Telephone versus Internet Wiretaps
A Technical and Legal Perspective

Steven M. Bellovin
AT&T Labs – Research
http://www.research.att.com/~smb

Legal Basis for Wiretaps

- Katz v. United States, 389 U.S. 347 (1967)
- Smith v. Maryland, 442 U.S. 735 (1979)
- 18 USC 2510 et seq. ("Title III", as amended by the ECPA)
  - Complex procedure, many restrictions; a lot of justification is needed.
- 18 USC 3121 et seq. (pen registers and trap-and-trace devices)
  - Orders are easy to obtain; simple, unchecked assertion of relevance is all that's needed.
- 50 USC 1800 (FISA)

Legal Principles

- Wiretaps are "searches" within the meaning of the 4th Amendment (Katz).
  - Telephone users have a legitimate expectation of privacy.
- But dialed digits are not protected (Smith).
  - They are voluntarily "given" to the phone company.
  - People know that the phone company can and does record them, i.e., for billing.
- FISA: generally restricted to non-"U.S. persons".

Telephony in 1967

- No enhanced services.
  - Touchtone phones barely existed!
- Anything dialed was a phone number.
- Most calls had exactly two parties.
  - Enhanced calls required manual assistance.
- No ambiguity about who was involved in the call.
  - Easy to tell where to serve warrants, as well.
- Mostly analog transmission technology, with in-band signaling, and (often) on dedicated wires.

Circuit-Switching

- Data path allocated at call setup time.
- Dedicated facilities (wire pairs, time slice interval, etc.) used only for that call.
- Any point along the path receives both directions of the entire call.
- But – no signaling information in the datapath after call setup.

Consequences

- Little ambiguity about who was being tapped.
  - Shared phones, party lines, pay phones, and Centrex did exist.
- All dialed digits intended for CO.
- Trap-and-trace was slow, painful, manual, and unreliable.

Telephones Today

- Digital transmission, many shared facilities, out-of-band signaling.
- Many services rely on post-dial signaling: prepaid phone cards, voice mail, conference services, information services, voice menus, etc.
- Some enhanced services *don't* involve third-party gear (i.e., home answering machines).

Consequences

- Varied formats and signaling schemes led to CALEA.
  - Much debate about feasibility and meaning of some "punch list" requirements.
- Ambiguity about meaning of post-dial signals – on whom should warrants be served?
  - What type of court order is needed to listen to an answering machine's PIN?

Tapping the Internet

- Packet-based.
- International.
  - No strong notion of real-world geography.
- Strongly layered architecture.
  - Fields at different layers may be intended for different parties.
  - One layer's content is another layer's signaling.
- Strictly in-band signaling.
- Ubiquitous shared facilities.
- Intelligence at the edges, not the middle.

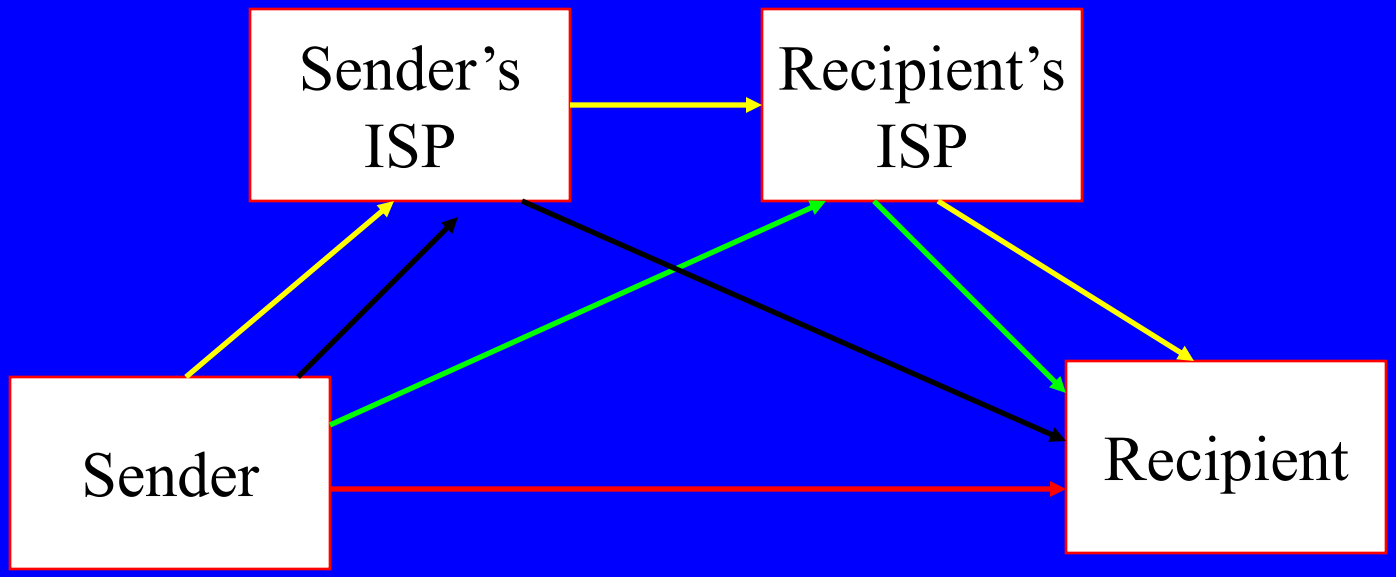
Packet-Switching

- Messages broken up into individual packets.
- Each packet has source and destination address.
  - Source address may be forged with little effort.
- Packets are routed individually via shared media.
  - Different packets can take different paths, though they usually don't over reasonably short time scales.
  - Return packets *often* take a different path through the backbone.

Consequences

- Easy to miss a few packets.
  - If address assignment packets are missed, subsequent collection is jeopardized.
  - Meaning of some packets is context-dependent.
  - Eavesdropper may have different view than communicants do.
- Unclear what packets are intended for whom, and hence what (legitimate) expectations of privacy there are.
- International nature makes matters murkier.

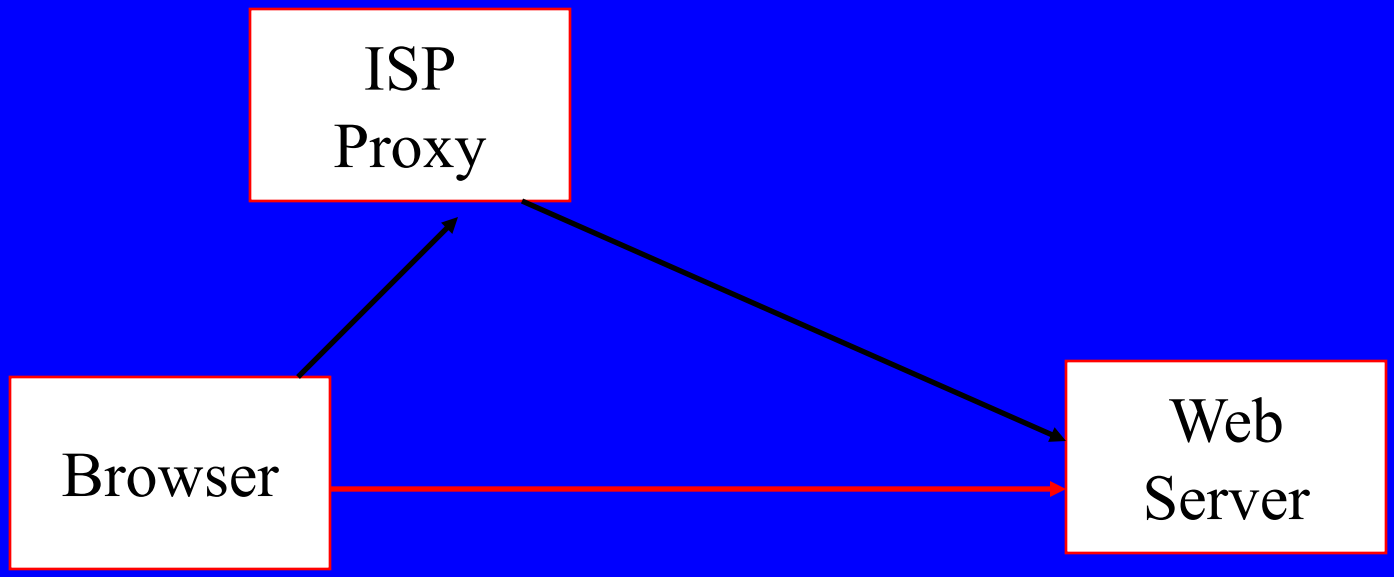
Email Scenarios



Who Receives What?

- Network-layer Path:
  - No expectation of privacy
  - May or may not be end-to-end for the underlying communication.
- To: and From: information:
  - Appears *twice* – in mail "envelope" protocol and mail header (the two can and do differ).
  - May or may not be end-to-end.
  - If not end-to-end, what if one ISP is in another country, with stronger privacy guarantees?

Web Scenarios



Who Receives What?

- User sees connection as end-to-end.
  - Probably expects privacy.
- Browser may be configured to use ISP's proxy server.
  - Most users know nothing of this.
  - Never any per-URL billing.
  - Users probably see this as equivalent to end-to-end case.
- ISPs sometimes use "transparent proxies"
  - Violates knowledgeable users' expectations.

Intelligence at the Edges

- In the telephone world, most intelligence is in the network.
  - But that's slowly changing, with things like remote-control answering machines, etc.
- In the Internet, virtually all intelligence is on the end systems.
  - Any user can create a new service, without help from (or knowledge of) the ISPs.
- Hard to tap if you don't know what it is, or what rational privacy expectations are.

What Do You Learn from Taps?

- Much interesting information is not end-to-end.
  - End-user IP addresses are generally transient.
- Higher-level information from log files can be more useful.
- This may change if and when peer-to-peer protocols become common.
  - But the bad guys will then have to solve the rendezvous problem, which provides another monitoring point.
- What kind of court orders are needed?
- Is the end-user a “U.S. person”? How do you know?

Conclusions

- The telephony wiretap model does not fit the Internet very well.
  - It's fitting the telephone world less and less well, too.
- Much of the difficulty stems from the (possible) end-to-end nature of the Internet.
- Low-burden court orders for pen register analogs may not be constitutional.
- But full-content wiretap orders are overkill.
- I suggest that the standard for non-content Internet taps be similar to that for search warrants.