Liability Issues In A VOIP Environment

Colleen Boothby

The effects of 911 and wiretap regulations could put an added bite into VOIP costs.

Voice over IP (VOIP) applications for enterprise customer networks have significant advantages in terms of features and functions, as well as attractive cost characteristics, which will continue to drive enterprise customer networks to VOIP for the next several years, despite some lingering regulatory uncertainty about how VOIP "fits" into the world of traditional telecommunications services.

Much of the controversy over VOIP has centered on relatively obscure issues—whether VOIP should be classified as a regulated "telecommunications service" or an unregulated "information service"; whether it can be regulated by the state public utility commissions or only by the FCC; whether the service will be accepted in other countries so that it can be used economically for international traffic; whether it is subject to the same state and federal taxes that apply to traditional communications services; and whether VOIP providers will be required to pay state and federal universal service fees and access charges, which could raise the cost of providing, and thus the price for using, the service. (For more on these topics, see this issue, pp. 10–12.)

But VOIP technologies also introduce some very practical legal issues that enterprise customers should keep in mind as they deploy the technology, to reduce the risk of unpleasant financial surprises down the line.

911 Calls

Enterprise customers need to protect themselves from traditional liability issues, which can arise when VOIP service doesn't behave like the traditional telephone services most people are accustomed to using.

Traditional telephone service is geographically specific—carriers assign unique telephone numbers to individual telephone lines that have fixed geographical locations, with corresponding street addresses that carriers store in their databases. Emergency response services have exploited this characteristic of traditional circuit-switched telephone service for many years. By tapping into a carrier's database of the street addresses associated with customer lines, emergency service providers can use the automatic number identification ("ANI") of an incoming emergency call to look up the caller's street address and send emergency services to the caller's location.

What happens in a VOIP world, where a caller's physical location may not correspond to the ANI associated with the terminating end of a VOIP call?

Consider, for example, this increasingly familiar scenario. Your company decides that employees should use VOIP for remote access to the enterprise network. Employees receive a VOIP handset to use at home or on the road in conjunction with broadband Internet access service.

The phone is pre-programmed to ride the Internet to your company's PBX when the employee uses it. The PBX then acts as a gateway to the public switched telephone network ("PSTN")—performing any necessary protocol conversion and routing the employee's calls to the company's long distance provider or points in the local exchange, just as if the phone were a station behind the PBX. In effect, the PBX is providing the dial tone for your employee's phone.

Now assume that your employee has plugged the phone in at home when a family member is visiting or a neighbor drops in. A medical emergency occurs and the visitor places a 911 call from the company-provided VOIP phone.

Within minutes, ambulances and fire engines arrive—at the company office where the PBX is located. This happens because, absent some additional technology at the PBX which may or may not be available or properly installed, the ANI associated with the emergency call will be the PBX's, not the employee's home number. As the VOIP gateway to the PSTN, the PBX is the network location the PSTN "sees" when it first picks up the emergency call and transmits ANI information to the emergency response system.

Colleen Boothby is a partner at Levine, Blaszak, Block & Boothby, LLP. The firm represents enterprise customers in the acquisition of telecommunications and technology products, in the resolution of disputes with providers, and on regulatory and public policy matters before the FCC and the federal courts.

CALEA applies to carriers, but it will affect end users

In this situation, the enterprise customer is at risk of being held liable for any adverse consequences that may result when emergency help is denied or delayed by the misdirected emergency response. Even if an injured party ultimately loses any claim for damages against the enterprise customer, responding to such a claim can be burdensome and expensive.

Prudent enterprise customers should therefore consider taking appropriate steps to educate employees about the nature and capabilities of the VOIP phones they distribute. Possible steps might include affixing stickers or labels on the VOIP handset indicating that emergency calls should not be placed from that phone. The enterprise customer might also provide an information sheet for employees to review and sign when they receive their VOIP phone, which explains in clear, non-legalese the phone's limitations in emergency situations.

Other measures may be appropriate depending upon the operating characteristics of the particular VOIP system you deploy.

E-911

Enhanced 911 or "E-911" refers to a more complicated system for emergency services that can pinpoint a caller's location more precisely than the current system.

The E-911 concept requires a detailed database that records not only the street address associated with a phone number but additional location information as well, such as the exact location of, and directions for reaching, some minimum square footage of searchable, contiguous floor space where the phone is located.

At their most complex, E-911 systems can require businesses to map their premises onto a standardized grid that breaks floor space into units of a particular size. The business must then store (and update, in a database maintained by the emergency response system) the telephone number of every handset located in each unit of floor space so that a caller's ANI can be used to send emergency personnel to the right floor space unit.

Once again, the idea that a handset's (or laptop's) ANI can always be associated with a specific physical location, a fundamental assumption of E-911 service, is at odds with some of the very features that make VOIP appealing to an enterprise customer. Many enterprises are attracted to VOIP technology because it reduces the cost and difficulty of tracking employees and their phone numbers when offices are rearranged or the employee has no fixed location on site. VOIP technology enables IP appliances, be they laptops or VOIP handsets, to register their presence on the enterprise network, and begin sending or receiving voice calls, as soon as the employee plugs the device into any available port on the network.

Some states have adopted legislation that requires the telecommunications systems of enterprise customers to include E-911 capabilities. Many have not. The issue is under active consideration at the FCC.

If an enterprise customer has locations in a state with E-911 requirements, or a state that decides to adopt E-911 requirements in the future, the enterprise may be confronted with an expensive upgrade if its existing VOIP technology has no means of collecting location information and associating it with traffic on the system.

Some technologies already on the market allow enterprises to record the physical location of a data port and assign identifying information to every packet from that port so that the originating location of an emergency call can be determined. Enterprises could install features that require users to register their location when they log in to the enterprise's VOIP system, akin to the approach followed by some commercial VOIP service providers.

At a minimum, enterprise customers should determine whether the law of the state in which they are using VOIP service requires E-911 capabilities for private systems and whether the technology they use satisfies its requirements.

CALEA

Enterprise customers periodically express concern, and no small amount of confusion, over the obligations they may have under the "Communications Assistance for Law Enforcement Act" ("CALEA"). Contrary to the suggestions of some carriers, however, CALEA does not impose requirements directly on end users.

Congress passed CALEA 10 years ago, reflecting its concern that new network technologies, and in particular packet technology, might eliminate the wiretapping and call tracing capabilities of traditional networks. To ensure that lawfully authorized wiretaps and call tracing can still occur as networks migrate away from circuit-switched technologies and towards packet technologies, CALEA requires phone companies to design and build their services in whatever way is necessary to ensure that law enforcement agencies with the requisite court order or other authorization can still tap or trace calls from individual subscribers.

Thus, CALEA applies only to "telecommunications carriers," not end users, and by its terms does not apply to Information services or "private networks."

Enterprise customers should nevertheless be aware of CALEA for another reason: Carriers have complained to the FCC that CALEA compliance is expensive. The FCC is therefore considering whether to require carriers to add yet another regulatory surcharge to end-user bills to recover their costs (also see this issue, pp. 66–65).

When the FCC first considered this issue, it concluded that carriers would bring themselves into compliance with CALEA in the course of "general network upgrades," recovering any

additional cost through their "normal charges." But the FCC recently changed its tune, stating that it expected CALEA to require significant capital expenditures in the future, even though it also conceded that solid cost estimates for CALEA implementation have never been generated.

Despite the lack of solid cost information, and prior payments to carriers from a $500 million fund established by Congress for CALEA compliance costs, the FCC has asked whether it should let carriers collect a new flat monthly charge, like the subscriber line charge or "SLC," to recover CALEA costs directly from end users.

Although it's hard to predict whether the FCC will end up adopting a SLC for CALEA, it's not hard to predict that, should the FCC go that route, the monthly charge paid by enterprise customers will be set higher than the residential charge, regardless of any actual cost differences between the two kinds of customers. State and federal regulators find it hard to resist using business customers as a subsidy source for residential rates. That's why, for example, the federally mandated SLC for residential customers is far lower than the SLC for multiline businesses, despite the fact that business lines tend to be much cheaper to install and operate than residential lines.

It is not too late for enterprise customers to weigh in on this issue. If you object to the prospect of yet another monthly charge for the same old services, consider filing comments at the FCC opposing the proposal□