12.701 ELECTRONIC SEARCH WARRANTS

References:

United States Code (USC) 18USC2510-18USC2522, et al - Federal Wiretap Statutes
18USC2703 - Release of subscriber information to law enforcement under court order
18USC3127 - Authority to issue orders pursuant to 18 USC 2703
42USC2000 - Publishers Privacy Act/Publisher Protection Act
Ohio Revised Code (ORC) 2933.52 - Interception of wire, oral or electronic communications
ORC 2933.53 - Application for interception warrant
ORC 2933.56 - Contents of warrant; sealing of application and warrant; disclosure; retention
ORC 2933.58 - Instructions to investigative officers; procedures for interception; territorial validity
ORC 2933.59 - Execution of warrant or oral order; recording or resume; termination; tampering; destruction of documents; disclosure
ORC 2933.61 - Service of inventory on intercepted persons; inspection of materials
ORC 2933.64 - Training in wiretapping and electronic surveillance
ORC 2933.65 - Civil and criminal actions for violations
ORC 2933.76 - Authorization of use of a pen register or trap and trace device
ORC 2933.77 - Authorization for TSP to charge for services outside of the normal course of business and for technical assistance and equipment
ORC 2933.21 - Search warrant
ORC 2933.22 - Probable cause
ORC 2933.23 - Affidavit for search warrant
ORC 2933.241 - Inventory of property taken
U.S. Supreme Court No. 98-83 - Wilson v. Layne
Procedure 12.809 - Telephone Court Orders
Procedure 12.700-SEARCH WARRANTS/CONSENT TO SEARCH

Purpose:

To ensure uniformity in conducting electronic search warrants and direct the warrants to the proper investigating authority.

Policy:

Obtain supervisory review and approval of electronic search warrants and court orders before contacting the court. A supervisor from the Intelligence Unit will be the primary approving supervisor. In the event an Intelligence Unit supervisor is unavailable, a supervisor from the Major Offender Unit (MOU) will approve the search warrant. Assistance in drafting the electronic search warrant or court order should come from the City Prosecutor’s office.

All electronic search warrants and court orders are signed by a judge from the Court of Common Pleas, Criminal Division, after review by the City Prosecutor.

The use of data-reading software, known as Secure Techniques for on Site Preview (Stop) or similar authorized software to examine electronic data contained in electronic data storage devices prior to seizure, are to be conducted by authorized Department personnel only.

Upon seizure, all forensic examinations of stored electronic data contained in computers are conducted by Regional Electronic Computer Investigation Section (RECI). All forensic examinations of cell phones, Blackberries and other similar devices are conducted by Police Criminalistics Section.

Information:

There is a difference between an electronic search warrant and a court order. A computer, usually the hard drive, is actually searched to obtain information on its contents. Much like searching a house for evidence, the computer is the property of another, but it may contain evidence of a crime. To search the property of another requires the consent of the owner or a search warrant. Due to wording in the laws concerning searches of electronic media, the Criminal Division of the Commons Pleas Court is used as the issuing authority for the search warrant. A municipal court warrant may allow the seizure of the computer, but it takes a Common Pleas warrant to search the computer.

All that is required to obtain subscriber information from an Internet Service Provider (ISP) is a court order. There is no search involved and the ISP owns the subscriber information. It is the same as obtaining a telephone number with a court order.

Should a subscriber store e-mail on the ISP's server or have a file share stored on an ISP's server, a search warrant would be needed, as that information is the property of the subscriber, not the ISP.

Procedure:

A. Electronic Search Warrants and Court Orders

1. The search warrant or court order will be approved by a supervisor from Intelligence Unit or MOU.

2. The search warrant or court order will be reviewed by the City Prosecutor’s office.

3. The search warrant or court order will be signed by a judge from the Court of Common Pleas, Criminal Division.

4. Computers seized for forensic examination are submitted to RECI along with the following:

a. A case summary or a RECI evidence submission sheet.

1) RECI evidence submission sheets can be obtained by contacting RECI.

b. A copy of the search authority (search warrant, Form 601, Consent to Search Without a warrant or RECI consent form).

1) When using a consent to search form, it is imperative that officers obtain consent from all parties who have an expectation of privacy. Access to all parts of the electronic device may require additional paperwork. RECI officers can give further advice in this area.

2) If the electronic device is from a business, the consent to search form must also be signed by the supervisor of the business, and include a copy of the business' user agreement.

a) The supervisor must have direct authority over the electronic device in order to give consent. RECI officers can give further advice in this area.

B. Electronic Court Orders

1. To obtain a court order, personnel will contact the Intelligence Unit. Only certified Intelligence Unit officers can write these court orders.

2. All telephone court orders require the following information on the affidavit:

a. Requesting officers need to provide their name, rank, unit of assignment, working hours, telephone and fax numbers. Officers must include the criminal charge, with the ORC section number for the investigation, and a brief statement of probable cause.

b. The probable cause statement must include how the telephone number is involved in the criminal activity and how the requested information will assist law enforcement in the criminal investigation.

3. Court orders can be obtained for:

a. Subscriber information

1) This gives the name, address, and credit card information on the person(s) who is/are responsible for the payment of

the Internet service. This information comes from the ISP, such as America On Line, Roadrunner, Zoomtown, etc.

b. Internet provider address information

1) This information can be obtained for certain types of investigations. For example, if an officer needs assistance in identifying a person using a certain moniker in a chat room or on a blog posting.

c. Cellular telephone information

1) Officers requiring information on phone numbers received and called should refer to Procedure 12.809, Court Orders for Telephone Records.