308.10.7 TRAINING
In addition to the initial department approved training required to carry and use a Taser device, any personnel who have not carried a Taser as a part of their assignment for a period of six months or more shall be re-certified by a Departmental defensive tactics instructor who has completed a Taser Instructor course prior to again carrying or using the device. A reassessment of an officer's knowledge and/or practical skill may be required at any time if deemed appropriate by the department's designated defensive tactics instructor(s).

308.11 REPORTING USE OF CONTROL DEVICES AND TECHNIQUES
Any application of a control device or technique listed in this policy shall be documented in the related incident report and reported pursuant to the Use of Force Policy.

Pertinent segment from procedural manual (Cell phones):

F. EVIDENCE RELATING TO STORED COMMUNICATIONS

The Stored Wire and Electronic Communications Act (SCA), 18 USC §§2701-2712, which is part of the Electronic Communications Privacy Act (ECPA), limits law enforcement access to the stored records of providers of electronic communication services and remote computing services. An **electronic communication service** is any service that provides users the ability to send and receive wire or electronic communications. 18 USC § 2510(15). For example, cell phone companies and Internet service providers are electronic communication service providers. However, a company that merely receives and sends wire or electronic communications, such as Amazon, is not an electronic service provider.

A **remote computing service** provides off-site storage or processing services for computer related data on behalf of its customers. 18 USC § 2711(2). An electronic bulletin board is an example of a remote computing service. *Steve Jackson Games v. United States Secret Serv.*, 816 F.
Supp. 432, 443 (W. Dist. Tex. 1993).

Often a service is both an electronic communication service provider and a remote computing service depending on the type of service provided. Yahoo!, for instance, is an electronic service provider when it provides users the ability to send e-mails, but is a remote computing service with respect to opened e-mails that users store on its servers.

NOTE: Although the SCA distinguishes between electronic communication services and remote computing services, that distinction has little practical meaning. That is because the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F3d 1066 (9th Cir. 2003), effectively eliminated the differences between the legal process required to obtain the records of an electronic communication service and the records of a remote computing service.

1. Records Available

Electronic communication service providers and remote computing services create, maintain, and store information that may be useful in criminal investigations. The categories of information created by the SCA are subscriber information, transactional records, and content.

a. Subscriber Information

Subscriber information includes basic information about a customer. The SCA defines subscriber information as the following:
(A) name;
(B) address;
(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), 18 USC § 2703(c)(2).

b. Transactional records

The SCA defines the second category of information as "records or other information pertaining to a customer or a subscriber." 18 USC § 2703(c)(1). This type of material commonly is referred to as transactional records and includes everything that is neither subscriber information nor content. Examples of transaction records include e-mail addresses of sent and received e-mails, cell site data, and account logs showing web sites visited.

NOTE: A subscriber or customer of a service provider does not have a constitutionally protected privacy right in subscriber information or transactional records held by service providers. *State v. Johnson*, 340 Or 319, 335-36, 131 P3d 173, *cert den*, 127 S Ct 724 (2006) (subscriber information from cell phone provider); *State v. Magana*, 212 Or App 553, 159 P3d 1163, *rev den*, 343 Or 363 (2007) (same); *State v. Delp*, 218 Or App 17, 178 P3d 259 (2008) (subscriber information from Internet service provider).

c. Content

Under the SCA, content "includes any information concerning the substance, purport, or meaning of a communication or data file." 18 USC § 2510(8). For instance, content includes the text or subject line of e-mails, word processing files, and voicemail messages.

2. Compulsory Disclosures

The SCA sets forth the procedures that law enforcement must follow to compel service providers to disclose records in their possession. Any court of competent jurisdiction may issue orders under Act, which includes a state court of general criminal jurisdiction authorized to enter orders authorizing the use of a pen register or trap-and-trace device under state law. 18 USC § 3127.

a. Preservation Letter

18 USC § 2703(f) provides that "a provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." Government requests pursuant to § 2703(f) commonly are made in writing and are referred to as preservation letters. Upon receiving such a request, service providers are required to maintain the records that are the subject of the request for a period of 90 days. The government has no remedy if a service provider fails to comply with a lawful request, however.

PRACTICE TIP: Preservation letters are an essential step in any criminal investigation that might rely on evidence in the possession of service providers. To ensure that records are not destroyed or lost, a preservation letter should be sent the moment the need for the records of a service provider becomes apparent. The letter should ask for preservation of any documents that could be relevant to the investigation. Once the documents are preserved, an officer may follow up with a request for the specific information needed.

b. Consent of Subscriber or Customer

The government may require a service provider to disclose subscriber information and transactional records if the governmental entity has the "lawful consent of the subscriber or customer" to such disclosure. 18 USC § 2703(c).

NOTE: A service provider may – but is not required to – divulge the contents of communications to a government entity, if the entity "obtains the lawful consent of the originator or an addressee or intended recipient of such communication, or the

subscriber in the case of a remote computing service." 18 USC § 2702(b). As discussed, *infra*, a governmental entity may require the disclosure of the contents of a communication only pursuant to a warrant. 18 USC § 2703(a).

c. Subpoena

Pursuant to 18 USC § 2703(c)(2), a provider of electronic communication service or remote computing service shall disclose subscriber information to a governmental entity when that entity "uses an administrative subpoena authorized by a Federal or State statute or Federal or State grand jury or trial subpoena." The governmental entity is not required to provide notice to the subscriber prior to issuing the subpoena. 18 USC § 2703(c)(3).

The 2007 Legislature amended ORS 136.595, which prescribes how subpoenas are to be served, to provide that "a subpoena for the production of papers, documents, records and other tangible things may be served on a corporation or limited partnership in the manner provided by ORCP 7 (D)(3) for the service of a summons." ORCP 7 (D)(3) provides for alternative methods of service when a business does not have a registered agent available for personal service in the county where the criminal action is pending. An alternative method of service may include mailing the subpoena to the principal office or place of business of the corporation or limited partnership.

NOTE: Many out-of-state corporations that conduct business in Oregon are willing to accept – and, in fact, prefer – service of a subpoena by facsimile. That is because accepting service by facsimile, in lieu of service on a personal representative, often is more efficient for the corporation. Even so, prosecutors should verify that a corporation is willing to accept service by facsimile prior to issuing a subpoena.

d. Order Pursuant to 18 USC § 2703(d)

Under 18 USC § 2703(d), a court may order the disclosure of subscriber information or transactional records if "a governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that [the information or records] sought are relevant and material to an ongoing criminal investigation." An application for a 2703 (d) order should include a request for a non-disclosure provision, to prevent the service provider from alerting the suspect that the suspect's account is the subject of a criminal investigation.

PRACTICAL SUGGESTION: A sample application and order prepared by the Criminal Justice Division of the Department of Justice are attached as appendices to this chapter.

e. Warrant

A governmental entity may require a service provider to disclose the contents of any communication or record only pursuant to a search warrant. 18 USC § 2703(a). Although the SCA provides for a lower standard of process for content retained by a remote computing service or an electronic communication service if the content has been in electronic storage for more than 180 days, the Ninth Circuit has interpreted the SCA in a manner that has rendered those provisions ineffective. *See Theofel v. Farey-Jones*, 359 F3d 1066 (9th Circuit 2003). Moreover, although no Oregon appellate court has held that a customer has a constitutionally protected privacy right in the contents of his or her past communications that are stored and kept by a service provider, the Supreme Court has suggested that such a privacy right does exist. *State v. Johnson*, 340 Or 319, 335-36, 131 P3d 173, *cert den*, 127 S Ct 724 (2006) (noting that a defendant has a cognizable privacy interest in the content of his real-time telephone conversations). For that reason, even assuming that the Ninth Circuit incorrectly interpreted the SCA's provisions in *Theofel*, law enforcement should obtain a search warrant for the content of a suspect's stored communications.

A governmental entity also may rely on a search warrant to compel the disclosure of subscriber information and transactional records. 18 USC § 2703(1)(c)(A).

3. Non-compulsory disclosures

In addition to the compulsory process described above, a service provider may divulge the contents of communications to a governmental entity:
(1) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of a remote computing service;
(2) if the governmental entity is a law enforcement agency and the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime; or
(3) if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency. 18 USC § 2702(b).
A service provider may disclose subscriber information and transactional records to a governmental entity:
(1) with the lawful consent of the customer or subscriber; or
(2) if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.
18 USC § 2702(c).

4. Suppression

Nonconstitutional violations of the SCA do not require suppression. 18 USC § 2708. However, a person aggrieved by a violation of the Act may be entitled to a civil remedy. 18 USC § 2707.

We have no policy/procedure concerning citizens videotaping officers. All of our patrol vehicles are equipped with mobile audio/video recording units for the protection of officers and citizens alike (policies can/will be produced upon request). ORS 163.700 and 163.702(b) outline prohibited and exempt practices, which means pretty much everything else is legal although Oregon law leaves a lot to be desired in this area.