T
he debate over government interce-
ption of Internet communications has expanded to a new
technology, namely Voice over Internet Protocol ("VoIP") transmissions. Indeed,
representatives of the FBI's Electronic Surveillance Technology Section in
Chantilly, Virginia have been meeting secretely with the Federal Communications
Commission since July, 2003, exploring ways to provide the FBI with more regu-
laratory authority to "wiretap" Internet communications. In particular VoIP
transmissions, The FBI along with the US
Drug Enforcement Administration and
the U S Department of Justice want VoIP
providers declared as "telecommunications carriers" under the Federal Communi-
cations Act of 1996 and the Communi-
cations Assistance for Law Enforcement Act of 1994 ("CALEA").
These three federal law enforcement
organizations declared that if left unregu-
lated, VoIP would provide a means of
communications whereby "terrorists, spies,
and criminals...can most likely evade
lawful electronic surveillance.
Voice over Internet Protocol allows
analog voice signals to be digitized into
packets of data, sent over a series of net-
works, and reassembled at the other end.
In other words, telephone calls that have
traditionally, since the late 19th century,
been made through Public Switching
Technology Networks ("PSTN") are
now initiated, transmitted and received
through computer networks, and thereby
avoid long distance telephone charges.
The technology, introduced in 1995,
stumbled along until recent improvements
in the sound quality and transmission reli-
ability have made "phone carriers...practi-
cally tripping over each other to announce
aggressive VoIP strategies aimed at both
consumers and businesses.
Today, VoIP transmissions constitute
up to ten percent of all calls made in the
United States, with estimates of up to 2.5
million U.S. subscribers. By 2006, it is
anticipated that well over 7 million VoIP
units will be in circulation.
The most popular reason that busi-
nesses and consumers give for switching
to VoIP is cost savings. Flat rate service
plans, including unlimited local and long
distance calls range from $20-$40, which
is 20-40% lower than service plans being
offered by PSTN companies. The main
reason for the cost savings is that VoIP
transmissions are not regulated like regular
telephone service. VoIP providers there-
fore do not have to pay the same taxes and
access fees that are passed onto consumers.
A technological benefit of VoIP is more
efficient use of the broadband cable,
which currently carries half of all VoIP
transmissions. Voice, data (e.g., faxes, e-
mail, instant messaging), and video can
all be transmitted simultaneously through
broadband cable, record an outgoing
message and leave it in their customers,
voice mail inboxes with one click, instead
of repeating the same message several
times a day. Moreover VoIP transmissions
can be recorded, labeled, indexed, stored,
and retrieved when necessary. These tech-
nological benefits have made VoIP the
new "target" of the Federal Governments
War on Terrorism.
Under existing federal wiretapping laws,
the FBI already has the ability to seek a
court order to conduct surveillance of any
broadband user through its DCS 1000
system, previously called Carnivore. But
Voice over Internet Protocol

federal law enforcement agencies worry that unless Internet service providers, and in particular VoIP providers, offer surveillance hubs based on common standards, lawbreakers can evade or, at the very least, complicate surveillance by using VoIP providers such as Vonage, Time Warner Cable, Net2Phone, SX8, deltathree and Digital Voice.

The origins of this debate date back nine years, to when the FBI persuaded Congress to enact a controversial law called the Communications Assistance for Law Enforcement Act ("CALEA"). The 1994 legislation requires that telecommunications services rewire their networks to provide police with guaranteed access for wiretaps. The legislation also empowered the FCC to issue regulations defining what categories of companies were subject to the broad sweeping legislation. So far only traditional PSTN (analog) companies and wireless phone services have been subject to CALEA.

The FBI now has taken the position that the combination of the federal wiretap laws, originally enacted in 1964, and amended numerous times since, along with CALEA, give it the authority to wiretap DSL and other types of broadband services, including VoIP.

Critics are worried about privacy issues. Under CALEA, "telecommunications services," as defined under CALEA and the 1994 Federal Communications Act, are required to modify their equipment so that law enforcement officials can effectively "wiretap" both data and voice transmissions. In particular, since VoIP represents the "blending" of data and real time voice transmissions, privacy advocates worry that VoIP "wiretapping" will lead to "dataveillance", where data such as location information will be routinely collected for surveillance, without any investigatory predicate. Moreover, neither VoIP providers nor the FBI can explain what will be done to ensure that private parties do not engage in illegal monitoring of private citizens, gaining access to privileged information, confidential business/trade secrets, or even sensitive medical information.

Moreover, the FBI has said that if broadband providers cannot isolate specific VoIP calls to and from individual users, they must give police access to the "full pipe"—which, therefore, inevitably would include hundreds or thousands of customers who are not the target of the investigation. This technological shortcoming of VoIP "wiretapping" would inevitably lead to over-inclusive sweeps of conversations and data transmissions that are not the "target" of any government probe.

Some companies like MetaSwitch and Cisco Systems, Inc. have already cooperated with the FBI's request for CALEA compliance to make their VoIP hardware products "surveillance friendly." These two companies have developed backdoor technology in their VoIP products that enables the FBI to eavesdrop at will. Yet segregating particular voice packets not the target of a search warrant still presents technological hurdles to many VoIP providers, leaving many VoIP transmissions subject to interception despite falling outside of the scope of the federal search warrant that authorized the interception.

On the other hand, not all Internet service providers see themselves as "adverse" to the interests of the FBI. EarthLink, for instance, wants CALEA and the Federal Wiretapping Statutes applied to VoIP calls. If VoIP calls escape being subjected to this expanded regulatory scheme, it would mean that VoIP stays "unregulated" as far as the FCC is concerned. Such de-regulation of Internet services would allow the Baby Bells such as Verizon and BellSouth to raise the rates charged to ISP's, such as EarthLink, for access to the copper wire that runs to subscribers' homes and businesses.

EarthLink, as an ISP provider has, therefore, admitted that it sees "the FBI as an ally of sorts?" said David Baker,
EarthLink's vice president for law and public policy.

The federal courts are split on this issue of expanding government power to regulate and therefore intercept Internet transmission, and in particular VoIP. The Ninth Circuit Court of Appeals, for instance, in October, declared, to the delight of Internet Service Providers (ISP's) such as EarthLink, that the cable operators to the extent that their broadband services use the Internet, are telecommunications providers, making them subject to state and federal regulations, including FCC regulations.

In the same month, a federal district judge in Minnesota issued an injunction against the Minnesota Public Utilities Commission, barring it from seeking to impose tariffs on VoIP provider Vonage. Consequently, the Minnesota Federal District Court decision allows Vonage to escape being subjected to the FBI's request to the FCC to expand the reach of CALEA.

CONCLUSION

Everything is pointing to the exponential growth of VoIP use. VoIP usage might even exceed the prediction that by 2007, seventy-five percent of all voice traffic will travel over the Internet. Thus, it appears that the FBI's request for expansion of its "wiretapping" authority versus and the FCC Chairman Michael Powell's stated desire to further unleash the Internet, making it free from government regulation are set on a collision course.

The same statutes that allow for wiretapping also authorize other government activity such as taxation of the Internet and the mandating of services such as 911, guaranteed access, remote area service, and service for the hearing impaired.

On the other hand, if the Internet and in particular VoIP is ultimately declared to be free from the string of regulations and tariffs that surround traditional PSTN providers, then government officials seeking broader "wiretapping" authority may be stymied in their efforts to intercept VoIP transmissions and neutralize this new form of a national security threat.

Konrad Trope is a cyberspace and intellectual property attorney with a national practice, based in Los Angeles. Konrad's practice focuses on cyberspace, intellectual property and entertainment litigation, transactions, and regulatory counseling. Konrad is a member of the ABA Cyberspace committee and a member of the California State Bar Cyberspace Committee. Konrad can be reached at ktrope@earthlink.net.