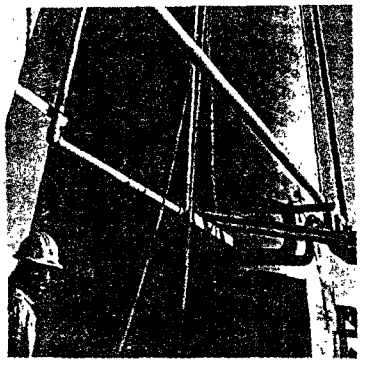
slowly, both geographically
of cases.
our risk significantly, even
to vacation in high-risk
e Cod, Nantucket and
d, the South and North
nnecticut River valley.
d wooded and scrubby
an't, wear long sleeves
cked into your socks. Use
sparingly, and at the end
k everyone for tiny, dot-

open beach or on a
obably safe, even on the
ds, says Dr. David T. Den-
tes Lyme programs for
)isease Control in Fort

re two years ago that led
aerial mosquito spraying
husetts health officials this

SENSE, Page 30

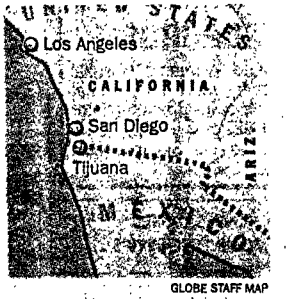


Housewives' group prodded government to revoke the license for this newly built incinerator.

small working-class barrio situated in a valley near the Tijuana River.

Since the industrial park opened over a decade ago, residents of Ejido Chilpancingo say, they have been living in the shadow of a chemical nightmare. Their livestock feed on toxic waste, their air is often blackened by pollutants and their water supply has been fouled by a network of open drainage pipes that poke out over the town from a bluff beneath the industrial park. Its tenants include subsidiaries to such corporate giants as Mobil Oil and Pepsi and to American Optical Corp., a Southbridge, Mass.-based firm that manufactures lenses.

When rain falls upon Ejido Chilpancingo, plant workers release into drainage pipes stockpiled industrial detergents, solvents, heavy metals and petroleum products. The outflow empties into dozens of meander-



GLOBE STAFF MAP

and San Antonio t
port for a North
Trade Agreement a
ed States, Mexico
argued that the
the antidote to the
problems that affli
like Ejido Chilpan
viding benefits to U
he reasoned, the ag
raise living standa
cans and America
"higher standards o
help people keep th
cleaner on both sides of the border."

The agreement has to be ratified b
gress, which is unlikely to deal with it
November elections.

To deal with the immediate problems,
billions to clean up, Bush has proposed
an Integrated Border Plan and asked th

BORI

GLOBE PHOTO / DAVID L. RYAN

s no ready answer to law enforcement's concerns.

COMMUNICATIONS

Snoops are vexed by digital era

As tapping phones gets harder, FBI looks to Congress for help

By Simson Garfinkel
SPECIAL TO THE GLOBE

If New York mobster John Gotti had used a cellular telephone, many of the conversations that helped lead to his conviction for murder and other crimes might have gone unheard and unrecorded by law enforcement agents.

Although nearly anybody can randomly intercept a cellular telephone conversation with a hand-held radio scanner, tapping in on a specific telephone is much more difficult.

The computers that route conversations between the cellular and conventional telephone networks can only monitor specific phone calls at special "service ports" located on the telephone switch itself. And until recently, there weren't enough service ports on New York City's cellular switches to satisfy the needs of various law enforcement agencies.

"Most of the switches had only four to seven 'ports,'" says James K. Kallstrom, engineering chief for the FBI. The equipment "was not designed to do wiretaps."

Kallstrom is worried that what happened in New York is going to happen again and again as communications systems are computerized – that new systems will be installed that don't have provisions for wiretapping. He fears that law enforcement will be dealt a major blow as criminals start using systems that offer total security, free from any possible surveillance.

"There were so many warrants to wiretap in New York that it overwhelmed the system," agrees John

WIRETAP, Page 34

Digital communications pose vexing pr

■ WIRETAPS

Continued from Page 29

Podesta, a Washington-based consultant.

"On any given day last year in New York City, there were upwards of 50 court orders [for wiretaps] waiting for the New York switch," says Kallstrom. "You are put in the difficult position of going through all the work – and there is a quite a bit of work to get a wiretap order, because it is the most intrusive of all investigative techniques – and then you are put on a waiting list."

Smaller metropolitan centers, such as Boston, don't necessarily have New York's problem, say those familiar with the situation. And although the Gotti case has been widely cited, the cellular telephone industry considers the concern overblown, and the Gotti example, in particular, a red herring.

Had there been a request to tap a cellular phone the mobster was using, says JoAnne Basile, director of federal relations for

'I think that the one thing that is clear to them now is that the business opposition to their proposals extends well beyond the traditional telephone companies.'

JOHN PODESTA, *Washington-based consultant*

the Cellular Telephone Industry Association, it would have been given priority. In addition, she says, "Any capacity problems that may have been identified in New York have been relieved."

But law enforcement officials are not easily reassured.

With a conventional telephone, wiretapping is as easy as attaching two clips to a telephone line. Many people think it's too easy.

"Anybody with a little bit of knowledge could climb a telephone pole today and wiretap someone's lines," says Kallstrom.

As communications are increasingly digitized and computerized, however, all a wiretapper – legal or otherwise – will hear with a pair of clips is a hiss, as a hundred thousand digital zeros and ones move across the wire every second. To make sense of it, wiretappers need expensive digital equipment to reconstruct voice from the digital stream.

"When the digital network goes end-to-end digital, that will preclude amateur night. It's a much safer network from the privacy point of view," Kallstrom concedes.

Kallstrom and the FBI insist, however, that increased privacy for the consumer should not come at the cost of hobbling law enforcement. "If a friend of yours is kidnapped or [someone] puts a bomb in Fenway Park, and to solve [the case] we need to intercept communications, we need to be able to do it," he says.

Codes, cyphers and encryption techniques for securing voice and data communications pose greater problems still. The new digital telephone systems lend themselves to encryption, which can make it mathematically impossible for a wiretapping eavesdropper to understand what the two parties are saying.

Some see a boost for privacy

Many people familiar with the technology see the new computerized communications as a boost for privacy and security.

"This technology is needed by US businesses to protect sensitive business information transmitted over electronic networks from unauthorized eavesdropping by foreign intelligence agencies and others," US Rep. Jack Brooks (D-Tex.) told a congressional hearing on encryption in early May.

But many law enforcement officials and the Bush administration have a different view. They see advances in communications as a threat to the fight against drugs, terrorism, kidnappers and white collar crime, and they are seeking legislation to ban equipment that cannot be monitored.

In New York, says Kallstrom, "Routinely, [wiretap warrants for] the major drug and crime cases" went unfulfilled. "This is a microcosm of what will happen when the general public switch telephone network goes digital."

Law enforcement officials are quick to add that they do not oppose new technology; in some ways, digital telephony will make their jobs much easier. For example, a person being monitored by a digital wiretap cannot detect the monitoring; there is no tell-tale click on the line.

Digital wiretaps also will mean tapes with compact disc-quality sound.

"It's mind-boggling how good it is. It doesn't have any moveable parts. The clarity

'Any proposal that attempts to control communications technology inevitably reaches to all computer technology – personal computers, workstations, local area networks.'

MITCH KAPOR, *founder Lotus Development Corp. and Electronic Frontier Foundation*

is wonderful," says Roseanne DeMaria, chief of the organized crime and narcotics unit in the Manhattan district attorney's office. "But if we can no longer intercept, we are in trouble. ... We would be in an impossible position."

Early this year, FBI director William Sessions and Attorney General William Barr went to Capitol Hill to argue for legislation that would compel all makers of electronic communications systems to build wiretap capabilities into their systems or face a fine of $10,000 per day.

It would also require that all existing electronic communications systems be modified to permit wiretaps by law enforcement officials, both on site and remotely.

The FBI withdrew its draft of the legislation after an ad hoc coalition of communi-

ɔose vexing problems for snoops

'Any proposal that attempts to control communications technology inevitably reaches to all computer technology – rsonal computers, workstations, local area networks.'

MITCH KAPOR, *founder Lotus Development Corp. and Electronic Frontier Foundation*

/onderful," says Roseanne DeMaria, chief he organized crime and narcotics unit in Manhattan district attorney's office. it if we can no longer intercept, we are in ible. ... We would be in an impossible ition."

Early this year, FBI director William sions and Attorney General William Barr t to Capitol Hill to argue for legislation would compel all makers of electronic munications systems to build wiretap ca- lities into their systems or face a fine of 000 per day.

t would also require that all existing ronic communications systems be modi- to permit wiretaps by law enforcement ials, both on site and remotely.

he FBI withdrew its draft of the legis- n after an ad hoc coalition of communication equipment vendors, computer companies and civil libertarians voiced their opposition, and a revised version is now being privately circulated inside the administration by the Office of Management and Budget for other agencies' reactions, says Podesta, who was retained by the Electronic Frontiers Foundation to fight the legislation.

"I think that there has to be a way of assuring that the FBI can conduct lawful, warranted wiretaps," says Jerry Berman, director of the foundation, a civil liberties watchdog group that is coordinating the opposition. "At the same time, this broad proposal to review, monitor and license all technologies coming online is far more extreme and sweeping than necessary for the current problem."

US Rep. Don Edwards, a California Democrat who heads the House Judiciary Subcommittee on Civil and Constitutional Rights, calls the proposal unprecedented and says it "would give the government a role in the design and manufacture of all telecommunications equipment and services."

Civil rights advocates worry that building wiretap capability for the police into every phone system will make it easier for anyone – from computer hackers to foreign spies – to listen in as well.

"Anytime there is a hearing on computer hackers, computer security, or intrusion into AT&T, there is a discussion that these companies are not doing enough for security," says Berman. "Now here is a whole proposal saying, 'Let's make our computers more vulnerable.' If you make it more vulnerable for the FBI, don't you make it more vulnerable for the computer thief?"

The legislation covers all forms of electronic communications – cellular telephones, fiber optics, satellite, microwave and wires – as well as electronic mail systems, fax machines and all networked computer systems.

Last Wednesday, representatives from computer companies such as Lotus, IBM, Microsoft, Apple and Prodigy met with the FBI in a three-hour session to voice opposition to the legislation.

"I think that the one thing that is clear to them now is that the business opposition to their proposals extends well beyond the traditional telephone companies," says Podesta.

Two systems converged

These issues are arising because computers and communications systems have converged, says Mitch Kapor, founder of Lotus Development Corp. and, more recently, of the Electronic Frontier Foundation.

"All computers communicate, and all communication systems use computers," he says. "Any proposal that attempts to control communications technology inevitably reaches to all computer technology – personal computers, workstations, local area networks. There really isn't any way of making a distinction that is a principled distinction."

The real showdown is likely not to be over wiretapping – most players concede the validity of the government's wiretapping need – but rather over encryption systems.

Last year, a bill was introduced in the Senate that would prohibit US companies from selling encryption programs or equipment that could not be decrypted by law enforcement agents with an appropriate court order. The bill was withdrawn after an outcry from the computer industry, which argued that encrypted messages that could be broken by law enforcement could be broken by others as well.

'If a friend of yours is kidnapped or [someone] puts a bomb in Fenway Park, and to solve [the case] we need to intercept communications, we need to be able to do it.'

JAMES K. KALLSTROM, *engineering chief for the FBI*

"Sessions said that he wanted to come back to the encryption issue, but [the wiretap legislation] didn't deal with it. That has been their line in public," says Podesta,

"They haven't given up on the notion that encryption is bad for law enforcement and potentially bad for America," Kapor adds. "The approaches which are being suggested now aren't facing up to the real problem.

"Given that we have mathematical ways of making totally secure communications, how is law enforcement going to be able to do its job? That's a profound question to which there aren't ready answers at hand."

Simson Garfinkel is a free-lance writer who lives in Cambridge.