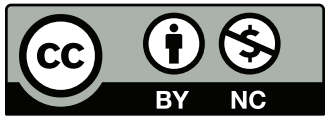
Wiretapping and Surveillance



What is Wiretapping?

Photo from Wikimedia Commons

- We all know what wiretapping is—some police officer with a *buttset* uses alligator clips to listen in on a phone line
- Higher-end wiretappers use tape recorders
- More or less this is actually done

Loop Extenders

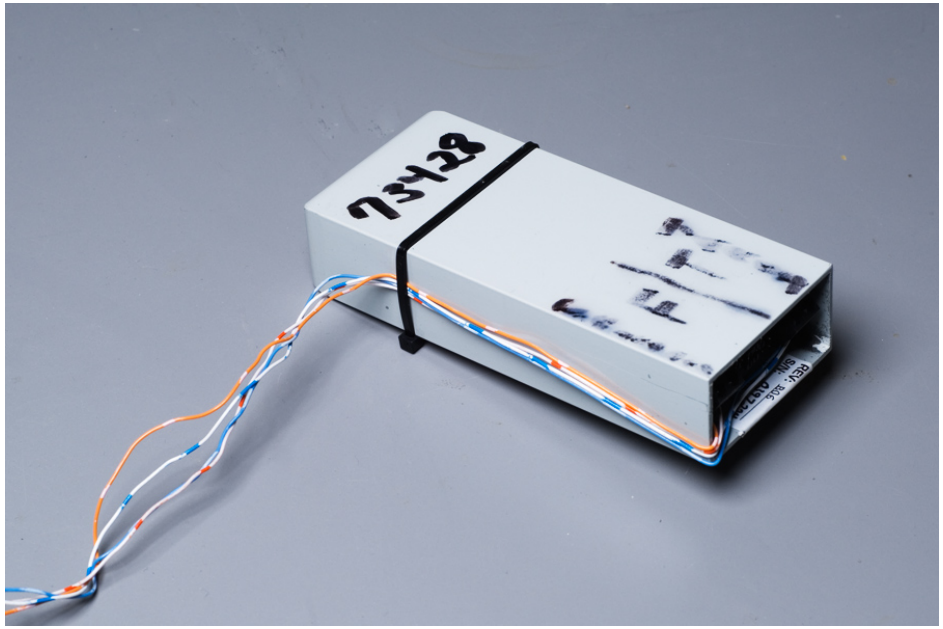


Photo © Matt Blaze; used by permission

- Attach one set of wires to the target's line.
- Attach the other set to an unused "friendly pair" to run the signal back to the central office.
- Listen in from the comfort of an office environment—no more cold vans. . .

What is Picked Up?

- Butt sets and tape recorders pick up sounds
- The numbers you dial are sounds
- If you have CallerID, the calling number is also a set of sounds

Pen Registers: What Numbers Did You Dial?

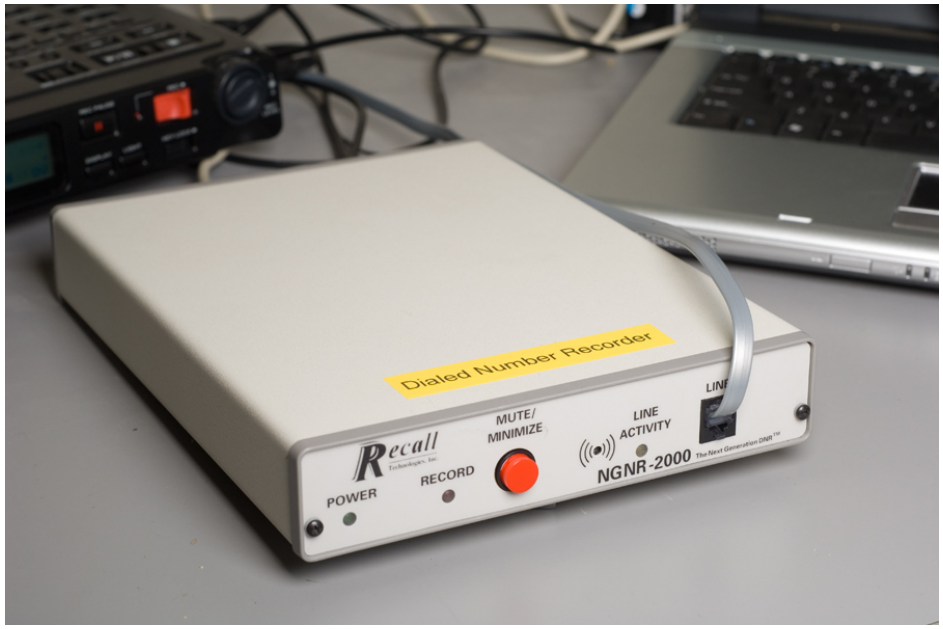


Photo © Matt Blaze; used by permission

- Note the phone jack on the front—it's designed to plug in to a standard phone line
- It just listens to dialing tones and records them
- The "minimize" button suggests that it's part of a general wiretap setup. "Minimize"?

Legal Distinctions

- Not all telephone “sounds” are treated the same way
- Who is the target of the wiretap?
- To whom are the sounds sent?

Why?

- Searches in the US are regulated by the Fourth Amendment to the US constitution
- (Is a wiretap legally a “search”? It is now—but before 1967, it wasn’t considered one)
- The Fourth Amendment bars “unreasonable searches”
- A warrant must “particularly describing the place to be searched, and the persons or things to be seized”
- Warrants require “probable cause”; mere suspicion isn’t enough

Minimization

- If a warrant names Person A, listening to Person B is not permitted
- “Minimization” is the process of excluding parts of the conversation not permitted by the warrant
- (But what if something incriminating is said by someone else?)

Content/Non-content

- Legal principle: if you voluntarily give information to a third party, you no longer have a “reasonable expectation of privacy” in it
- To make a phone call, you tell the phone company what number you’re calling
- You have therefore voluntarily shared it, so no warrant is required
- Legally, this is *non-content*

Metadata

- Metadata is the set of non-content information associated with a call
- For telephony, at a minimum that is the calling number, the called number, and the call duration
- Often, much more is revealed

The Full Setup

Photo © Matt Blaze; used by permission

- The recorder is hooked to the dialed number recorder
- A laptop controls everything

The Importance of Metadata

- It is very hard to hide metadata
- You can encrypt the call—but the phone company *must* know the number you're calling
- Metadata is very revealing

The EFF's Examples

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes.
- They know you called the suicide prevention hotline from the Golden Gate Bridge.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour.
- They know you received a call from the local NRA office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after.
- They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day.

(From `https://www.eff.org/deeplinks/2013/06/why-metadata-matters`)

Traffic Analysis

- A person from a suspicious country has a pattern: a short Skype call at the same time every week
- One week, there's a long call
- The next week, there's nothing. . .
- An agent checking in, a planning call, then the plan is in motion?
- Or a student hearing from home, learning of an illness, and then hurriedly returning?

Language Identification via Metadata

- On cell phones and VoIP phones, voice is compressed to save bandwidth
- Small frames (10–30 milliseconds) are compressed and sent as a single packet
- (The frames have to be short, to stay within the *delay budget*)
- Compression efficiency depends on the sounds in the frame—and different languages have different patterns of sounds

☞ This has been used to identify language in *encrypted* voice

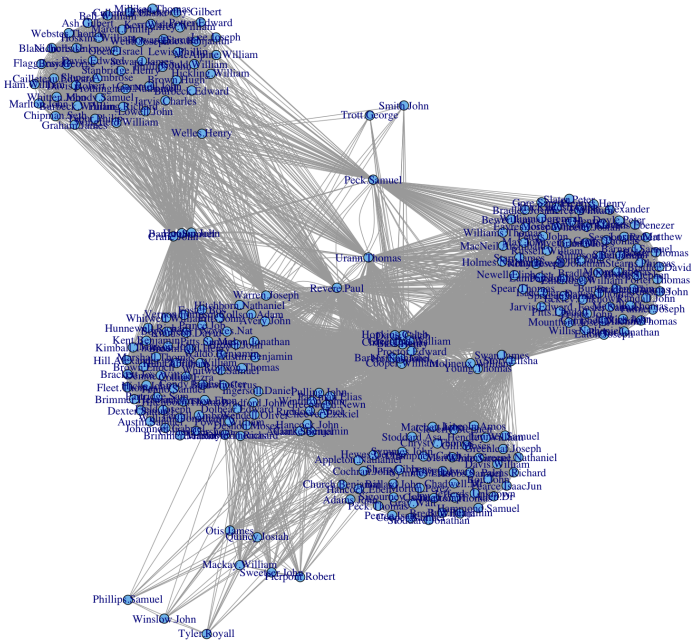
Contact Chaining

- Police are monitoring Alice, a known criminal
- Suppose Alice calls Bob.
- ☞ The metadata shows the association between them
- Now Bob calls Carol
- ☞ There is thus an indirect link between Alice and Carol
- Is she implicated?

Whom You Call is Unique

- No one else calls the same numbers that you call
- This can identify you, even if you change your phone number
- This has been done experimentally
- The same analysis picked out “communities of interest”: people whose calls tend to stay within the group

Finding Paul Revere Through Metadata



(From `http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/`)

Voluntarily Given: Samsung

"If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

`https://www.samsung.com/sg/info/privacy/smarttv.html`

Voluntarily Given: Verizon Patent Application

“To illustrate, access device 402 may detect, by way of detection device 406, that two users are cuddling on a couch during the presentation of the television program and prior to an advertisement break. Based on the detected ambient action, access device 402 . . . may select an advertisement associated with the ambient action. . . . To illustrate, access device 402 and/or the corresponding server device may utilize one or more terms associated with cuddling (e.g., the terms ”romance,” ”love,” ”cuddle,” ”snuggle,” etc.) to search for and/or select a commercial associated with cuddling (e.g., a commercial for a romantic getaway vacation, a commercial for a contraceptive, a commercial for flowers, a commercial including a trailer for an upcoming romantic comedy movie, etc.)”

US Patent Application 20120304206

Wiretapping in the Digital Age

- Less than half of Americans use traditional twisted pair land line telephones
- The FCC projects that by 2018, the traditional phone system will cease to exist
- You can't tap a cell phone with alligator clips!
- And what about data?
- The FBI understood this more than 20 years ago

Enter CALEA

- In 1994, Congress passed CALEA: *Communications Assistance for Law Enforcement Act*
- It required a standardized interface to tap calls, from the comfort of their own offices
- Applied to any “entity engaged in providing commercial mobile service” or “a replacement for a substantial portion of the local telephone exchange service” (P.L. 113-414(103)(8)(B))
- Did not apply to “entities insofar as they are engaged in providing information services” (P.L. 113-414(103)(8)(C))
- It now applies to ISPs, despite that last clause. . .

Lawful Intercept

- Most other industrialized nations have passed similar laws
- The generic concept is known as “lawful intercept”
- All major manufacturers of phone switches and IP routers support it
- Precise rules for access are different in each country

What's the Trouble?

- "It's only a software change"
- ☞ But phone switch software is *very* expensive
- Congress authorized some money for switch upgrades, but not nearly enough
- The system required complex software—and that's *always* a recipe for trouble

They Were Warned. . .

- “It’s too complex”
- “It’s vulnerable to remote hacking”
- “The real bad guys will use crypto”
- Guess what happened?

Hacking

- What if someone hacks into the wiretap platform?
- Could they delete data? Insert false data? Modify data?
- Could they use the lawful intercept mechanism to spy on someone else?

The Athens Affair

- Vodaphone Greece bought a phone switch with (legally mandated) lawful intercept capability
- Someone—just whom has never been established—installed binary patches into the phone switch to (ab)use this mechanism
- The attacker tapped about 100 cell phones belonging to senior government officials, including the Prime Minister
- One phone number on the list belonged to someone at the American embassy
- A copy of every call was relayed to another cell phone number
- These were prepaid phones, bought over the counter for cash
- A key person was found dead, an apparent suicide, just after the attacks was detected

What Happened?

- Writing the intercept software took a great deal of skill
- Planting it took a very sophisticated hacking attempt or cooperation from an insider
- Various log books were destroyed
- There was good “tradecraft”
- Was it an intelligence agency? Which one?

Other Hacks?

- "Israeli companies, spies, and gangsters have hacked CALEA for fun and profit, as have the Russians and probably others, too" (*I, Cringely*, July 10, 2003)
- Major wiretap scandal in Italy: "A team of security consultants ostensibly hired to test the security of Telecom Italia's security systems allegedly used Trojan horse malware and illegal wiretap techniques to spy on targets including Carla Cico, chief exec of Brasil Telecom, the Kroll investigative agency, and journalists Fausto Carioti and David Giacalone of Italian newspaper *Libero*." (*The Register*, April 14, 2008)
- More?

We Told You So

- CALEA wiretaps appear to be *more* expensive than conventional ones
- As a result, they're used much less often than predicted
- The predicted security problems have indeed appeared

Pen Register Complexities

- Under CALEA, what is a pen register supposed to capture?
- Dialed digits? Which dialed digits?
- Digits before you hit “Send” on your cell phone? How?
- Digits dialed after the call is established? Sometimes right, sometimes not — how can you tell?

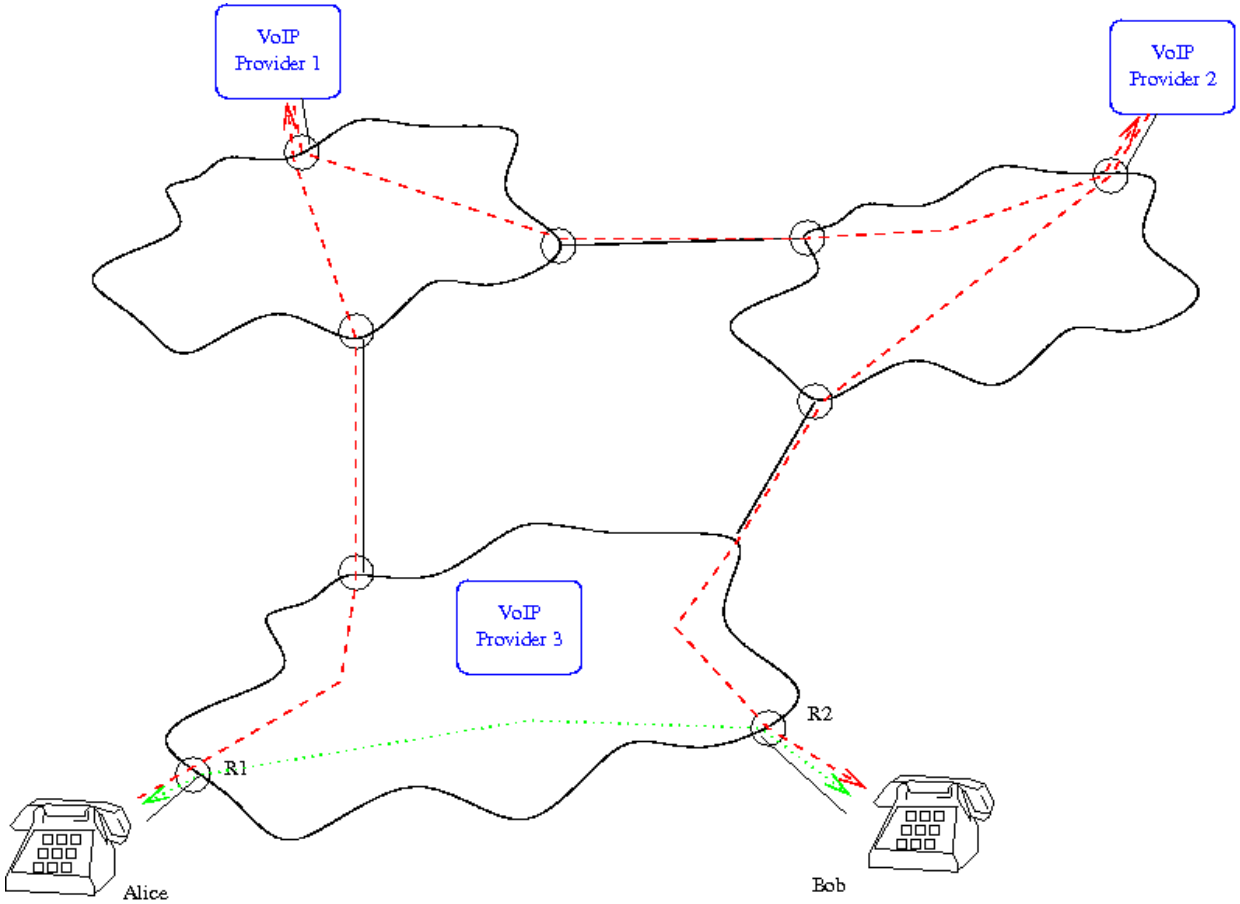
Yesterday's Answers to Today's Technology

- It used to be easy to captures digits as dialed, so the FBI wanted that ability to remain
- They ignored the fact that today's devices just aren't built that way
- Maybe the devices could be modified to do it if needed, but then taps would be detectable
- They tried to adapt to prepaid calling cards—but ignored other tone response systems: "For new reservations, press 1; for existing reservations, press 2; for the FBI guy who's listening to you, press 3"?

The Problem with VoIP

- VoIP calls can be tapped at two layers, the voice layer and the IP layer
- The IP layer knows nothing of telephony concepts like phone numbers
- If the signaling channel is encrypted, the ISP can't even look at it
- This means that a voice-layer tap should be done—but that doesn't work

Running VoIP



Tapping VoIP

- The ISP and the VoIP provider may not be the same
- The voice path isn't the same as the signaling path
- The ISP will be local—but the VoIP provider can be anywhere

Skype Makes it Harder

- Skype uses a peer-to-peer signaling network; there are no trusted nodes on whom the FBI can serve a court order
- The actual signaling path can vary from call to call
- Skype uses a strongly-encrypted voice path—*no one* can tap it
- The technology used is fundamentally incompatible with the model used by CALEA

Tapping IP is Hard Enough

- Connections are broken up into packets
- Packets can and do take different paths through the network
- It isn't easy to predict how any given packet will be routed, though different packets from the same connection tend to follow the same path
- Most inter-ISP paths are asymmetric, for sound network engineering reasons
- Conclusion: the only good place to tap IP is at the edge

What is Tappable?

- Phone lines are (mostly) point-to-point; there's a single pair of wires from the Central Office (CO) to a house

☞ A tap on that pair *physically* can't pick up any other people's phone lines

- The Internet is primarily composed of shared media

☞ The tap has to intercept lots of calls and then—via software—pick out the right ones

- How accurate is this process? Is there some violation from picking up everyone's traffic first?

But. . .

- The FBI was right in their prediction: conventional phones would go away
- For various other reasons, some of the newer phone technologies are of more interest to the mob and other targets
- You need sophisticated technology to tap these calls, but the sophisticated technology is *inherently* buggy