Computers and Society

Carnivore

Chris Brooks

Department of Computer Science
University of San Francisco
Carnivore is a system developed by the FBI to track and intercept email.

If the FBI wants to monitor a person’s email, they place Carnivore on the person’s ISP’s incoming email.

Carnivore is a “packet sniffer”

Court order required.

All email for that person is filtered and captured by Carnivore.

Can also capture downloaded files and chat room logs.
1: *Relationship to phone tapping*

- Law enforcement has long had the ability to conduct telephone surveillance.

- Two types:
  - Wiretapping - conversation is recorded. High standard of evidence needed. (probable cause)
  - List of phone calls made/received. Lower standard needed.
    - Trap-and-trace, pen register. Can be used for background info.

- How does email compare to telephone conversations?
There’s not a practical way to only filter one person’s email without putting a program on their computer.

- Unlike your phone line, there’s no way to directly “tap in” to your computer.

Phone records are subject to a lower standard because of the lack of private information they contain.

- Email headers might contain more sensitive information

Law enforcement is being trusted not to look at other email.
Arguments for Carnivore

- Terrorists, organized crime, con artists, drug dealers, and child pornographers all use email (and the Internet more generally) to plan and commit crimes.
- Electronic surveillance is commonly accepted in mail and telephone.
- Federal laws protecting privacy require that authorities get a court order before using Carnivore.
- There are strong legal penalties for misuse of Carnivore.
-4: Arguments against Carnivore

1. The FBI has kept the working of Carnivore a secret.
2. How can we verify that the system cannot be misused?
   - We have no way of knowing if other information is being recorded.
3. Carnivore collects more information than is legally allowed.
4. Carnivore lowers a legitimate user’s ’expectation of privacy’
5. Past FBI abuses provide an air of skepticism about innocent people’s email being read.
5: Relevant issues

- What are peoples’ fundamental rights in cyberspace?
  - Real-world analogues don’t always map directly.

- How do we balance the legitimate needs of law enforcement against our country’s long-held right to privacy and presumption of innocence?

- What sorts of safeguards can help?
In my opinion, the FBI should make the Carnivore system available for inspection and evaluation to an independent group of security and privacy rights experts.

△ The FBI has been reluctant to reveal details of Carnivore, which makes it look worse than it may be.

This would allow skeptics to verify that appropriate safeguards were in place.

Potential “back doors” or misuses could also be identified.

The FBI should also provide private ISPs with filtering tools.

△ Under court order, an ISP could then provide the same information that Carnivore would be used to collect, without government filtering of other emails.
-7: References

6 FBI’s Congressional statement on Carnivore. Available at: http://www.fbi.gov/congress/congress00/kerr090600.htm