TIA COMMITTEE TR-45 MOBILE & PERSONAL COMMUNICATIONS STANDARDS (TR-45)

TITLE: **Method for Identifying Telecommunications Services and Information Services for Packet-Mode Communications Subject to Surveillance Under CALEA**

ABSTRACT: **This document identifies a method for identifying a packet stream as a telecommunications service, in which case call identifying information can be provided to law enforcement on a pen register or trap and trace court order.**

DATE: **May 3, 2000**

SOURCE: **Universal Wireless Communications Consortium (UWCC) Packet Data Focus Group (PDFG)**

Contact: Bill Marshall (AT&T)

Email: wtm@research.att.com

CONTRIBUTION #: **CJEM503-101R1**

RECOMMENDATION: **Review and adopt as a JEM position.**

1. Introduction

The industry standard for Lawfully Authorized Electronic Surveillance, J-STD-025[1], includes procedures for the interception of packet mode communication, and delivery of the contents of the packet mode communication to a Law Enforcement Agency. Delivery of the content of intercepted packets, even under a pen register order, was challenged by several groups as violating the balance between the rights of law enforcement and the rights of individuals to privacy. The FCC concurred that this raised significant privacy concerns, and requested TIA to study the matter further and recommend steps that can be taken to better address the privacy concerns[2].

The FCC has concluded that packet data and packet-switching technology are potentially usable for both information services and telecommunications services, but that such technology is subject to CALEA requirements only to the extent it is used to provide telecommunications services, and not for information services[3][4][5]. The statute expressly excludes "information services" from its assistance capability requirements. Section 102(6) of CALEA (47 U.S.C. § 1001(6)) states that the term "information services" (A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network. If the packet sequence is providing an information service, then the requirements of CALEA do not apply, although the full content of the communication may still be intercepted under a Title III order[6].

The contribution identifies a potential method for separating information services (not subject to CALEA requirements) from telecommunication services (subject to CALEA requirements) when the packet technology being employed is capable of simultaneously delivering both to a subscriber.

2. Information Service versus Telecommunication Service

The primary technical challenge in applying CALEA to packet mode communication is the determination, for each individual sequence of packets sent by a subject under surveillance, whether the packet sequence is providing an information service or whether the packet sequence is providing a telecommunication service. If the packet stream is providing an information service, then no interception capability is required by CALEA.

Consider a typical information service, sending and receiving of electronic mail. Sending of an email message is observable by the packet data service provider only as a sequence of packets sent by a subscriber to a remote system, which accepts the packets for later retrieval by the recipient. Receipt of an email message is observable only as a sequence of packets originating from a remote system, and destined to the subscriber.

The subscriber chooses the specific email retrieval system for processing and storage of their incoming messages (e.g. aol.com, hotmail.com, etc). Consider the above simple email message exchange, where the two participants have configured their home computer as their private email servers. From the perspective of the packet data service provider, the observable behavior is identical – there is a sequence of packets sent by a subscriber to the email server at a remote system.

Only the address of the email retrieval system is known to the packet data service provider, and not the intended recipient of the email message. If messages are sent frequently, the packet data service provider does not know whether they are all to the same person, or to many different people using the same retrieval system. It is not uncommon for a subscriber to send a large burst of messages, at the rate of many per second, all of which are destined for the same email retrieval system. It is also possible for the subscriber to send multiple messages to the same address, even at the rate of multiple messages per second. From the perspective of the packet data service provider, the observable behavior is identical – there is a sequence of packets sent by a subscriber to the email server at a remote system.

Email messages may contain attachments, such as documents, etc. The presence or absence of attachments is unknown to the packet data service provider, as they are completely encoded within the text of the message. Email messages may contain attachments that are recordings made through the use of a microphone attached to the home computer. The presence or absence of this type of attachment is likewise unknown to the packet data service provider. From the perspective of the packet data service provider, the observable behavior is identical – there is a sequence of packets sent by a subscriber to the email server at a remote system.

The packet data service provider has no control over the information storage facilities, the storage mechanism, or the processing done by the email retrieval system on receipt of a message. The email system may display the messages immediately, rather than waiting for a retrieval request. The email system may play audio attachments immediately upon receipt as well, without the knowledge of the packet data service provider. From the perspective of the packet data service provider, the observable behavior is identical – there is a sequence of packets sent by a subscriber to the email server at a remote system.

This example has shown how a simple packet-mode information service, namely an email exchange, can be slowly modified into a real-time two-way audio service that is indistinguishable from a telecommunications service. At no point along the way did the packet data service provider know the purpose of the packet exchanges. Further, the packet data service provider is unable, at each and every step along the path, to examine the packets being sent and received by the subscriber, and determine they are anything other than ordinary email exchanges.

Many other examples exist where protocols clearly defined for information services can be used to provide telecommunication services. The specific protocols chosen by standards bodies for transport of telecommunication services (e.g. IETF's Real-Time-Protocol, RTP) is used by many other information services as well (e.g. retrieval of stored music, video clips, etc.), and cannot itself be used as a distinguishing factor.

Therefore, a conclusion could be that it is not technically feasible to determine whether a packet stream is being used for an information service or being used for a telecommunication service. It is not possible to make this determination on a packet-by-packet basis, nor is it possible to make this determination by observation of a stream of packets. It is only by mechanisms outside of the packet stream itself (described later) that the determination can be made regarding information service or telecommunications service.

In the absence of an indication of the packet stream purpose, the privacy concerns raised by the FCC in their Third Report and Order would argue against a default determination of a packet stream as a telecommunication service. Therefore, the default could be that the packet communication is providing an information service.

3. Requirements for identifying a Telecommunications Service

There are several protocols in existence today for the establishment of telecommunications sessions over packet media. The two most prominent ones are ITU's H.323, and IETF's SIP. Both have the characteristic of allowing, and even encouraging, a service provider to operate and administer a functional element within the packet network for the purpose of establishing sessions between communicating entities. These functional elements within the packet network, called a GateKeeper in H.323 and a Proxy in SIP, can provide traditional telecommunication services such as call forwarding and conference control.

It is only by the subscriber's use of such a GateKeeper/Proxy that the packet data service provider can identify a packet stream as belonging to a telecommunication service instead of an information service. The GateKeeper/Proxy could identify, in a technology-specific manner, sufficient information for the packet data service provider to identify the packets belonging to this service. In the case of the Internet, and networks that use the Internet Protocol, this is typically a filter-spec consisting of a IP source address, IP destination address, source port number, destination port number, and protocol identifier. For other technologies, the packet stream identification would contain different information.

This GateKeeper/Proxy could provide the call identifying information required by CALEA to be delivered to law enforcement under a surveillance order. Transport of this call identifying information to a Law Enforcement Agency may require a separate interface standard dependent on the service provider and technology employed for the packet mode communication.

No further call identifying information, beyond that available to and provided by the GateKeeper/Proxy, may be present in the packets containing call content.

4. Third party providers of Telecommunications Services

Special problems arise when the facilities of the packet data service provider are used for transport of telecommunication services, but the packet data service provider did not assist in the session establishment of the telecommunication service.

Such situations often arise in the Internet, where the Internet Service Provider (ISP) provides only the raw transport capability for IP packets. Other entities provide various registration services and/or meeting services that enable the subscribers to establish packet

mode communication that provides telecommunication services. These other entities may provide an H.323 GateKeeper, or a SIP Proxy, for performing these functions. An example of this is NetMeeting.

If the packet data service provider did not provide the GateKeeper/Proxy used to establish the connection, then the packet data service provider has no indication that the packet stream is other than an information service. The third party provider of the GateKeeper/Proxy could be viewed as the entity providing the telecommunication service, and has the obligations under CALEA to report call identifying information and possibly call content to law enforcement agencies if the participant is under a surveillance order. The packet data service provider could consider the packet stream an information service, and has no interception obligation under CALEA. However, the packet data service provider could, at its option, share the CALEA responsibility for call content interception with the third party provider.

5. Summary

The potential method can be summarized as:

(*Technically infeasible*) It is not technically feasible to determine, on a packet by packet basis, whether the packet is being used as part of an information service or as part of a telecommunication service. It is not technically feasible to determine, by observation of a stream of packets, whether the packet stream is being used as part of an information service or as part of a telecommunication service.

(*Default is information service*) Packet data and packet communication is an information service, unless the service provider knows, through some prior mechanism outside of the packet stream (e.g. completion of a session establishment protocol such as H.323 or SIP), that it is part of a telecommunications service.

(*Packet Stream Identification*) In order for a packet stream to be classified as a telecommunications service, the packet data service provider must be able to determine (e.g. through the service provider's participation in a session establishment protocol, such as H.323 or SIP, for the specific communication), the technology-dependent information required to isolate that communication from all others.

(*No Call-Identifying Information in the Packet Data*) When a packet-mode connection is established, and will be used as a telecommunication service, call identifying information is provided only by the session establishment protocol, and not via the packet mode communication itself. All call-identifying information is to be supplied by the session establishment agent (e.g. H.323 Gatekeeper or SIP Proxy). Transport of this call-identifying information to a law enforcement agency may require a separate interface standard dependent on the service provider and the technology employed.

(*Third party providers*) When a third party, other than the packet data service provider, establishes packet mode connections between two parties for purposes of providing telecommunications service, responsibility under CALEA lies with the third party and not with the packet data service provider. The packet data service provider may, at its option,

share this responsibility with the third party; otherwise the packet data service provider considers the packet stream to be an information service.

6. References

[1] Telecommunications Industry Association (in association with Standards Committee T1 Telecommunications), INTERIM STANDARD (Trial Use Standard): Lawfully Authorized Electronic Surveillance, J-STD-025 (December 1997).

[2] Federal Communications Commission, Third Report and Order, Docket 97-213, released August 31, 1999, FCC document number 99-230, available at http://www.fcc.gov/wtb/f99230.pdf, §55.

[3] Federal Communications Commission, Second Report and Order, Docket 97-213, released August 31, 1999, FCC document number 99-229, available at http://www.fcc.gov/wtb/Fcc99229.pdf, §27.

[4] Federal Communications Commission, Further Notice of Proposed Rulemaking, Docket 97-213, October 22, 1998, FCC document number 98-282, available at http://www.fcc.gov/Bureaus/Common_Carrier/Notices/1998/fcc98282.pdf. §63.

[5] Federal Communications Commission, Third Report and Order, Docket 97-213, released August 31, 1999, FCC document number 99-230, available at http://www.fcc.gov/wtb/f99230.pdf, §48.

[6] Omnibus Crime Control and Safe Streets Act of 1968, modified by the Electronic Communication Privacy Act of 1986.