance at a domestic level. Policy considerations, principles and rights which temper the use of electronic surveillance are discussed in section 4. The primary concern in this regard is the protection of an individual's right to privacy, a right necessarily infringed in the conduct of surveillance. Section five canvasses the speed of technological development and the difficulties rapid technological advancement might present to legislators, as well as the regulation of private security personnel. Finally section six concludes by discussing the technical and administrative challenges associated with the use and regulation of electronic surveillance.

1.7 Definitions

Where possible the following definitions have been taken from the United Nations Convention Against Transnational Organized Crime (TOCC):

Organized criminal group shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.

Serious crime shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.[1] (The jurisdictional disparities between what constitutes "serious crime" are discussed further below).

Special investigation techniques means techniques applied by law enforcement in the context of criminal investigations for the purpose of detecting and investigating serious crimes, and aimed at gathering information in such a way as not to alert the target persons.[2]

Warrant shall include "authorization" and "direction".[3]

Surveillance (or "electronic surveillance") is rarely itself defined in the legislation delineating its use. Instead, relevant provisions will often provide a definition of "intercept", "communication" and other more device-specific definitions, which range from succinct to

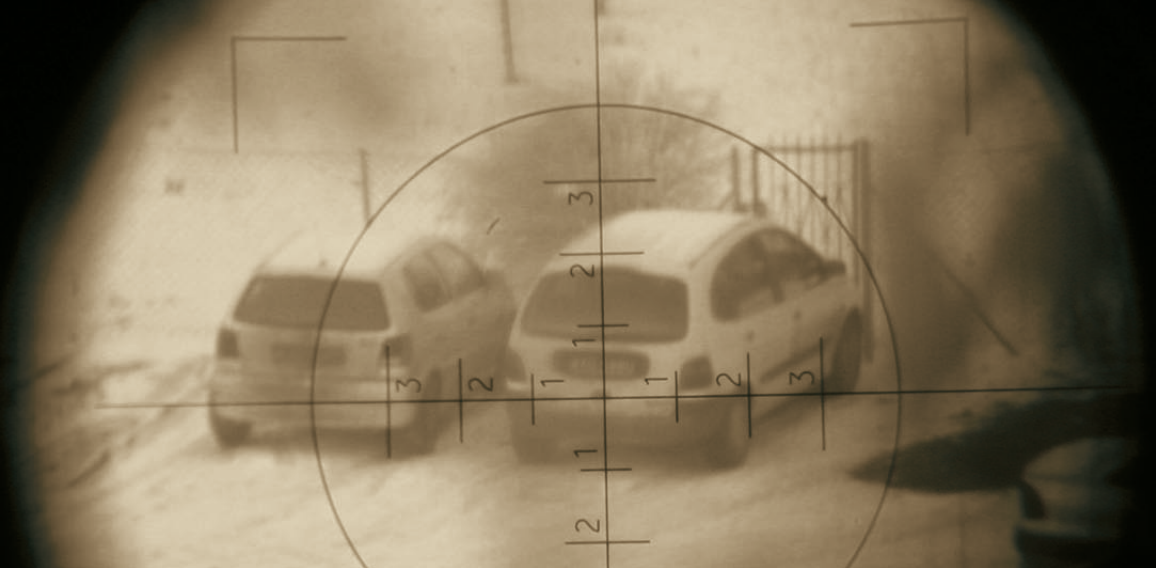
[1] *United Nations Convention Against Transnational Organized Crime* Art 2.

[2] Council of Europe Committee of Ministers, Recommendation Rec (2005) *10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism*, https://wcd.coe.int/ViewDoc.jsp?id=849269&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 at 5 February 2009.

[3] The terms "authorization" and "direction" are used by some jurisdictions to denote an authority which is, for our purposes, the same as that of a warrant, and thus these three terms are used interchangeably.

complex. For the purposes of this document, and in the context of law enforcement, surveillance is the collection or monitoring of information about a person or persons through the use of technology. This document will focus on surveillance for the stated purpose of preventing crime or prosecuting offences.

Electronic surveillance: see section 1.1.



2. MULTILATERAL AND INTERNATIONAL APPROACHES AND ISSUES

2.1 The international framework

The United Nations Convention Against Transnational Organized Crime (TOCC) is the fundamental international instrument calling upon Member States to criminalize organized and serious crime globally. Its purpose is to promote cooperation to prevent and combat transnational organized crime more effectively and constitutes the foundation document for the UNODC's anti-organized crime initiatives. Article 20 of this document refers to "special investigative techniques".

Article 20 of the TOCC provides that:

2. For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

The domestic regulation of electronic surveillance does not occur in a vacuum. Regional and international considerations are also relevant, including domestic obligations under international instruments. The right which is most frequently referred to in this context and is generally most juxtaposed against the use of surveillance is the right to privacy. The right to protection from arbitrary invasion of privacy is a fundamental human right, laid down in article 17 of the International Covenant on Civil and Political Rights (ICCPR). The ICCPR has 160 state parties and thus creates obligations which stretch across most of the world.

Article 17 of the ICCPR:

1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation

2. Everyone has the right to the protection of the law against such interference or attacks

The European Convention on Human Rights also contains a similar provision protecting the privacy of its citizens. Claims in the European Court of Human Rights (ECHR) have been made pursuant to article 8 of the European Convention on Human Rights which protects the "right to respect for private life" (see further at 4.1.1 of this document).

Article 8 of the European Convention on Human Rights stipulates:

1. Everyone has the right to respect for his private and family life, his home and his correspondence

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The ECHR has dealt with several cases involving electronic surveillance conducted by law enforcement.[4] These are expanded upon further in section 4.1.1 of this document.

Concern for the protection of the right to privacy has also been enshrined in the CoE's European Code of Police Ethics. The Code specifically protects an individual's right to privacy vis-à-vis police conduct. Further, the CoE Code stipulates that the use of data obtained by police shall be dealt with in accordance with international data protection principles.[5]

[4] Case of the Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria (no. 62540/00) 28 June 2007; Elahi v United Kingdom (no. 30034/04) 20 September 2006; Hewitson v United Kingdom (no. 50015/99) 27 August 2003; Khan v United Kingdom (no. 35394/97) 12 May 2000; Malone v United Kingdom (no. 8691/79) 2 August 1984. Note that the Human Rights Act 1998 (UK) adopted the European Convention on Human Rights into United Kingdom law and this may have contributed to a disproportionate increase in cases from the United Kingdom being brought before the ECHR in the last decade.

[5] Council of Europe, *European Code of Police Ethics*, ss 41 and 42. The "data protection principles" were established in 1980 by the OECD. They broadly prohibit the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

2.2 Cross-border cooperation

As organized crime increases its global reach, it is important that law enforcement also have (at least) reciprocal global capabilities. Indeed with the increased globalization of organized criminal networks, the need for effective cross-border cooperation is likely to increase. In practice, requests for assistance for cross-border electronic evidence gathering or surveillance is often avoided for both practical reasons to do with efficacy, and frustration with bureaucratic delays.

2.2.1 Cross-border cooperation: jurisdictional issues and challenges

Cross-border investigations present unique challenges to law enforcement and other investigating authorities. The use of electronic evidence gathering in another jurisdiction will require a request from the investigating jurisdiction to the country in which surveillance is anticipated to occur. The latter will likely only pursue an investigation where the relevant offence is also an offence under their own criminal law. Practically this is often the case. However, ongoing electronic evidence gathering from one jurisdiction into another is rarely smooth or speedy. In the actual initiation of electronic evidence gathering, bureaucratic procedures and red-tape can cause relatively lengthy delays. In addition, the jurisdiction requested to conduct the surveillance will want to understand the evidence so far obtained in order to determine whether an offence against their criminal law, has been, is being, or is likely to be committed.

Evidence obtained in a country other than that in which the criminal trial will occur can be of questionable admissibility. Domestic law in this area is complex and invariably, jurisdictions will each possess somewhat different systems to maintain the chain of custody. More generally, where evidence has been gathered in a jurisdiction not the host of the criminal trial, it may be difficult to satisfy the local legal requirements regarding admissibility of evidence.

In both expert group meetings, participants noted that requesting data from another jurisdiction is problematic. Challenges faced in this respect include:

- Delay;
- A lack of commitment and flexibility from the authority from which evidence is requested;
- The form in which evidence is provided to the requesting jurisdiction is one that can cause prosecutorial challenges;
- Differing definitions of serious criminal offences between jurisdictions.

2.2.2 *Intangible data held on computer networks spanning several countries*

The cross-jurisdictional challenge is compounded by the increase in intangible data held on foreign servers but accessible locally. The 2009 expert group meeting raised the issue of accessing data hosted in another jurisdiction, such as information stored on a foreign computer network, but accessible domestically. Discussion centred on the extent to which this presents a legal predicament in which one of two implications will follow. Either it will be necessary to limit what law enforcement can do, or law enforcement will be conducting investigations which could be unlawful in the jurisdictions hosting the data they are accessing. This predicament is further exacerbated where the jurisdiction of the network hosting the electronic data is not known.

2.2.3 *Mutual legal assistance treaties (MLATs)*

Article 18 of the TOCC extends an obligation on states parties to provide mutual legal assistance in the investigation and prosecution of serious offences. The provision of mutual assistance appears to be reflected in some, but few, of the national legislative instruments regulating electronic evidence gathering.[6] Organizations such as EUROJUST and EUROPOL facilitate and encourage cross-border cooperation regionally, but such initiatives are not found across all regions. Thus, there is scope for further development of effective strategies to assist and encourage mutual legal assistance in the investigation and prosecution of serious offences.

Historically MLATs have played an important role in cross-border criminal investigation. In general such treaties seek to expedite and assist cross-border cooperation in criminal investigations. Usually each country will designate an authority for direct communication between the countries or jurisdictions in such instances where cross-border assistance may be required. However, no MLAT gives open permission for cross-border surveillance to occur; they merely operate, in the most part, to create open lines of communication. An authorization or warrant is only valid in the country in which it was obtained. If country A wishes to conduct surveillance in country B it may offer the grounds on which it considers such surveillance necessary, but ultimately it is country B's sovereign decision. Assistance may be denied where the offence is not one mutually recognized by the countries parties to the agreement or where certain offences are specifically excluded.

2.2.4 *Multilateral agreements*

With the increasing speed of technological advancement, communication and world travel, the internationalization of crime has also grown exponentially. In this context multilateral agreements are of increasing relevance.

[6] Regulation of Investigatory Powers Act 2000 (UK) s 5.

The EU Convention on Mutual Legal Assistance in Criminal Matters was adopted on 29 May 2000. It provides an example of multilateral cooperation in cross border surveillance.

The Convention 'aims to encourage and modernise cooperation between judicial, police and customs authorities within the Union as well as with Norway and Iceland by supplementing provisions in existing legal instruments and facilitating their application.'[1]

Articles 17-20 deal with the interception of communications and provide the basis upon which a request for interception can occur and require that the receiving Member State shall undertake to comply with such a request.[2]

[1] European Commission, Justice and Home Affairs <http://ec.europa.eu/justice_home/fsj/criminal/assistance/wai/fsj_criminal_assistance_en.htm> at 3 January 2009.

[2] Similarly, the Inter-American Convention on Mutual Assistance in Criminal Matters has been in force since 1996 and has more than 20 state parties in the Americas, however, it does not specifically consider telecommunications interception nor surveillance

Where no MLAT or other relevant treaty or agreement exists, the TOCC may itself serve as a basis for cooperation between Member States.

In the expert group meetings frustration was expressed with the delay that can be caused to an investigation by following international protocols. Participants commented that currently informal cooperation seemed a more effective cross-jurisdictional tool. That is, having personal contacts in foreign investigating agencies. The primary problem with this approach is that if formal mechanisms are not followed the evidence gathered may be inadmissible in court in the requesting jurisdiction.

2.2.5 Other networks and programmes

Informal and formal networks of those involved in the investigation of serious crime are increasingly valuable for the smooth operation of cross-border cooperation in electronic evidence gathering. In both expert group meetings, participants were unanimous in their support for further initiatives to improve cross-border cooperation. One example of recent efforts in this regard comes out of the United Kingdom.

The United Kingdom Crown Prosecutors Service is currently putting forward a proposal for the establishment of a "Global Prosecutors E-Crime Network" (GPEN), an initiative supported by the International Association of Prosecutors. Their proposal points out that the global increase in internet use has

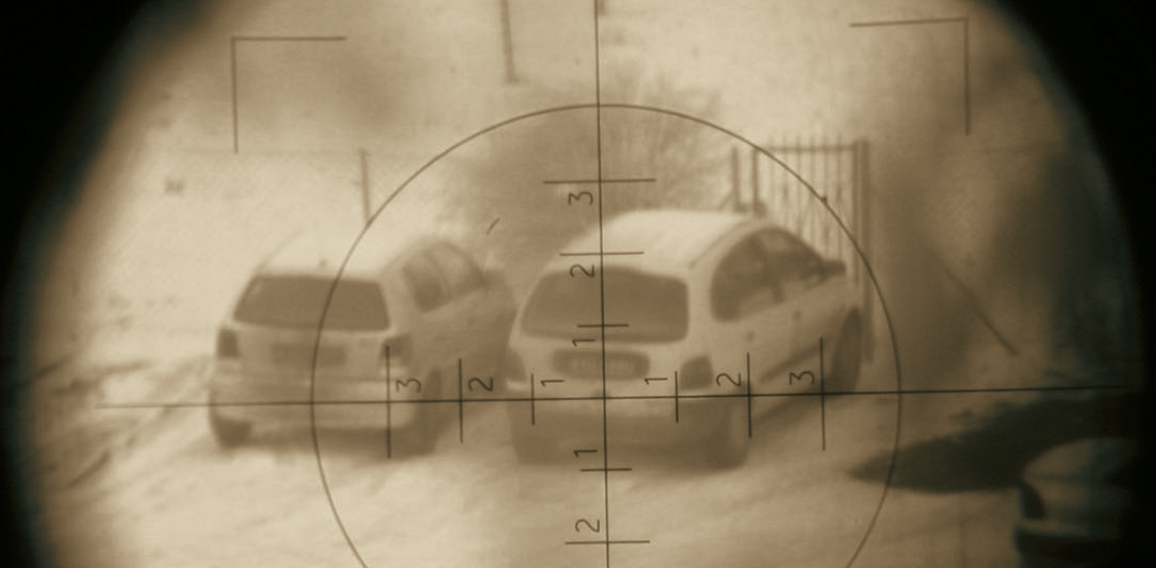
> [C]lear implications for law enforcement and prosecution agencies as criminals exploit the opportunities that information and communication technology provides. On the internet, there are no global boundaries for criminals and it is widely recognised that e-crime is the most rapidly expanding form of criminality. The technical nature of such cases is increasing, as is the availability of the tools with which to commit these crimes.

> There is also an increasing number of sophisticated international computer attacks. So it is essential that prosecutors are able to both advise police officers during the investigation and prosecute such cases effectively.
>
> To this end, the GPEN will consist of a secure website which serves as a database for prosecutors from all over the world and also provides online training courses and presentations.

Other networks that focus on cross-border surveillance issues include:

- The Cross Border Surveillance Working Group
- The AGIS programme, which is focused on operational issues (organized by Austria and includes countries neighbouring Austria)
- International Surveillance Committee. This group meets once a year and includes Australia, New Zealand, the United States, Canada, the Netherlands and the United Kingdom.
- European Electronic Surveillance Working Group
- European Judicial Network[7]
- Red Iberoamericana de Cooperación Jurídica Internacional (IBERRED)
- Southeast European Prosecutors Advisory Group
- The International Association of Chiefs of Police

[7] See in relation to mutual legal assistance in criminal matters: www.consilium.europa.eu/cms3_fo/showPage.asp?id=475&lang=EN&mode=g# at 3 January 2009.



3. REGULATION: WARRANTS AND AUTHORIZATIONS

3.1 When is a warrant or authorization required?

The use of electronic evidence gathering techniques by law enforcement is commonly regulated by a warrant-based system, subject to some form of oversight.[8] Not all electronic surveillance will require a warrant. Electronic surveillance conducted by law enforcement in a public place will not always require a warrant. This will usually include, for example, visual surveillance such as in-car video systems, body-worn video devices[9] and police-monitored CCTV. These forms of surveillance are typically regulated by codes of practice and guidelines, if at all.[10]

Where surveillance is conducted in a situation where the subject of surveillance would hold a reasonable expectation of privacy, then a warrant will usually be required. These forms of surveillance include for example the interception of communication such as via landline phones, mobile phones and VOIP and the installation and monitoring of

[8] *Interception of Communications and Surveillance Ordinance* (Hong Kong) ch 589, s 3; *Criminal Procedure Code* (Germany) s 100a; *Criminal Procedure Code* (Republic of Serbia) arts 226 and 228; *Code of Criminal Procedure* (Poland) ch 26; *Code of Criminal Procedure* (Slovakia) s 88; *United States Code* Title 18 ch 119 ss 2510-2519; *Crimes Act 1961* (New Zealand) part 11A; *Canadian Security Intelligence Service Act* (R.S., 1985, c. C-23) (Canada) part II; *Criminal Code* (R.S., 1985, c. C-46) (Canada) part XV ss 487.01 and 492.1; *Regulation of Investigatory Powers Act 2000* (UK); *Surveillance Devices Act 2004* (Australia); *Telecommunications (Interception and Access) Act 1979* (Australia); *Regulation of Interception of Communications and Provision of Communication-related Information Act 2002* (South Africa).

[9] For example, the United Kingdom has trialled and subsequently introduced the use of cameras in the hats of police officers. See: Home Office, Police and Crime Standards Directorate, 'Guidance for the Police use of Body-Worn Video Devices' (2007) http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/guidance-body-worn-devices?view=Binary at 5 February 2009

[10] For example: Home Office, Police and Crime Standards Directorate, 'Guidance for the Police use of Body-Worn Video Devices' (2007) http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/guidance-body-worn-devices?view=Binary at 5 February 2009; Office of the Information and Privacy Commissioner for British Columbia, *Public Surveillance System Privacy Guideline*, (2001) www.oipc.bc.ca/advice/VID-SURV(2006).pdf at 5 February 2009. Note also that codes of practice and guidelines also exist for the practice of covert surveillance, however, these are usually complementary to a legislative regime, for example see: United Kingdom Home Office, *Covert Surveillance Code of Practice* http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/covert-cop?view=Binary at 5 February 2009.

tracking devices. The attainment of authorization in advance ensures that the evidence is obtained lawfully which may have implications for the admissibility of that evidence.

Where a warrant to conduct surveillance is not required, there are usually other factors limiting its use. These include consideration of the subject's reasonable expectation of privacy, the attainment of some other permission (albeit non-judicial),[11] and the requirement of notice for overt surveillance, which are discussed in this document in sections 3.2 and 4.

The method of regulation in this regard varies. In some jurisdictions authority to conduct surveillance is issued by the court in accordance with legislation. In other countries, the courts have a primary regulatory role. That is, a judge may permit surveillance to occur on the merits of the case without any legislative restrictions.

3.2 The applicant

In some jurisdictions an application for a warrant to intercept communication must first be approved by a very senior public servant, such as the Attorney-General, before the application may be heard before a judge.[12] In some countries an authorization may also be applied for by other public servants of a specified level of responsibility.

It should be noted that the respective roles of prosecutor and law enforcement officer differ substantially in common law as compared to civil law jurisdictions. Whereas in common law systems, police have relative autonomy over the investigative process, in civil law systems this is not necessarily the case. The public prosecutor often plays a leading role in overseeing the conduct of the investigation. In many civil law systems, for example, the prosecutor is able to authorize a warrant to conduct electronic surveillance.[13] Conversely, in traditional common law systems, the prosecutor can never issue warrants.

> The United States federal jurisdiction offers an example of an exception to this general trend. While, technically speaking, the prosecutor neither issues nor applies for the warrant, it is standard practice that the prosecutor approves and oversees the application, as prepared by law enforcement officers, before it is reviewed by a judge.

The applicant for electronic surveillance was the subject of some debate at the 2009 expert group meeting. Opinions were divided as to whether the prosecutor should have oversight in relation to applications for authorization to conduct electronic surveillance. The group

[11] See for example *Anti-Corruption Act 1997* (Malaysia) s 39 which allows the Public Prosecutor to authorize the interception of communications; or section 184(2) and 184.2 of the Canadian *Criminal Code* which permits the interception of communications where the consent of the originator or intended recipient of the communication has been obtained. Note also that there are often general exceptions for the incidental interception of communications by telecommunications personnel, for example section 3(3) of the *Regulation of Investigatory Powers Act 2000* (UK).

[12] Title 18 Chap 119 § 2516 US Code

[13] *Code of Criminal Procedure* (Slovak) s 88; *Criminal Procedure Code* (Germany) s 100b(1); *Police Act* (Poland) art 19a(3); *Anti-Corruption Act 1997* (Malaysia) s 39(1).

was divided largely down civil law/common law experience and it is clear that there is a difference between the two systems on this issue.

In general, common law countries argued that for reasons of accountability it was important that the officer applying was the person/s conducting the investigation (usually, but not always, police). In civil law countries it is viewed that only prosecutors should have the authority to appear before a judge to apply for authorization. Given that this matter is one of structures fundamental to both systems and which are unlikely to change, the question of which system is to be preferred is moot. Difference along similar lines also arose in relation to whether the prosecutor should have the capacity to authorize electronic surveillance (see below at section 3.3).

3.3 The authorizing body

3.3.1 Who authorizes the use of electronic evidence gathering techniques?

Where a warrant for electronic surveillance is required, jurisdictions tend to use one of three authorities to oversee and permit surveillance to be carried out. These authorities are (in no particular order):

- Judge
- Prosecutor
- Commission/commissioner or other authority

Some jurisdictions have set up special independent commissions or authorities to oversee the use of electronic surveillance by the government, including by law enforcement.

> In the state of Queensland in Australia, section 324 of the *Crime and Misconduct Act 2001* allows the Governor in Council to appoint a "public interest monitor" to monitor applications for, and the use of, surveillance warrants and covert search warrants. It specifically states that the person must not be a member of the police service or the Office of Public Prosecutions.

In other jurisdictions permission to conduct electronic surveillance in the investigation of serious crime is a matter for the prosecutor.

> In Poland the prosecutor may authorize surveillance and the recording of the content of telephone conversations in order to detect and obtain evidence for pending proceedings or to prevent a new offence from being committed.

Whether a prosecutor could or should be authorized to permit electronic surveillance without further oversight was a subject discussed at the 2009 expert group meeting.

Some participants expressed concern that a prosecuting authority might not be sufficiently far removed from the investigation to make an independent decision on the use of surveillance as balanced against the subject's right to privacy.

3.3.2 Surreptitious electronic evidence gathering by consent

In some countries where a person who is a party to the conversation consents to the conversation being taped, that is sufficient to allow electronic evidence gathering to occur and for its recorded form to be admissible as evidence. This is the case notwithstanding that other parties to the conversation may have no knowledge that the recording is taking place. The rationale for this approach is that if conversations to which one party consents to recording were inadmissible, then the court would ultimately not hear the conversation. Instead it would be reliant on the testator's memory as to what was said as he or she recounted it to the court. Advocates of this approach suggest that it ensures that the court hears the most accurate evidence.

Pursuant to section 184.2 of the Canadian Criminal Code, a private communication may be intercepted where a person who is a party to the conversation consents. There must still be an application for authorization brought before a judge. However, there are fewer elements which must be proven in order for this type of authorization to be granted as compared to a situation where no party consents or knows about the interception. The judge needs to be satisfied that:

> *(a)* there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed; and
>
> *(b)* either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and
>
> *(c)* there are reasonable grounds to believe that information concerning the offence referred to in paragraph *(a)* will be obtained through the interception sought

As a result, the application is thus less onerous to prepare and, arguably, also less onerous to process.

Other jurisdictions do not require any form of authorization where a party to the conversation consents to the recording. This is particularly useful where an undercover operative is involved.

In new legislation proposed in New Zealand the recording of a voluntary conversation by a consenting party will not require any form of authorization. Nor is there any restriction on audio recording of private conversations if entry onto the premises where the conversation has occurred is pursuant to lawful authority and that authority covers the right to hear the things being recorded.

3.4 Notice

In some countries there is a requirement that after covert surveillance has taken place, the subjects of the surveillance must be notified that this has occurred. Although this is usually subject to exceptions and will not necessarily include all those persons who were recorded or observed partaking in the relevant communication or activity such as non-targeted family and friends of the suspect.

In Canada, section 196 of the Criminal Code requires that within 90 days of the interception (or other period fixed by the judge issuing the authorization) of the interception, the person who was the object of the interception shall be notified in writing of such interception.

Where the investigation is continuing an extension of time can be granted by a judge of a superior court on application by the Attorney-General or the Minister. This exception to the notice requirement applies not only where the investigation of the initial offence is continuing but also where the initial surveillance uncovered evidence of other crimes not the subject of the first warrant. The extension of the period within which notice must be given is not to exceed three years.

Similarly, in Japan the Act on the Interception of Communications requires that the subject of intercepted communications must be notified of the interception within 30 days of the surveillance having been completed. Where an ongoing investigation might be compromised by such notice, a district court judge can extend the period of time within which the subject must be notified.

Other countries require notice to be given not whenever surveillance is conducted but instead only when it has been conducted unlawfully.

Section 48 of chapter 589 of the Hong Kong SAR Ordinance requires that where the interception of communications is deemed to have occurred unlawfully, notice must be given to the person targeted.

3.5 Contents of warrant application

Where a warrant-based system of regulation is in place, there are usually requirements as to what an application for a surveillance warrant must contain. Typically these will include the following:

- The subject/target of surveillance and an outline of the facility and location of surveillance;

- The necessary duration of the surveillance;
- An outline of the investigative techniques that have been tried and failed or why they cannot be employed;
- The justification for the use of surveillance (further discussed below);
- To whom the warrant is issued.

In the new surveillance regime being introduced in New Zealand, warrant applications can be made orally, electronically or by personal appearance. Personal appearance can be dispensed with where the judicial officer is satisfied that there is adequate information to enable a decision to be made without the personal appearance of the applicant.

3.6 Justification for warrant

Each jurisdiction elucidates in differing terms the circumstances that must exist in order for a warrant for the use of electronic surveillance to be issued. The applicant must generally prove that the use of electronic surveillance is necessary in the interests of national security or for the purpose of preventing or detecting crime.

Sometimes for the use of phone-tap or interception devices, the applicant must show that the relevant crime falls within a stipulated category of "serious crime". What constitutes "serious crime" varies between countries. As mentioned above, under the TOCC, a serious crime is one that under national legislation is punishable by a sentence of four or more years. States parties to the TOCC should review whether their electronic surveillance regime is in line with the Convention.

Some countries use the maximum term of imprisonment as a benchmark for measuring "serious crime", others create a list of offences considered "serious crimes". However, certain offences appear to arise almost universally. These include the investigation of terrorism-related offences, treason, and serious violent offences such as murder and kidnapping. At the lower end of the scale there is more disparity. For example, in some instances the investigation of theft and fraud related offences may be sufficient for the issue of a warrant.[14] Some jurisdictions also permit the issue of electronic surveillance warrants where the matter of concern affects the country's economic well-being[15] or is part of an international agreement of mutual assistance.[16] Others provide that a warrant for the use of a surveillance device may be issued for the investigation of any crime, provided that the issuing judge is satisfied of certain matters.[17]

[14] *Criminal Procedure Code* (Germany) s 100a; *Crimes Act 1961* (New Zealand) s 312B; Title 18 Chap 119 § 2516 US Code.
[15] *Regulation of Investigatory Powers Act 2000* (UK) s 5; Title 18 Chap 119 § 2516 US Code
[16] *Regulation of Investigatory Powers Act 2000* (UK) s 5
[17] *Criminal Code* (Canada) s 184.2(2)(a) and (3); *Listening Devices Act 1984* (New South Wales, Australia) ss 15-16.

Often legislation will expressly outline the factors that a decision-maker must consider in determining the grant of a warrant for the use of surveillance for the investigation of crime. Obviously the basis for such an application will be that there are reasonable grounds to believe a relevant offence has been, will be or is being committed.[18] Other factors for consideration commonly include:

- The evidentiary value of the evidence that the surveillance is likely to obtain;[19]
- Whether there are alternative means of obtaining the evidence sought;[20]
- Whether it is in the best interests of the administration of justice to issue the warrant.[21]

The applicant's belief that the perpetration of a particular serious crime is imminent or ongoing, and that its investigation necessitates the use of electronic surveillance, must meet a certain standard of reasonableness.[22] The onus is upon the applicant to prove that their belief meets this standard. Evidence of "reasonable belief" is typically provided in one of three ways: in writing, on oath, or both in writing and on oath. While many jurisdictions do not specify the precise matters to which the written or oral evidence must attest, others are quite specific about its requisite content. In addition, the presiding judge will have legislative (if not inherent) authority to require additional evidence to be provided.

3.7 What a warrant authorizes

3.7.1 Scope

Warrants for the use of surveillance by law enforcement are limited in scope. Most national systems which regulate the use of electronic surveillance will prescribe the information that a corresponding warrant must contain. This is usually substantively the same as that required within the application, which is both logical and necessary for law enforcement to understand the scope of lawful surveillance which they have been permitted. Consequently, and to a large extent, the warrant will mirror the application. Thus the duration, target and location and type of surveillance will appear on both the application and the warrant. The latter will differ from the former at the discretion of the decision-maker.[23]

The warrant will usually authorize the installation and retrieval of a surveillance device into or onto a specific place or thing. Sometimes there is a requirement that if the circumstances that justified the use of surveillance (and thus also the warrant) cease to exist, the person responsible for the surveillance will be obligated to cease the surveillance.[24]

[18] *Criminal Code* (Canada) s 487.01; see also Crimes Act 1961 (New Zealand) s 312B; *Criminal Procedure Code* (Germany) s 100a.

[19] *Listening Devices Act 1984* (New South Wales, Australia) s 16.

[20] *Crimes Act 1961* (New Zealand) s 312B and 312C; see also *R v Araujo* [2000] 2 S.C.R. 992 (Canada) which established in the Canada that in order to satisfy the investigative necessity test set out in 186(1)(b) of the Criminal Code, the police must establish that there is no other reasonable method of investigation.

[21] *Criminal Code* (Canada) s 487.01.

[22] This standard will vary somewhat between jurisdictions.

[23] See 2.2.2 for a list of typical requirements for the content of a surveillance warrant application

[24] *Criminal Procedure Code* (Germany) s 100b (4); Title 18 Chap 119 § 2510(5) US Code; *Surveillance Devices Act 2004* (Australia) s 21.

In Australia, section 21 of the Surveillance Devices Act stipulates that where the chief officer is satisfied that the use of a surveillance device under a warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of a relevant offence or the location or identity of the offender, then that chief officer must take steps to ensure that the use of the surveillance device is discontinued.

In general, the principles or policy considerations which limit the use of electronic evidence surveillance in the investigation of serious crime include:

- *Necessity:* that the use of electronic evidence gathering is necessary to gather the evidence or information required.
- *Subsidiarity:* that other less intrusive forms of inquiry or investigation are not sufficient to gather the confidentiality: that there are mechanisms in place to protect the confidentiality of the information obtained, including the privacy of third parties not the subject of the authorization or warrant.
- *Judicial control:* that the process of evidence gathering is overseen by a judge or independent other of a certain requisite and specified level of authority.
- *Proportionality:* that the intrusion into privacy is proportionate to the seriousness of the suspected offence and the evidence it is anticipated will be obtained.

Where these principles do not specifically appear (in one form or another) in legislation they are sometimes incorporated into other regulatory instruments such as codes of practice.[25]

For example, in Guatemala's recently enacted *Regulations for the Application of the Investigative Technique of Telephone Tapping and Other Forms of Interception of Communications,* principles limiting the use of telecommunications interceptions are specifically listed as follows:

Article 3. Principles. The principles guiding this special technique shall be:

(a) Principle of necessity. The principle of necessity shall be understood to mean that there is a need to use the technique of interception of communications where existing investigative techniques reveal the use, in offences committed by members of organized criminal groups, of communication methods identified in the Law against Organized Crime;

(b) Principle of confidentiality. The principle of confidentiality shall be understood to mean the requirement that the activities forming part of this special technique shall be known only to the officials authorized by the law;

[25] See for example paragraphs 2.4 to 2.5 of the United Kingdom Home Office 'Covert Surveillance Code of Practice' issued pursuant to section 71 of the *Regulation of Investigatory Powers Act 2000*.

> *(c)* Principle of judicial control. The principle of judicial control shall be understood to mean the requirement that the activities forming part of this special technique shall be known only to the officials authorized by law;
>
> *(d)* Principle of appropriateness. The principle of appropriateness shall be understood to mean that, in view of the nature of the offence concerned, it may be decided that the interception of communications will be effective in obtaining background information that will make it possible to avoid, interrupt or throw light on the commission of offences by members of organized criminal groups."

3.7.2 Duration

The length of time for which a warrant may authorize the use of electronic surveillance is usually expressly limited in the legislation. The duration varies between jurisdictions which regulate this, and ranges from 10 days to three months.[26] However, most systems that stipulate a time period for surveillance also provide that extensions of time may be permitted, where necessary, upon application to the original issuer. Additionally, the issuer will usually retain the right to revoke the warrant at any time.

3.8 Use of surveillance data

There are limitations on the use of data, recordings and images acquired as a result of electronic surveillance. Where evidence is obtained through the use of surveillance not authorized under a warrant, its admissibility becomes questionable. Conversely, where evidence has been lawfully obtained pursuant to a warrant or relevant authorization, it is likely to be admissible, subject to ordinary rules of evidence. Rules regarding the admissibility of evidence play a somewhat lesser role in civil law jurisdictions due to the wide-ranging discretion of the trial judge to act as inquisitor and call what evidence he/she thinks fit and also, arguably, because there is no jury to "taint".

3.8.1 Use of surveillance data: intercepted communications

> In India, pursuant to section 46 of the Unlawful Activities (Prevention) Amendment Act 2004, evidence gathered by the interception of communications is admissible as evidence against the accused provided that the accused has been furnished with a copy of the authorizing order under which the interception occurred at least 10 days before trial. Alternatively, where it is not possible to give 10 days notice, the evidence may still be admissible provided that the judge determines that the failure to give 10 days notice does not prejudice the proceedings.

[26] *Act on Interception of Electronic Communication* (Japan) (10 days); *Criminal Procedure Code* (Germany) s 100b (2) (3 months); *Code of Criminal Procedure 1997* (Poland) art 238 (3 months); *Code of Criminal Procedure* (Slovakia) s 88 (6 months); *Regulation of Investigatory Powers Act 2000* (UK) s 9 (3 months for standard warrants); *Surveillance Devices Act 2004* (Australia) s 17 (90 days).

This can be compared with the situation in the United Kingdom and Hong Kong SAR. It should be noted, however, that the United Kingdom might soon be amending its legislation in this regard.

Conversely, in the United Kingdom the evidence obtained by interception of communications is prima facie inadmissible in proceedings, subject to certain exceptions.[1] The primary use of intercepted material is as information to assist an investigation. Once that intercepted material has served its purpose in this regard, it is destroyed.[2]

[1] These exceptions include in any proceedings for a relevant offence. What constitutes a relevant offence is specifically defined and primarily includes offences against telecommunications and interception legislation rather than serious criminal offences. *Regulation of Investigatory Powers Act 2000* (UK) ss 17 and 18.

[2] Note that this position is currently under review in the United Kingdom.

In Hong Kong SAR conversations recorded as a result of the interception of communications are not ever admissible as evidence. Rather a witness must attest to the conversation as he or she heard it. Police have expressed concern that the admission of the recorded data as evidence might compromise police methods by alerting organized crime syndicates to the techniques used.

3.8.2 Transcription

At the first expert group meeting, participants pointed out that transcribed evidence of recorded conversations is often questioned by defence counsels on the basis of its accuracy. The transcribing of audio into a verbatim transcript is often a tedious and lengthy task relegated to clerks not necessarily familiar with the case. It is important to ensure that the transcript of recorded voices is precisely accurate in order not to leave the prosecution's case exposed to what would be a legitimate attack by the defence counsel should the transcription be inaccurate. This is especially important where the material to be transcribed is in a foreign language. It is thus crucial that such transcription is diligently monitored by persons intimately involved in the case.

The Spanish system avoids this dilemma entirely by requiring that all transcription be undertaken by a clerk of the court in the presence of both counsel for the defence and prosecution. Any disagreement as to the accuracy of the transcription is thus resolved at this stage of proceedings, rather than during the trial.

Although in some countries it is the audio itself that is played to the court, it is the transcripts which decipher conversations which are often muffled or virtually inaudible. As such, conflicts over accurate transcription are likely to continue even where the audio is admissible as evidence. Therefore it is advisable to have available and offer both the audio and a transcript of the audio to the trier of fact.

3.8.3 *Information obtained about persons or offences not the subject of the warrant*

The situation becomes more complex where a warrant was obtained to conduct covert surveillance on person A and in doing so evidence is obtained against person B. Similar evidentiary issues arise where evidence of offences other than those for which the warrant was obtained is discovered. At least one jurisdiction specifically provides that such information may be disclosed to other law enforcement officers as appropriate, or otherwise used in the proper performance of law enforcement duties.[27] Another allows such information to be retained as long as it is necessary for the protection of national security or the prevention or detection of serious crime.[28] This is an area in which there is no consistency of approach between jurisdictions. Two examples of converse approaches are provided below.

In Canada, where the authorized electronic surveillance uncovers evidence of an offence not mentioned in the authorizing warrant, the surveillance may continue unabated. The evidence thus obtained is considered "windfall evidence" and is lawful. However, if an extension of time is required, beyond that authorized in the initial warrant, the additional offences or suspects discovered must be mentioned in the subsequent application.

The Canadian approach is in contrast to that of Spain.

In Spain, if a judicial authorization is given for electronic evidence gathering to be conducted and the subsequent surveillance uncovers information pertaining to additional offences not anticipated or mentioned in the initial authorization then surveillance must cease. The overseeing judge must be contacted in order to obtain authority for the electronic evidence gathering to continue and to include the gathering of evidence in relation to the additional offence/s.

3.8.4 *Chain of custody*

Maintaining the integrity of the material obtained through electronic surveillance is essential for ensuring that it will be admissible as evidence in court. This issue was raised at both expert group meetings. Countries tend to take slightly different approaches to maintaining the integrity of evidence.

In relation to the interception of communications, in Japan all conversations in the authorizing period are recorded and then sealed by the person conducting the electronic surveillance. That material is then kept by the judge and is admissible as evidence.

[27] Title 18 Chap 119 § 2517(5) US Code.

[28] *Regulation of Investigatory Powers Act 2000* (UK) ss 15(3) and (4)(a).

In Jordan, where the originals of all recordings of intercepted communications are sent to the court for safekeeping, the investigating agency retains only the copies.

The length of time for which captured electronic surveillance data is stored is also important and may have implications for rights of the person/s subject to the surveillance.

In Italy, at the end of the trial the judge directs the prosecutor as to what is to be done with the electronic evidence gathered. For example, if no crime was found to have been proven the computer may have to be returned, or if paedophilia was found to be on it, the judge may order that the computer be destroyed.

In other jurisdictions the length of time for which material is retained will depend on whether it is relevant to other ongoing investigations, and the length of time in which the accused has a right to appeal. It should be noted that retaining material for long periods can raise technical issues: technology is quickly outdated and as a result the medium needed to play such recordings become obsolete.

3.9 Reporting requirements

Although not a universal requirement, it is common practice that reports are required to be compiled detailing the issuance and use of surveillance warrants.[29] Where reporting requirements exist, there are two distinct types, each operating as a check on the use of surveillance warrants by law enforcement. The first is regular reporting or updates to the issuing judge on the success or otherwise of the electronic surveillance, this occurs during the term of the surveillance. The second is statistical reporting, usually annual, which will often include, among other things, details of the number of warrants applied for, approved and refused.

3.9.1 Reports to issuing judge

A number of systems call for the law enforcement officer to whom the warrant was provided to report to the issuing judge as to the manner in which the power conferred by the warrant was exercised, and the results obtained.[30] Some countries require that the judge be given an update on the progress of the electronic evidence gathering every few days. Moreover, due to the confidential nature of electronic surveillance operations, reporting is often done either orally in front of the judge who authorized the surveillance or a written report is personally delivered to the judge. In our initial expert group meeting some

[29] *Criminal Procedure Code* (Germany) s 100e; *Crimes Act* (New Zealand) s 312P; *Criminal Code* (Canada) s 195.

[30] *Crimes Act 1961* (New Zealand) s 312P; *Criminal Procedure Code* (Germany) s 100e; *Spanish Criminal Law Procedure* art 579.

participants found this unnecessarily onerous, particularly where reporting must be done in person as often as every 72 hours. This may require some flexibility when frequent reporting is required, for example, every few days.

> In India the authority appointed to issue orders of authorization to intercept communications may require regular reporting at intervals that he/she thinks fit. The regular reports should indicate that progress has been made towards the authorized objective and that there is a continued need for ongoing interception.[1]

[1] *The Prevention of Terrorism Act 2002* (India) s 42(2).

3.9.2 Annual reports

Other systems require a more general annual report, which will usually include statistical details such as the number of surveillance device warrants applied for, approved and refused.[31] Some jurisdictions require that the report lists the number of persons arrested, or against whom proceedings were commenced, as a result of surveillance carried out pursuant to a warrant.[32] At least one country requires a tally of the number of warrants approved and declined by each respective judge.[33]

However, during the first expert group meeting it was noted that such reports can paint a false picture. For example, a distorted impression can be given where reports require a list of the number of warrants issued compared against the number of convictions in that year. Trials often last longer than a year and the conviction that is the result of the electronic evidence gathering may not occur until years after the surveillance was conducted. These reports remain of value but care should be taken in interpreting their contents.

3.10 Implications of non-compliance

As mentioned above, in those jurisdictions where authorization is required for the conduct of electronic evidence gathering, it is usually an offence to either intercept communications, or conduct covert surveillance without a warrant, particularly in circumstances where the subject has a reasonable expectation of privacy.[34] Thus, *prima facie* the officer who conducted such surveillance will be criminally liable. However, this is subject to a number of exceptions, including for example where a warrant has been obtained[35] or where the officer is acting on good faith that the surveillance has been authorized.[36]

[31] *Criminal Code* (Canada) s 195.

[32] *Interception of Communications and Surveillance Ordinance* ch 589 div 5 s 49 (Hong Kong); *Criminal Code* (Canada) s 195(2).

[33] *Interception of Communications and Surveillance Ordinance* ch 589 div 5 s 49 (Hong Kong).

[34] For example: *Criminal Code* (Canada) s 184(1); *Interception of Communications and Surveillance Ordinance* (Hong Kong) ch 589 div 5 ss 4-5;

[35] For example *Interception of Communications and Surveillance Ordinance* ch 589 div 5 s 4 (Hong Kong); *Telecommunications (Interception and Access) Act 1979* (Australia) s.7

[36] *Criminal Code* (Canada) s 184(2); *Interception of Communications and Surveillance Ordinance* ch 589 div 5 s 65 (Hong Kong).

Criminal liability of the officer who conducted unlawful surveillance is rarely (if ever) pursued. Instead, in common law jurisdictions, the most significant outcome of failing to conduct the relevant surveillance lawfully is that evidence obtained will be inadmissible in proceedings against the suspect. This is not necessarily so in civil law countries where evidence obtained by the unlawful use of electronic surveillance will not necessarily render it inadmissible.

Unlawful surveillance, or unlawful use or disclosure of information obtained by surveillance, may also constitute a breach of respective privacy laws and this could expose an agency or individual to a civil suit.

Section 54 of the Hong Kong SAR Interception of Communications and Surveillance Ordinance imposes an obligation on the head of a department to report non-compliant behaviour to the Police Commissioner on Interception of Communications and Surveillance. The report should include details of the case as well as any disciplinary action taken in respect of the officer/s responsible.

In Denmark and Norway electronic evidence gathering is conducted under the supervision of the prosecutor. If the prosecutor proceeds with electronic evidence gathering methods without judicial authorization, this will not render the evidence obtained inadmissible. Instead this will be a factor that the judge considers at trial and will affect the weight to be given to the information obtained as a result. Nevertheless, illegal electronic evidence gathering by a prosecutor is a very rare occurrence. If it is not the result of an honest mistake, it can result in disciplinary action, including criminal charges.

3.11 Emergency or urgent circumstances

Often regulating instruments will contain special provisions for a situation where law enforcement or the relevant investigating authority reasonably believes that urgent or emergency circumstances exist and that these circumstances require the immediate use of electronic evidence gathering or the interception of communications. As with other areas of surveillance, there is no universal approach across jurisdictions.

In situations constituting an emergency, legislation will usually permit the use of covert surveillance either without a warrant or with the authorization of an office-bearer of lesser authority than that usually required. What constitutes an emergency is usually where there is a serious and imminent threat to national security, persons or property,[37] but may also include circumstances where valuable evidence might be lost without the use of surveillance.[38]

[37] *Telecommunications (Interception and Access) Act 1979* (Australia) s 10; *Surveillance Devices Act 2004* (Australia) s 28; *Criminal Code* (Canada) s 184.4; Title 18 Chap 119 § 2518(7) US Code.

[38] *Police Act* (Poland) art 19; *Interception of Communications and Surveillance Ordinance* (Hong Kong) s 20.

In the Republic of Korea, where there is an imminent risk of a serious crime being committed which may cause death or serious injuries to individuals, the investigating officer may conduct electronic surveillance without the authorization of the court. However, he or she must obtain judicial approval of the use of surveillance within 36 hours of the surveillance having begun.

An emergency authorization will sometimes be limited in duration, in some jurisdictions only a few days[39] and it is often required that during this time steps are taken to make an application for a warrant to be issued, either retrospectively[40] (as per the example above) or for any necessary ongoing surveillance which will extend beyond the period permitted under the emergency authorization.

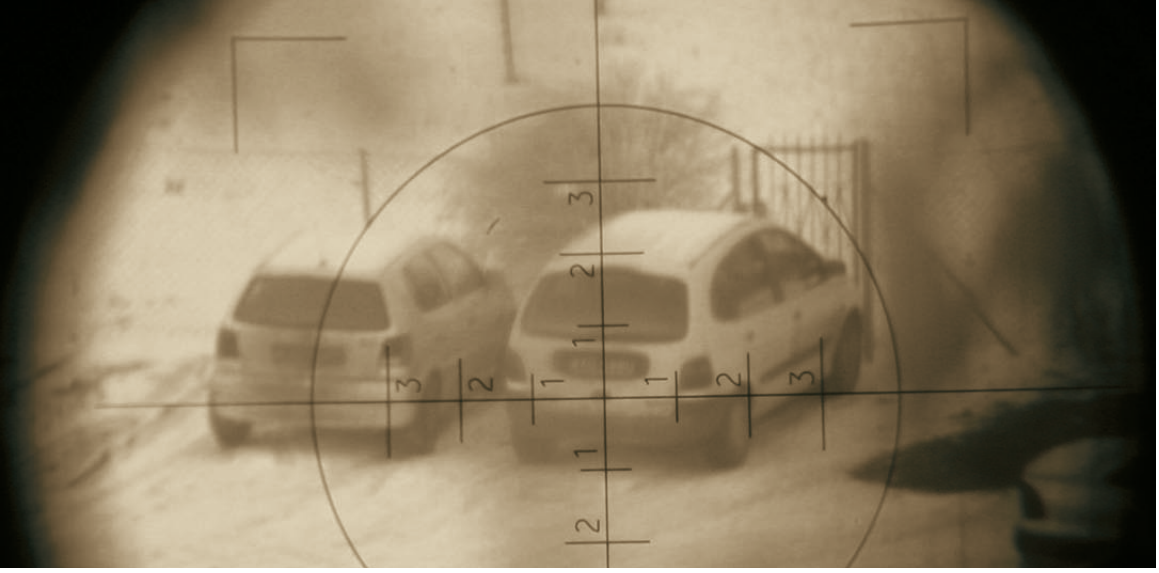
In Australia, emergency authorizations to conduct electronic surveillance may be issued where there are serious risks to person or property, or a risk of loss of evidence.[1] The law enforcement officer who possesses such concerns may apply to an "appropriate authorizing officer" for authorization in these circumstances. The appropriate authorizing officer is a Commissioner of Police or Senior Executive of the Australian Federal Police, where ordinarily judicial authorization would be required.[2]

[1] *Surveillance Devices Act 2004* (Cth) pt 3.

[2] Note that this Act does not apply to telecommunications interception, as that particular form of special investigative technique is regulated separately in Australia. However, the Act does apply to listening devices, tracking devices, data surveillance devices and optical surveillance devices.

[39] See for example Interception of *Communications and Surveillance Ordinance* (Hong Kong) s 21 allows emergency authorization of surveillance for a period of up to 48 hours.

[40] Title 18 Chap 119 § 2518(7) US Code.



4. OTHER PRINCIPLES GOVERNING ELECTRONIC EVIDENCE GATHERING BY LAW ENFORCEMENT

4.1 Reasonable expectation of privacy

As mentioned earlier, there is a clear and inherent tension between the consideration of the right to privacy held by citizens and the legitimate security concerns of governments. The potential of electronic evidence gathering to interfere with the right to privacy is often a paramount consideration in determining the use of electronic surveillance, whether or not a warrant is required. The right to privacy has been exercised by persons the subject of surveillance as a shield against the admissibility of the captured material as evidence.[41] Obviously, this is especially so where the right to privacy has been enshrined as a human right in domestic legislation, or implied through judicial interpretation into respective constitutions, or other legislation.[42]

In this regard, it is worth noting that in the last decade the relevant reports of various national law reform commissions have consistently viewed the interest of the State in conducting surveillance as balanced against the citizen's right to privacy.[43] Thus, from a policy standpoint, surveillance and the right to privacy are indeed juxtaposed. The "right to privacy" argument is more easily overcome where surveillance has occurred in a public place or where there is no reasonable expectation of privacy. However, there is an increasing perception that a reasonable expectation of privacy can exist outside the places traditionally thought of as "private".

[41] For example: *Khan v United Kingdom* (Application No 35394/97) Judgment 20 May 2000 (ECHR); *Hunter v Southam Inc.* (1984) 2 S.C.R 145 (Canadian Supreme Court); *Kyllo v United States* 533 U.S. 27 (2001) (US Supreme Court).

[42] *European Convention on Human Rights* art 8; *Human Rights Act 1998* (UK) sch 1; *Canadian Charter of Human Rights* art 8; *Fourth Amendment to the Constitution of the United States of America; Constitution of Spain* art 18; *Constitution of South Africa* art 14

[43] For example: Australian Law Reform Commission 'Review of Australian Privacy Law' (2007); Law Reform Commission of Ireland, 'Report on Privacy: Surveillance and the Interception of Communications' (1998); The Law Reform Commission of Hong Kong, 'Report on Privacy: Regulating the Interception of Communications' (1996).

The recent guidance issued by the United Kingdom Home Office on police use of Body Worn Video Devices (such as those installed in the hats worn by police officers) notes that "recordings of persons in a public place are only public for those present at the time, so those situations are therefore still regarded as potentially private".[1]

[1] Home Office, Police and Crime Standards Directorate, 'Guidance for the Police use of Body-Worn Video Devices' (2007) http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/guidance-body-worn-devices?view=Binary at 5 February 2009.

4.1.1 Right to respect for private life in the European Court of Human Rights

The ECHR is given particular attention because it is the only regional legal institution which has dealt comprehensively with right to privacy considerations in relation to electronic evidence gathering by law enforcement and because the examples it provides are both relevant and comprehensive.

Article 8 provides that everyone has the right to respect for his private and family life, his home and his correspondence (see section 2.1 for a full reproduction of article 8). There have been several cases before the European Court of Human Rights (ECHR) where article 8 has been invoked to challenge the admissibility of evidence obtained by electronic surveillance in criminal trials. Two examples are provided below. The first a specific instance challenging the admissibility of electronic evidence gathering and the second a case where the legitimacy of an entire act was challenged in the ECHR on the basis that it provided for possible breaches of the right to respect for private life.

Khan v United Kingdom[1]

In this case the applicant had travelled from Pakistan to England with a friend. At the airport in England the friend was found to have heroin in his possession with a street value of about £100,000. The applicant, Khan, was also interviewed and denied any involvement. He had no drugs in his possession, and was subsequently released. Khan then visited a friend. In this residence (for other unrelated reasons) the police had installed a listening device. Khan was subsequently recorded having a discussion in which he admitted that he had been a party to the importation of drugs. Consequently he was charged with drug importation offences.

The applicant alleged that the recording of conversation which took place constituted a violation of article 8 of the ECHR. The United Kingdom Government did not dispute that the surveillance constituted a breach of article 8 § 1 but contended that it was in accordance with article 8 § 2. That is, they argued that the use of covert surveillance was in accordance with the law and necessary in a democratic society for the prevention of crime.

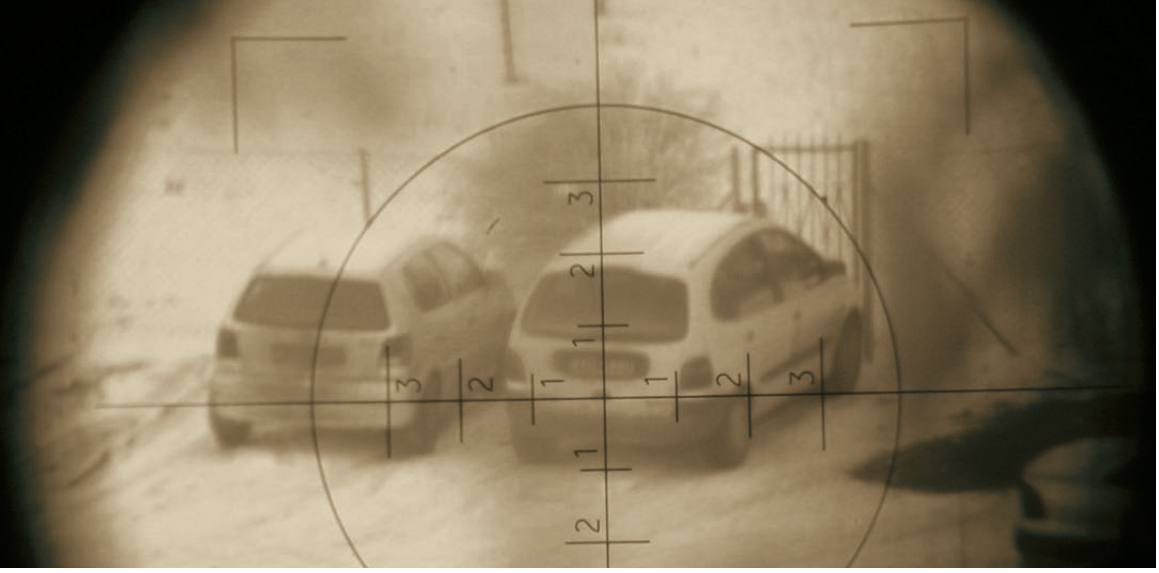
The European Court of Human Rights held unanimously that the interference with the applicant's right to private life was not in accordance with the law. In part this was because, at the time of the alleged intrusion, the United Kingdom had only guidelines and no legislative regime for the use of covert surveillance by the police. Thus there was no law with which the surveillance could accord.

1 (Application No 35394/97) Judgment 20 May 2000 (ECHR).

While the legislative gap that existed in the United Kingdom at the time of the above decision has since been remedied, the implications of this decision for those EU jurisdictions without regulation of covert surveillance remain pertinent. Where electronic surveillance is unregulated it may constitute a breach of article 8 and, if so, thus leave the work of prosecutors and law enforcement in gaining a conviction in local courts open to further appeal. Additionally, decisions of the ECHR resonate beyond the EU to those countries States Parties to the ICCPR or those which have the right to privacy constitutionally or legislatively enshrined.

The ECHR has also heard at least one case that challenged the legitimacy of surveillance regulating legislation in and of itself, on the basis that the relevant legislation permitted behaviour that would be in violation of article 8.[44] In that case it was found *inter alia* that there had been a violation of article 8 and that the law did not afford sufficient protections against the risks of abuse inherent in any system of covert surveillance.

[44] *Case of the Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (no. 62540/00) 28 June 2007.



5. ADDITIONAL POLICY CONSIDERATIONS

5.1 Regulation of other users of electronic surveillance: private security

In the context of the increasing use of private security firms to conduct what are/were essentially law enforcement activities, the regulation of private investigators and security personnel is worth considering. Moreover, it is a topic that was briefly broached by one country with lesser-developed surveillance regulation during our initial expert group meeting.

Generally private investigators and security personnel are subject to separate regulation which limits their capacity to engage in electronic evidence gathering. Private security are often regulated domestically through a system of licensing where certain criteria must be met before a licence is issued. The licence will permit certain limited and specified guarding or investigative activities.

Our research has not uncovered a regulatory regime that explicitly permits surreptitious telecommunications interception by private investigators. Private security firms may be able to use other forms of covert electronic evidence gathering such as bugs or video surveillance devices in situations where the subject does not have a reasonable expectation of privacy. It is not uncommon that legislation protecting personal data will also include consideration of the role and affect of private detectives or investigators in this regard.[45]

5.2 Regulating the use of changing technologies

Regulation of the use of surveillance by law enforcement (and others) changes regularly and is under frequent review. This is due in part to the rapid development of technology and also in response to domestic policy concerns.

[45] See for example *Personal Data Protection Code* (Italy) Title XI s 135.

By way of illustration, some of the formal reviews of surveillance regulation recently completed, and ongoing, are listed below:

- *New Zealand.* In June 2007, the New Zealand Law Commission released its report on "Search and Surveillance Powers" which recommends fundamental changes to the regulation of surveillance in New Zealand. To date, the only surveillance activities subject to regulation in New Zealand are the interception of communications by police and the use of tracking devices by police and customs. This has created uncertainty for law enforcement in the conduct of criminal investigations.[46]
- *Australia.*
  - In September 2007, the Australian Law Reform Commission released its report entitled "Review of Australian Privacy Law", which included consideration of communications interception legislation.
  - The Victorian Law Reform Commission is currently reviewing the regulation of the use of surveillance in public places.
- *United States.* On October 2 2007, the United States Congress Committee on Energy and Commerce announced its investigation into warrantless wiretapping.[47]
- *Hong Kong.* In 2007, the Hong Kong Law Reform Commission released its report "Privacy: The Regulation of Covert Surveillance".[48]
- *South Africa.* The South African Law Reform Commission is in the final stages of its inquiry into privacy and data protection, its discussion paper, released in late 2005, recommended greater regulation of data protection.[49]

Surveillance devices will often now have multiple capabilities, and as a result national systems are having to develop regulation which can deal with multifunction devices and even devices or surveillance capabilities which might not yet exist.

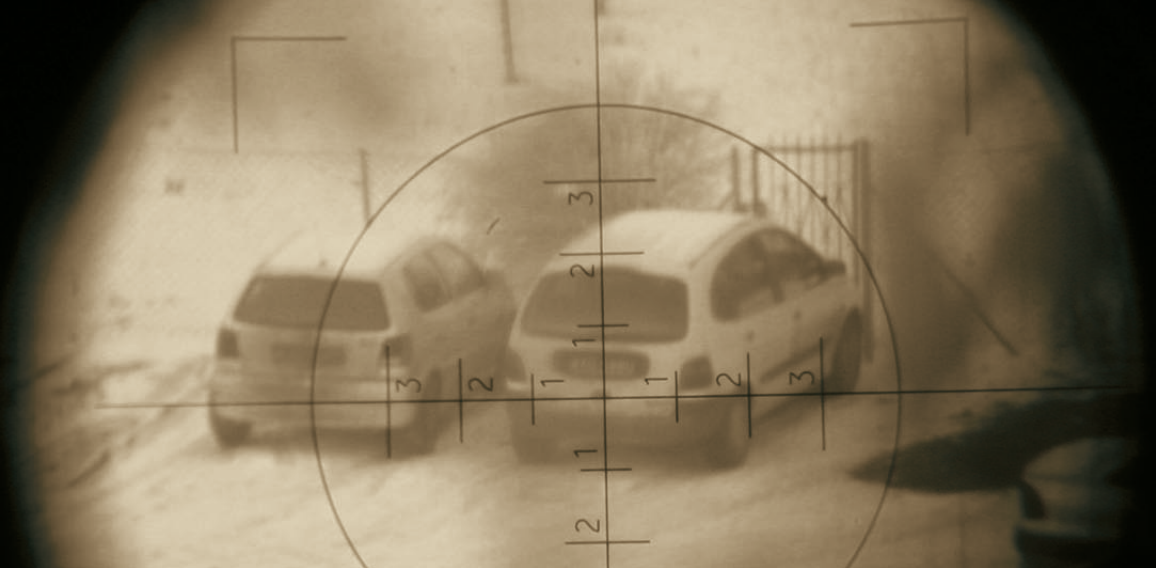
New proposed legislation in New Zealand proposes a residual warrant scheme to account for new surveillance technologies. Thus where a new technology is anticipated for use to conduct surveillance in a criminal investigation, the investigating officer may apply for a warrant permitting its use despite the fact that the legislation has not yet anticipated that particular device or function. This avoids the situation where a new evidence is deemed inadmissible because it was unauthorized where the lack of authorization occurred only because the technology used was not anticipated in the legislation.

[46] New Zealand Law Commission, *Search and Surveillance Powers* (2007) 25-26.

[47] United States Congress Committee on Energy and Commerce, *Committee Opens Investigation into Warrantless Wiretapping* http://energycommerce.house.gov/Press_110/110nr98.shtml at 5 February 2009.

[48] Hong Kong Law Reform Commission, *Privacy and the Regulation of Covert Surveillance* (2006) www.hkreform.gov.hk/en/publications/rsurveillance.htm at 5 February 2009.

[49] South African Law Reform Commission, *Discussion Paper 109: Privacy and Data Protection*, www.doj.gov.za/salrc/dpapers.htm at 5 February 2009.



6. ADDITIONAL CHALLENGES

6.1 Resource constraints

Electronic evidence gathering is necessarily a costly endeavour. It requires technology adequate to undertake the surveillance, which must be frequently updated to ensure that it remains effective. Additionally it requires sufficient manpower to not only undertake the surveillance or interception but also to process the information obtained. Often the material collected is in significant quantities and might take several officers a very lengthy period to disseminate. Thus the strain on resources is significant and may discourage investigative agencies and law enforcement from conducting such investigations.

6.2 Training

In the 2009 expert group meeting some participants emphasized that lack of specialist training for law enforcement significantly hindered their capacity to engage in electronic evidence gathering to any significant degree. Moreover, prosecutors and judges are not always aware of the latest technological advances for the conduct of electronic surveillance.

Training in the laws, regulations and operative procedures for conducting overt electronic surveillance should be mandatory for investigative officers involved in managing such techniques. Training is recommended also for other officials such as prosecutors and judges who will be involved in cases where such evidence is or may be used.

The Commission of the European Union recognizes regional judicial training as a new and important task for the European Union in particular in facilitating mutual legal assistance between Member States. In the Communication from the Commission to the European Parliament and the Council it is noted:

> "The adoption of a corpus of legislation that has become substantial and must now be implemented by the practitioners of justice, coupled with the development of the mutual recognition principle, which rests primarily on a high degree of mutual confidence between the Member States' judicial systems, means that judicial training is now a major issue."

6.3 Technological challenges

Inevitably regulation will always be playing catch-up with technological developments. And is not always the case that the technological advancements are in the hands of the investigators before they are in the hands of criminals. Resource constraints in particular limit the attainment and thus use of hi-tech surveillance equipment and technologies by investigating authorities. Some of the current technological challenges faced by law enforcement and investigators in pursuing electronic evidence gathering were discussed in the expert group meetings, particular that which took place in 2007. Some of the issues raised are listed below and they highlight the increasing complexity of such investigations.

6.3.1 Telephone number portability and roaming

Telephone number portability means that consumers can change telecommunication service providers (TSPs) without changing their phone number. In addition, mobile phones can roam different TSP networks. This can make it difficult for investigators to identify which service provider through which to intercept communications and this in turn can cause delay to investigations and thus risk failing to obtain important evidence.

6.3.2 Email, chat and voice over internet protocol (VOIP)

Email, chat and VOIP present unique technical and legal challenges. VOIP interception allows monitoring to occur in real-time. However, this risks the inadvertent recording or monitoring of material which could be legally privileged.[50] If the material is privileged it is not only likely to be inadmissible as evidence but it could throw into question the other evidence gathered in the investigation by the same technique.

Interception or monitoring of computer information is also complicated by the suspect's use of wireless internet hot-spots in places such as cafes, airports and other areas where free wireless internet services are available. In addition, legitimate computer software packages can create technological obstacles. A range of privacy protection and virus protection software is now available to consumers. Because the software is designed to protect personal computers from attack, the software can interfere with computer-based electronic evidence gathering.

[50] Generally, information or a conversation is considered legally privileged where its content is being divulged for the purpose of receiving legal advice

6.3.3 Pre-paid mobile telephones and internet cafés

Participants at the 2007 expert group meeting pointed out that the use of pre-paid mobile telephones by persons suspected of involvement in organized crime rendered tracking and interception of communications difficult if not near impossible. Similarly, the use of VOIP at internet cafés prevented easy interception of communications.

> In Italy it is a requirement that every person who purchases a mobile phone (whether pre-paid or on a plan), and every person who utilizes an internet café, must provide identification to the proprietor. The proprietor is required to keep a register of all such purchases. The Italian police have an agreement with one telecommunications provider which provides them with instantaneous access to the register of telephone owners. Other European countries have indicated that they will likely soon follow suit.

6.3.4 Telecommunications service providers

Telecommunications service providers (TSPs) play an important role in enabling the interception of communications. Participants in the initial expert group meeting suggested that although TSPs are generally cooperative, there have been instances where they have been reluctant to comply when there is no actual or perceived commercial advantage in doing so. Some countries have dealt with this by enacting legislation which not only requires TSPs to ensure that their networks are compatible with interception requirements of police but also that any request for assistance by law enforcement or the relevant authority is complied with, regardless of the cost.

> In Canada and in France there have been difficulties where TSPs have refused to cooperate with law enforcement unless they were paid. In Canada some TSPs encrypt or encode telecommunications so that even if intercepted the communications could not be deciphered. The dollar amounts the service providers demanded to permit access to the pure communication have been substantial and in some instances severely hindered the immediate furtherance of the investigation.

Some participants in the 2007 expert group meeting advocated the idea that TSPs should be offered immunity from liability for undertaking any acts pursuant to a warrant or authorization. Others baulked at the prospect of legal immunity for *any party*, including prosecutors and law enforcement, on the basis that all should be held accountable for their actions. It was pointed out by those of the latter perspective that where the interception was lawful and undertaken pursuant to a warrant, then no prosecution against them would succeed in any case.

Some participants had found that there was a lack of adequate training for the staff of TSPs, and that this could hinder a criminal investigation. Where information was required from them, TSPs were often unsure of what they could legally provide to the police. Thus

the level of cooperation from TSPs can differ depending on whether their staff (rightly or wrongly) believe they are allowed to disclose information or enable electronic evidence gathering to occur. Thus, improved training of relevant telecommunications staff was suggested in order to better facilitate the smooth operation of an investigation.

In 1994 the United States introduced the *Communications Assistance for Law Enforcement Act* which amended the United States Code. It clarified the obligations of telecommunications service providers to cooperate with and assist law enforcement in the interception of telecommunications. Included among a service providers' duties is an obligation to ensure that equipment and services are installed, designed or modified to have necessary surveillance capabilities. It requires telecommunications companies to assist law enforcement when requested, and to do so in a timely fashion.

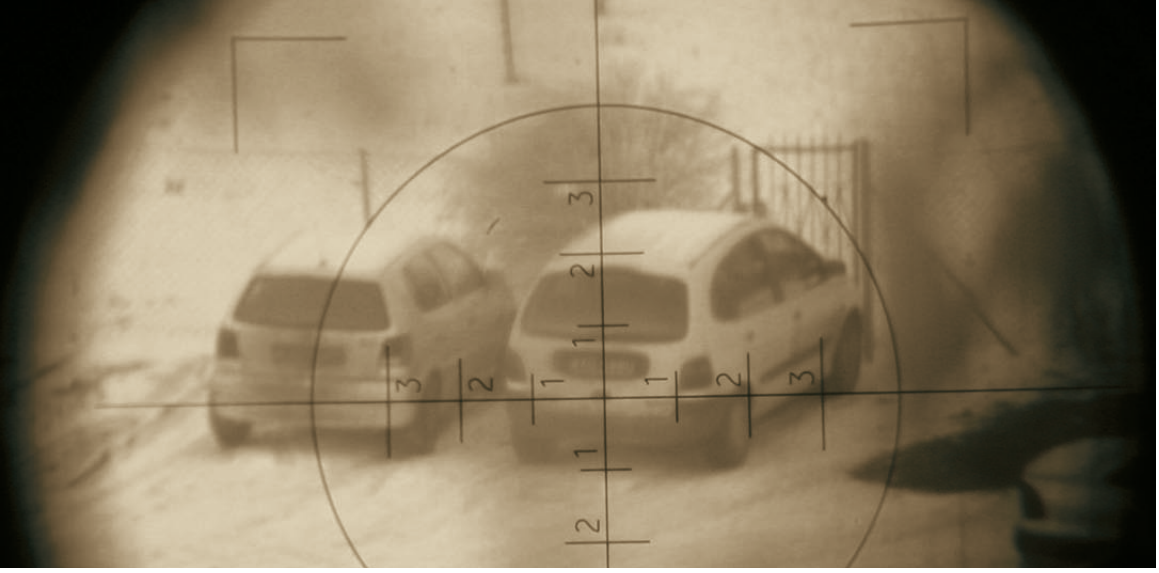
The Act also establishes the "Department of Justice Telecommunications Carrier Compliance Fund" for making payments to telecommunications service providers and manufacturers to assist in the cost of becoming compliant with the Act.[1]

[1] Title 47 Chap 9 § 1021 US Code.

6.3.5 Tracking

Tracking devices throw up another set of technological challenges. These devices are quite heavily power dependant and thus their use can be limited to that which their power source (often batteries) can sustain. Similarly, when tracking a suspect using the built-in GPS in a mobile phone, pulling the location drains the battery of the mobile phone.

When regulating for tracking devices it is important that legislators bear in mind not only the use of tracking devices which can be covertly installed into or onto objects by authorities but also the use of technology which already exists in objects such as GPS in cars and mobile-phones. That is, any system of authorization should anticipate the use by law enforcement of tracking devices already existent in the suspect's possession.



7. REQUEST FOR COMMENT

This document has broadly outlined some of current practices and challenges in electronic evidence gathering in the investigation of serious and organized crime. It has been developed with the aim of helping member states in a increasingly complex area. Comment on this document is welcomed and would be of great assistance. Also, the provision of relevant law, guidelines and training materials from all jurisdictions would be gratefully received and may be sent to Ms. Karen Kramer, Senior Expert, at karen.kramer@unodc.org

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

United Nations publication
Printed in Austria

ISBN 978-92-1-148246-1

Sales No. E.09.XI.19

V.09-86322—November 2009—640

USD 11
ISBN 978-92-1-148246-1