



# General Order J-11

Subject <b>ELECTRONIC SURVEILLANCE PROCEDURES</b>		
Distribution <b>"A"</b>	Date Published <b>11 July 2011</b>	Page <b>1 of 5</b>

*By Order of the Police Commissioner*

## POLICY

It is the policy of the Baltimore Police Department that members of the agency comply with the full text of the Maryland Wiretapping and Electronic Surveillance and Electronic Communication Law, Courts and Judicial Proceedings, Title 10, Subtitle 4, 4A, 4B, all applicable judicial orders and the following procedures. **Consultation with a prosecutor is required in every case.** Should an element of law or judicial order be more restrictive, that law or judicial order shall prevail.

## GENERAL

**Access of Electronic Communication in Storage** – A law enforcement officer may require a provider of electronic communications service to disclose the contents of an electronic communication that is in storage for 180 days or less or for 180 days or more without prior notice to the subscriber only with a search warrant. After 180 days the information may also be obtained under Grand Jury subpoena or court order with prior notice from the officer to the subscriber or customer.

**Access of Transactional Records** – A law enforcement officer may require a provider of electronic communications service to disclose transactional records or other information, pertaining to a subscriber or customer of the service with no requirement of notice, if the officer uses a warrant, a Grand Jury or court subpoena, a court order or has the consent of the subscriber. Transactional records do not include the contents of any communications to which provisions for access to communications in storage (above) apply.

**Cellular Telephone** – Non-consensual interception of a communication, made through a cellular telephone, requires a court order.

**Cordless Telephone** – A court order is required to intercept the radio portion of a cordless telephone communication, transmitted between the cordless telephone handset/headset and the base.

**Court Ordered Interceptions** – The Attorney General, State Prosecutor or any State's Attorney may apply to a judge of a court of competent jurisdiction, who may grant an order authorizing a law enforcement officer to intercept a wire, oral or electronic communication. A court order may be granted if the judge determines that the interception might provide or has provided evidence that an individual is committing, has committed, or is about to commit one of the below offenses:

1. Murder
2. Kidnapping
3. Rape
4. A sexual offense in the first or second degree

5. Child abuse in the first or second degree
6. Child pornography
7. Gambling
8. Robbery
9. Felony arson and/or felony malicious burning
10. Bribery
11. Extortion
12. Dealing in a controlled dangerous substance
13. A fraudulent insurance act
14. An offense relating to destructive devices
15. Sexual solicitation of a minor
16. An offense relating to obstruction of justice
17. Sexual abuse of a minor
18. A conspiracy or solicitation to commit an offense listed above

And, there is probable cause to believe a particular communication, concerning that offense will be obtained through the interception;

And, normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed if tried or would be too dangerous;

And, there is probable cause to believe the facilities from which or the place where the wire, oral or electronic communications are to be used or are about to be used are released to, listed in the name of, or commonly used by the person, who is the subject of the interception.

**Electronic Surveillance** – The aural or other interception of the contents of a wire, electronic or oral communication through the use of any electronic, mechanical or other device.

**Electronic Surveillance Device** – Any instrument the design of which renders it primarily useful for electronic surveillance or which is used or intended to be used for such a purpose. Electronic surveillance devices shall include, but not be limited to, body microphones or a “wire” suction cup or contact microphones, directional microphones, wall spikes, electronic stethoscopes, covert transmitter, tape recorders used to secretly record private conversations, pen registers, “clone pagers”, radio signal detection devices and trap and trace devices.

**Lawful Acts – No Court Order Required** – under the following circumstances:

1. **All Party Consent** – It is lawful for a person to intercept a communication when that person is a party to the communication and where all parties to the communication have given prior consent to the interception.
2. **Certain Communications Readily Accessible to the Public** – It is lawful for any person to access certain electronic and radio communications, which are readily accessible to the general public. (Refer to full text of the law for specific circumstances that apply.)
3. **Emergency Communications Center** – It is lawful for an officer, employee or agent of a governmental emergency communications center to intercept a wire or oral communication where the officer, agent or employee is a party to a conversation, concerning an emergency.

4. **Hostage and Barricade Situations** – It is lawful for a law enforcement officer acting in a criminal investigation or any person acting at the prior direction and under the supervision of such an officer to intercept a communication when any person has created a barricade situation and probable cause exists to believe a hostage may be involved, when the person is a party to the communication or one of the parties to the communication has given prior consent to the interception.
5. **Officer's Safety** – It is lawful for law enforcement personnel to use body wires to intercept oral communications in the course of a criminal investigation, if there is reasonable cause to believe that an officer's safety may be in jeopardy. However, communications intercepted under this exception may not be recorded or used against a defendant in a criminal proceeding.
6. **One-Party Consent** – It is lawful for a law enforcement officer acting in a criminal investigation or for any other person acting at the prior direction and under the supervision of such officer to intercept a communication for the purpose of providing evidence of any of the aforementioned offenses (listed on pages 1 and 2 of this Order) including Distribution of Non-Controlled Substances as CDS and Drug Paraphernalia, when the person is a party to the communication or one of the parties to the communication has given prior consent to the interception.

**Paging Devices** – Non-consensual interception of messages sent to a voice or display paging device requires a court order. No order is required to intercept a transmission made to a tone only pager.

**Pen Registers and Trap and Trace Devices** – A law enforcement officer may make written application to a state court of competent jurisdiction for an order and an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device. The order may be granted if the judge finds that the information likely to be obtained by the installation and use of the device is relevant to an ongoing criminal investigation.

**Sanctions for Violations** – Illegal interception of a wire, oral, or electronic communication, or disclosure or use of illegally obtained information, or illegal manufacture, assembly, possession or sale of any electronic surveillance device is a felony punishable by imprisonment for no more than five years, or a fine of no more than \$10,000 or both.

1. Any person whose wire, oral or electronic communication has been illegally intercepted, disclosed, or used shall have a civil case against the violator and be entitled to recovery of actual damages, punitive damages and attorney's fees.
2. Persons who engage in certain other conduct in violation of the wiretapping and electronic surveillance law shall be subject to imprisonment, fine and/or civil action prescribed by the law.

**Tracking (GPS) Devices** – No court order is required to monitor a tracking device, which emits a radio signal that enables the receiver to determine movement of the device. Under certain circumstances, a search and seizure warrant is required to place and monitor a tracking device.

**Video Surveillance** – Non-consensual interception of a closed circuit television broadcast (for example: a teleconference between two suspected criminals) requires a court order.

1. The use of a video camera in surveillance does not require a court order unless non-consensual interception of the oral communication of those viewed would be involved or if the area of surveillance is not in public view and a subject would have a reasonable expectation of privacy in the location.
2. The use of video cameras to monitor an area open to public view does not require a warrant or court order.

**REQUIRED ACTION****Member**

1. All requests for electronic surveillance assistance in any criminal investigation shall be initiated in writing, via proper channels, with prior approval of the Commanding Officer, Criminal Investigations Division or his/her designee.

**Commanding Officer, Criminal Investigations Division**

1. Review and approve/disapprove requests for electronic surveillance measures, as appropriate.

**Commanding Officer, Intelligence Section**

1. Maintain and deploy electronic surveillance equipment upon direction from the Commanding Officer, Criminal Investigations Division.

**RECISION**

Remove and destroy/recycle General Order J-11, "Electronic Surveillance Procedures" dated 4 October 1999.

**RELATED MATERIAL**

General Order J-14, "Video Surveillance Procedures"

**COMMUNICATION OF POLICY**

Supervisors shall be responsible for communication of this Order to their subordinates and to ensure compliance. This Order is effective on the date of publication and is to be read at all roll calls for five consecutive days and posted on Departmental Bulletin Boards.

**ANNEX****A. Consent for Wire or Verbal Interception Form**

**ANNEX A**

**Consent for Wire or Verbal Interception Form**

Consent for Wire or Verbal Interception  
Form 10/196

**POLICE DEPARTMENT  
BALTIMORE, MARYLAND**

**ONE-PARTY CONSENT FOR WIRE OR VERBAL INTERCEPTION**

Type of Case	Complaint Number	Date	Time
Primary Case Detective Rank and Name - PRINT CLEARLY	Sequence No.	Assignment	

**CONSENTING PARTY'S INFORMATION**

Name (Last, First, Middle)	Date of Birth	Education
Address (Number, Street, Apt. #)		
Address (City, State, Zip Code)		Telephone Number

**CONSENTING PARTY TO READ AND INITIAL ITEMS 1 - 6; PRIMARY CASE DETECTIVE TO COMPLETE ITEM 6 AS DIRECTED.**

1. I am not presently under the influence of alcohol, narcotics, or any medication which affects my ability to knowingly and intelligently make this consent. \_\_\_\_\_
2. I fully understand that by using electronic equipment to transmit or record conversations to which I am a party, my identity may be disclosed to a defense attorney before or during any prosecution that may result. \_\_\_\_\_
3. I fully understand that by using electronic equipment to transmit or record conversations to which I am a party, I may be required to testify at any or all trials that may ultimately occur. \_\_\_\_\_
4. I have not been forced, threatened, or coerced in any way to use electronic equipment to transmit or record conversations to which I am a party. \_\_\_\_\_
5. My decision to use electronic equipment to transmit or record conversations to which I am a party is a free and voluntary decision.  
\_\_\_\_\_
6. I hereby declare that I consent to the use of electronic equipment, to wit \_\_\_\_\_, for the purpose of transmitting and / or recording conversations to which I am a party so as to provide evidence relating to the crime of \_\_\_\_\_, effective on \_\_\_\_\_, and to continue as required until such equipment is removed by the Primary Case Detective. \_\_\_\_\_

Consenting Party's Signature	Primary Detective's Signature	
Witnessing Detective Rank and Name - PRINT CLEARLY	Sequence No.	Witnessing Detective's Signature