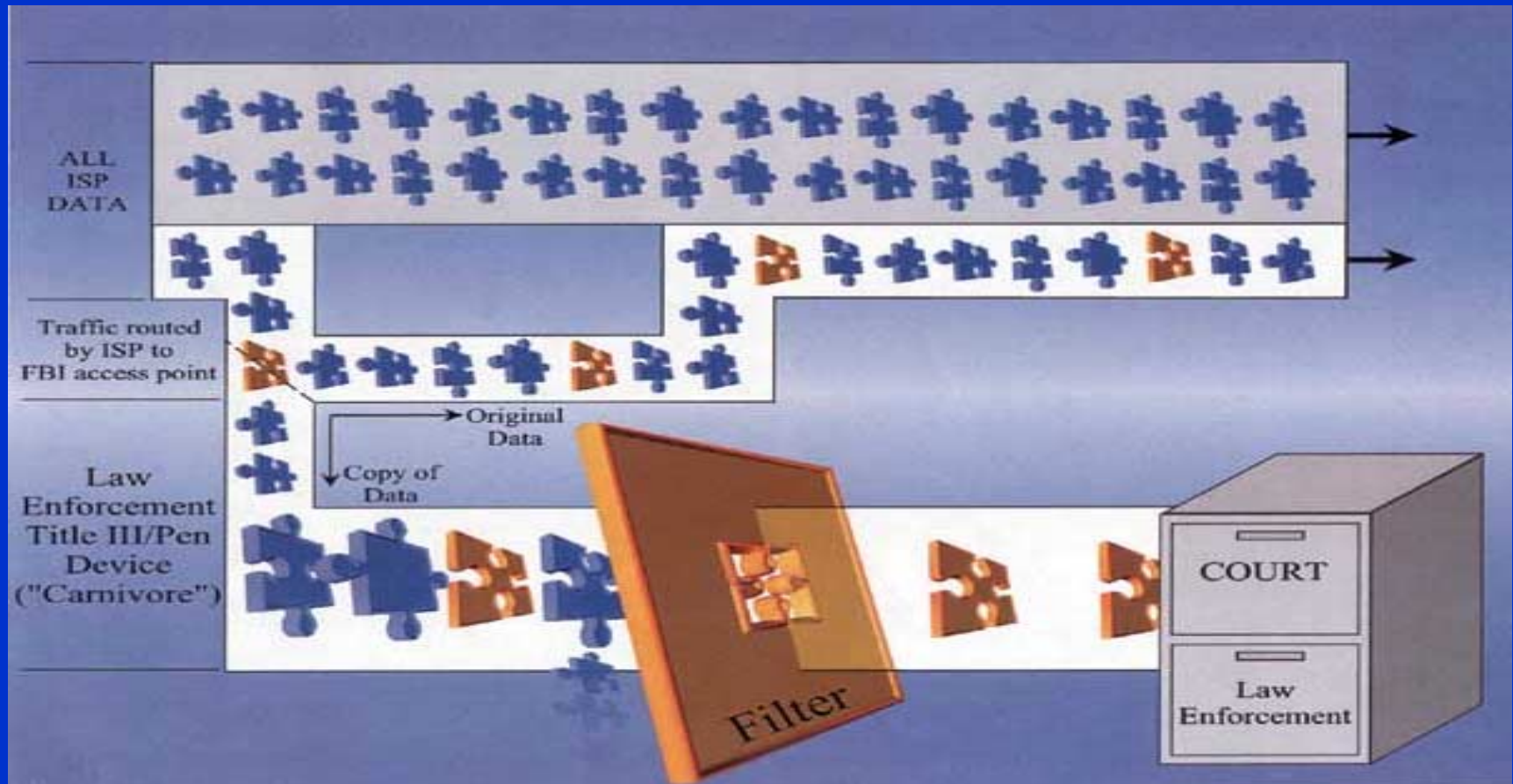


NE-ISSA/HTCIA Meeting January 23, 2001

Privacy, Law Enforcement and Carnivore: Good Ideas / Awful Names



Background

Where I'm Coming from...

NO.
I Do NOT Work for the FBI.

But I do have some “helpful” suggestions...

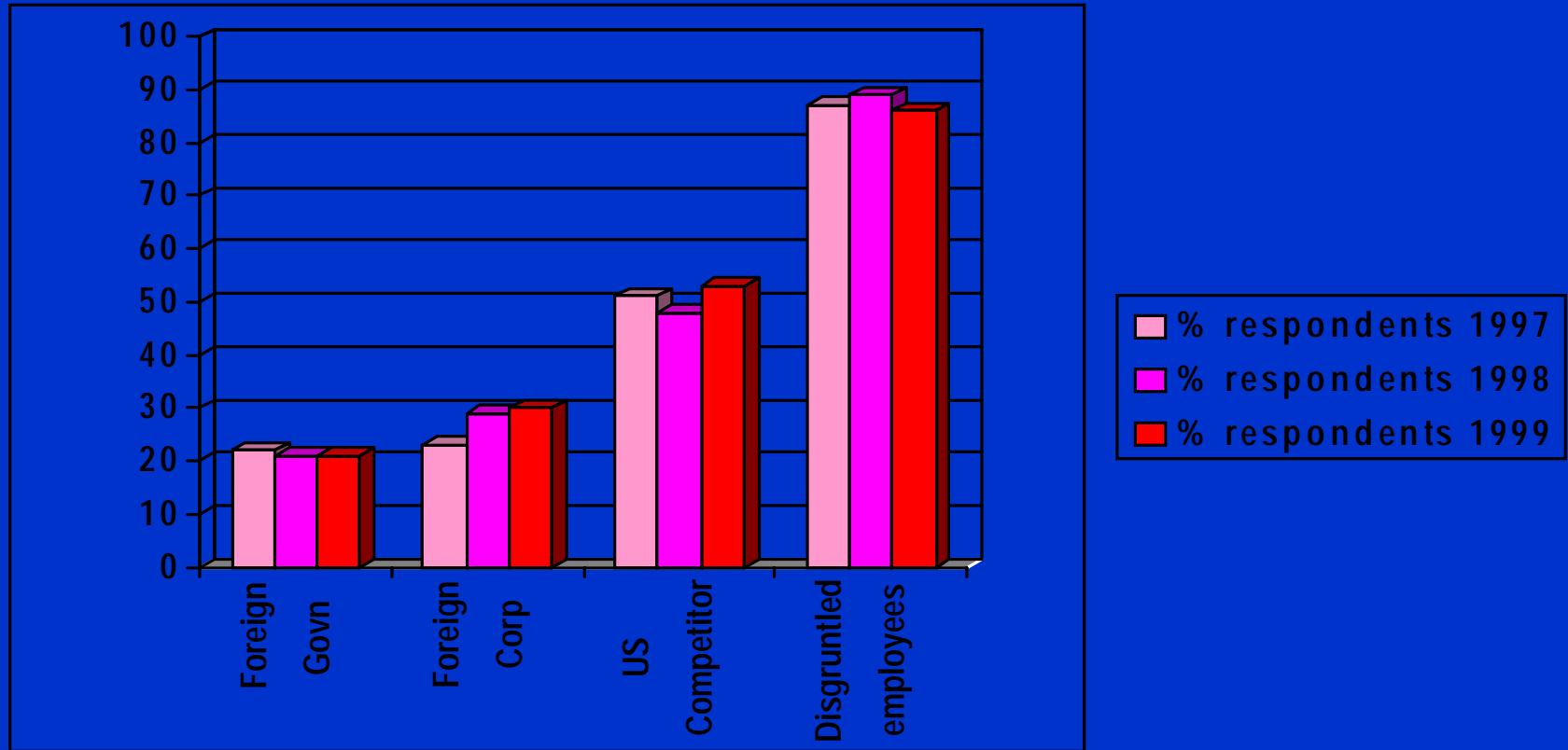
- Don't name it Carnivore 2.0, try something like:
 - The Packet Roadshow...
 - Snufalufagus
 - Bambi

Background:

Steady Rise in Computer Crime

- FBI/CSI 2000 Computer Crime and Security Survey:
- 90% (large corp./gov. agencies) detected breaches within the last 12 months.
- 70% reported serious breaches
- 74% acknowledged financial losses
- 42% were willing and/or able to quantify:
 - 273 respondents = \$265,589,940 Lost
 - The average annual total over the last three years was \$120,240,180.

Background: Who are the biggest threats?



Background:

How much does it hurt?

Loss experienced	1998	1999
None	28%	24%
Up to \$1,000	6%	8%
\$1,001 to \$10,000	8%	11%
\$10,001 to \$100,000	5%	6%
\$100,001 to \$500,000	2%	2%
\$500,001 to \$1,000,000	1%	<1%
\$1,000,000+	1%	1%
Unknown	49%	47%

Source: 1999 PricewaterhouseCoopers Information Week Survey

And It's Probably Worse Than We Think...

- Dept. of Defense (GAO - June 1996)
 - Estimated Attacks in 1995: 250,000
- DoD Controlled Study
 - Machines Attacked: 38,000
 - Machine Penetrated: 24,700 (65%)
 - Attacks Detected: 988 (4%)
 - Attacks Reported: 267 (27%)

Future - What's to come?

Start with the Charney Theorem

- + Add anonymity
- + Add global connectivity
- + Add critical infrastructures
- + Computer Forensics

= Trouble

Ask Yourself Four Questions:

- Should law enforcement play a part in addressing computer crime?
- If LE is going to play, don't they NEED a sniffer?
- Is there anything illegal about sniffer use?
- Is there something wrong with the particular sniffer (Carnivore) they have (other than the name)?

Should Law Enforcement Play a Part in Addressing Computer Crime?

DUH!

Should Law Enforcement play a part in addressing computer Crime?

- Corporations CANNOT deal with this problem alone:
 - Access problems
 - Publicity problems
 - Jurisdictional problems
 - There are places only LE can go
- It's not just computer crime anymore...
- FISA

If LE is going to play, don't they NEED a sniffer?

- The need is obvious:
 - Hacking 101 covers “looping”
 - Relying on the Victim/Provider is dangerous
 - Remember the stats on insiders?
 - Free/Anonymous/Rogue providers difficult
 - Logs are not perfect (if they exist at all...)

Legal Authority Clearly Exists:

- Legal authority clearly exists:
 - 18 U.S.C. 3122 (Pen/Trap)
 - 18 U.S.C. 2516(3) (Wiretap)
 - FISA (Wiretap and Pen/Trap)

The Legal Side of Pen/Trap

- Ok, so authority is about as clear as the 2000 Presidential Election results...
- 18 U.S.C. § 3127(3)
 - the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached...
- 18 U.S.C. § 3127(4)
 - the term "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication

The Legal Side of Pen/Trap

- Court order in the District where monitoring occurs (e.g., victim site)
- 60 days, plus extensions
- Very low legal threshold
 - “law enforcement or investigative officer” must “certify to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3123

Legal Side of Electronic Wiretap

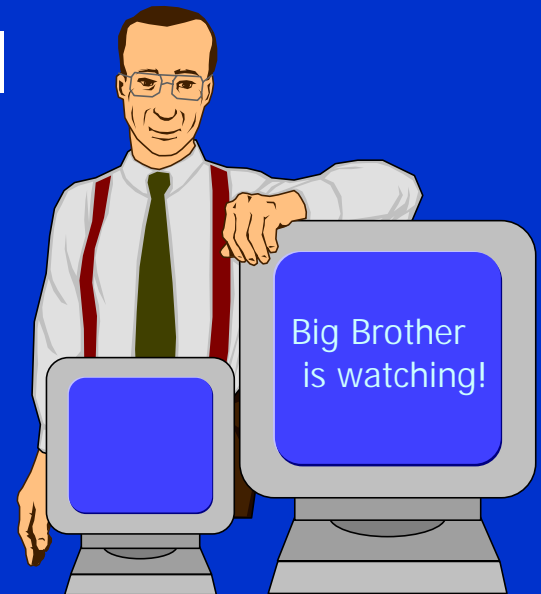
- Grabbing real time content from IP packets is an “interception” of “electronic communication” under 18 U.S.C. § 2511
- Sniffers that pick up packet content violate Title III unless you have a court order or an exception applies
- **BEWARE OF VOICE OVER IP** (Do even more stringent standards apply?)

Sysadmin use of Sniffers works in some cases...

- Two exceptions *usually* permit sysadmin of of victim machine to install a sniffer
- Self-defense, 18 U.S.C. § 2511(2)(a)(i)
 - “provider of . . . electronic communication service” may intercept communications on its own machines “in the normal course of employment while engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service.”

Banners and the Consent Exception

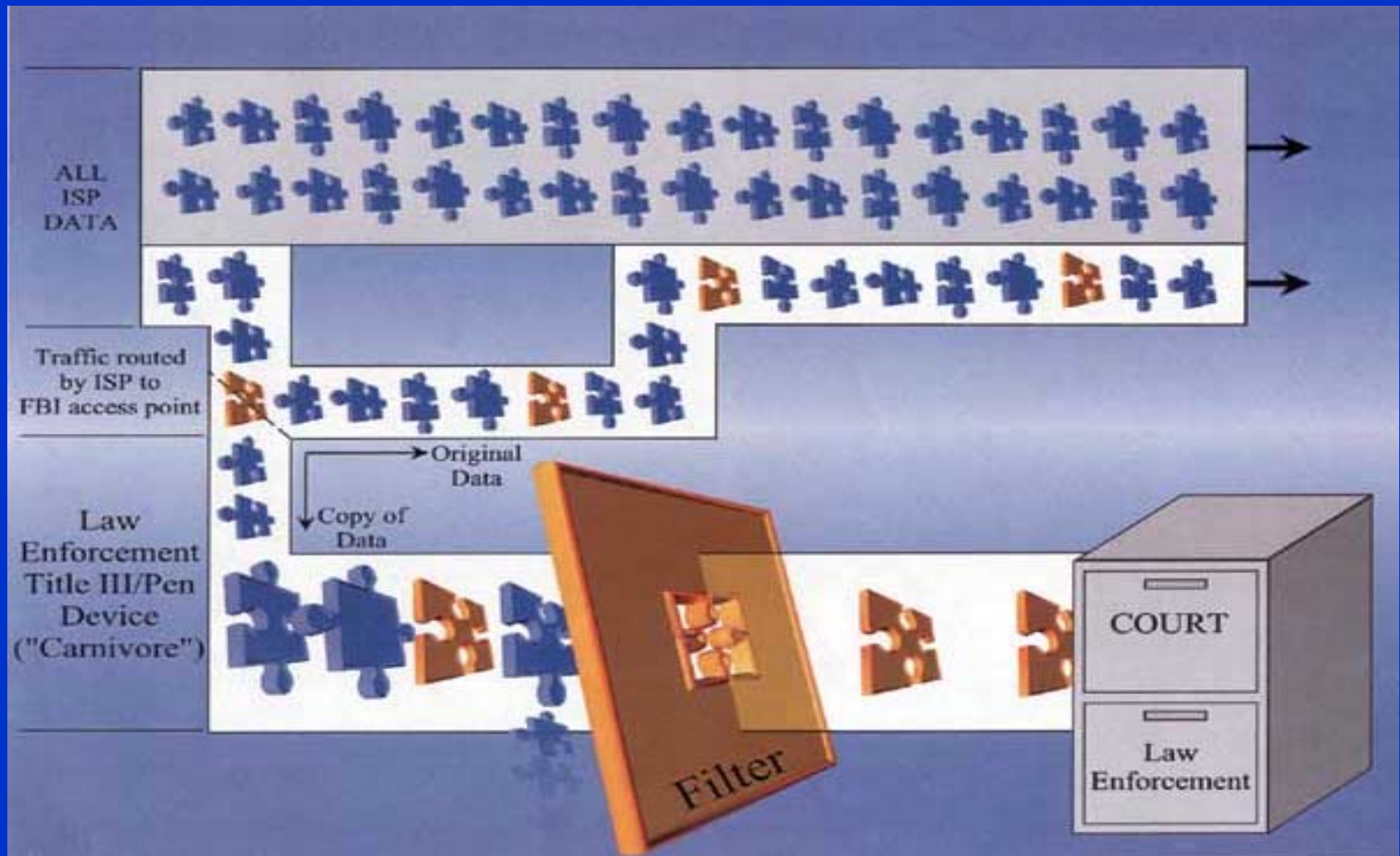
- 18 U.S.C. § 2511(2)(d)
 - May intercept a communication if a “party to the communication has given prior consent to such interception.”
- Banner announcing that “all communications may be monitored” on system creates “implied” consent, permits monitoring.



LE use of a sniffer works if...

- Consent exception applies equally
 - § 2511(2)(c) instead of § 2511(2)(d)
- If no banner is up, need Title III order
 - Allowed if P.C., interception “may provide . . . evidence of any Federal felony.” § 2516(3)
 - Less intrusive techniques “reasonably appear unlikely to succeed”
 - Short time period, minimization, etc.

So, is there something wrong with the sniffer they have?



Not Perfect...but consider the alternatives!

- Telephones are easy
- New technology = trial and error intercepts
- Carnivor is better than its predecessors (Oh, the stories I could tell...)

Carnivore's Advantages

- Known quantity
- Intended to allow compliance with court orders
- 3rd Party testing/Public Scrutiny
- Ongoing training program

Some weaknesses, especially for Pen/Trap orders...

- Devil is in the details
 - Translation from court order to data capture
 - Treatment of variable length headers
 - Remote access / security issues
- Pen/Trap and Wiretap capability in the same tool?
- No audit trails

Carnivore as Wiretap

- Should be less controversial (but isn't)
 - More precise minimization possible
 - Real Time: text string searches, time parameters, etc. (which causes some problems...)
 - Post collection minimization
 - Still less intrusive than telephone
- Could be better...
 - Audit functions
 - Hash of collected data / settings

Why do we care (so much)...

- Potential volume of data is SO huge that fear of extensive unjustified collection is probably unfounded.
- Even if data inappropriately collected, processing of random collections nearly impossible.
- Ever hear of encryption?

Work in Progress

- Current version(s) are just the beginning
- Tool will always be a few steps behind new technologies
- Source code releases may occur (but I wouldn't do it if I was [Ashcroft?]....)