

What is Carnivore?

A. : Carnivore is an electronic "wiretapping" tool, currently in use by the FBI.

Details of how the system works are short on specifics. What is known is that Carnivore would be installed at the suspect's Internet service provider to scan all incoming and outgoing emails--including sender and recipient addresses as well as subject lines--for messages related to a criminal probe. And while the system, a sophisticated combination of hardware and proprietary software, can perform fine-tuned searches, it is also capable of broad sweeps, potentially enabling the agency to keep tabs on all of the network's communications. "The FBI is placing a black box inside the computer network of an ISP," Dempsey told the Associated Press. "Not even the ISP knows exactly what that gizmo is doing."

What Can Carnivore Do?

The FBI has been reluctant to disclose many details about the Carnivore spy tool which has been in use since early 2000, but what is known is this: Carnivore is a combination of hardware and software, which can "sniff" (read or scan) all electronic packets that are sent to and from the ISP (Internet Service Provider) where it is installed. With this info, Carnivore can, theoretically:

- Read all incoming and outgoing e-mails, including sender, recipient(s), message subject and body;
- Monitor the web-surfing and downloading habits of all the ISP's customers, including web searches for information or people;
- Monitor and/or read all other electronic activity for that ISP- including instant messages (such as with ICQ), person-to-person file transfers, web publishing, FTP, Telnet, newsgroups, online purchases, and anything else that is routed through that ISP;

What Carnivore Could Do:

That's what Carnivore can do when installed at a single ISP. But what happens if Carnivore goes unchecked, and gets installed at most or all ISPs? All that would take is for the FBI to justify one Carnivore-based investigation at each ISP. This could happen within a year or two if left unchecked. Let's look at what it could mean if Carnivore, and the FBI, were installed at all ISPs in the US: The biggest threat would be the FBI's new ability to mandate Internet law. One of the great powers of the Internet is the fact that it exists beyond the control of any one person or agency. Almost all efforts to introduce Internet legislation has either been defeated or postponed, usually because enforcement is found to be impractical. Also, any activity that the U.S. might try to prohibit can still be conducted in another country with different laws, and, through the Internet, can still be accessed by Americans.

The Communications Decency Act (basically a censorship law) provoked such a massive e-protest that it was largely abandoned. Internet gambling, online auctions, and music sharing have all largely avoided regulation, because lawmakers know that if you ban it in one place on the 'Net, it will just show up somewhere else.

Carnivore could change all that. With Carnivore installed at all U.S. ISPs, the FBI could (for example):

- Ban any language or content found to be objectionable, by interception, deletion, or alteration.
- Monitor the country's communications, and target any person who was found or suspected to be a "problem." The judge of who or what is a "problem"?: the FBI.
- Invoke mandatory standards for web sites, such as a rating system (like with movies), or lowering security standards (like prohibiting encrypted messages and secure private web sites).
- Shut down or shut off the communications of any one person, website, company, or ISP. As columnist Robert Cringely put it, they could "Shut the Internet down."

Many people would like to believe the best about our Government, and assume that they wouldn't do such a thing. But most of the efforts by the U.S. Government to control the Internet have failed, not because they didn't want to make the law, but because the nature of the Internet (free and fluid) wouldn't allow it. Carnivore will change that, if we don't take action now. The United States is home to the vast majority of Internet traffic. AOL alone has over 50 million users, and the number of e-mail accounts in the U.S. has been reported as over 300 million. Most of this country's residents use the Internet in some way, and more so as time goes on.

What's more, communications technology is converging in such a way that traditional technologies, like phone, radio, cable TV, satellite, and wireless, are all becoming part of the Internet. More and more of our communications are sent over the Internet every single day, and the day will come when the Internet will be the transmission tool for virtually all communications (aside from "live," in-person talking). The U.S. is positioned to be the major provider of these services, for its own people, and the rest of the world.

A few years down the road, when your phone company, your cable TV provider, radio stations, and cell phone company are all part of your "ISP", and Carnivore is installed there, the FBI will have exclusive control of what you can and can't watch, say, or do while using these technologies. And if you happen to say, or read, or watch something that raises their suspicion (like, say, shopping for **hemp** clothing, or saying you **hate** something, or advocating **drug legalization**), you could very well find yourself being served with a search warrant, by people very much like the ones that seized Elian Gonzales from his Miami relatives. If that's not something you want to look forward to, then take action now, and let's get together and Stop Carnivore!

Why Carnivore Is Bad For You

There are a large number of problems with the FBI's use of a system like Carnivore, and some Americans may agree or disagree on any number of different points about it. But Carnivore is so offensive to the American Way that there are a few things about it which just about every American should agree are unacceptable.

Here are some reasons why Carnivore is bad for America, and, more specifically, bad for **you**:

It's Unconstitutional: The Constitution is largely a document of limits- limits on the ways in which Government may interfere with our lives. The Bill of Rights (the first ten Amendments to the Constitution) is a short list of specific aspects of our lives which Government may not interfere. The **4th Amendment** clearly prohibits such sweeping invasions of privacy and property as Carnivore commits: *"The right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

Internet communications would qualify as our "**papers and effects**". Even the actual suspects of FBI investigations are having their rights violated by Carnivore. Again, the 4th Amendment states that "no Warrant shall issue" except that which "particularly describ(es) the place to be searched, and the persons or things to be seized." In a Carnivore investigation, the "things to be seized" are not able to be particularly described

This is not a case of someone having documents in their house which may incriminate them, or of stolen goods which are part of a crime. A Carnivore warrant, when issued, is a warrant for documents which may or may not exist in the future- letters which have not been written. In Internet terms, the "place" which is being search cannot be "particularly described." If a suspect is surfing a website that is hosted in California, California is the "place" of that information- the place where the activity occurred, or the document's location, if it's a website. If the FBI's Carnivore system is installed at the suspect's ISP, in New York for example, how could the warrant include a search in California, or any of the other locations where the suspect's activity may take place? When seeking a Carnivore-based warrant, the FBI has no way of knowing or describing the "places" to be searched, or the "things" to be seized. Like it or not, our 4th Amendment prohibits broad-based Internet investigations, such as those conducted by the FBI's Carnivore system.

It Threatens Freedom and The Internet: The best thing about the Internet, the thing which has allowed it to prosper as much as it has, is lack of centralized control. An while there are those who would use this lack of control to their criminal advantage, it would be a far worse consequence to give up the "chaos" in favor of stringent control. All of the wondrous possibilities that the Internet offers us come at the price of it having no central control or governing body. To impose that type of control will be at the expense of the freedoms which have made the Internet what it is today. For 30 years, Government control stifled and suppressed the growth of the Internet. We must not allow such a fate to be reinstated.

The vast majority of Internet traffic travels through U.S. servers. Most users, designers, hosts and ISPs are located in the U.S. If Carnivore were to be installed at all U.S. Internet servers (which is a logical outcome of its deployment), the FBI would possess a "valve" or "filter" through which almost all of the world's digital information will pass. It will be in their power to intercept or interfere with the transmission of data, in the most specific ways, and in the most general. (For more on this, see [What Can Carnivore Do?](#) on this site.) In the fight against pornography, the FBI could block the viewing of any images with certain suspicious filenames, or block access to pornographic domains.

In the fight against drugs, the FBI could shut down legalization advocacy sites, educational information about safe drug use, and information explaining the manufacture, use, or distribution of "illegal" drugs. (There is [a bill before Congress right now](#) which would give them legal authority to do this. Carnivore would give them the ability to enforce it.) Additionally, they would be able to scan everyone's e-mail for drug references, and monitor everyone's surfing to find "offending" sites. In the fight against hackers and terrorists, the FBI could seize control of any portion of Internet traffic, under the guise of national security or investigative need, shutting off accounts, ISPs or even cities or regions to "contain" whatever it is they are investigating. In the fight against "hate crimes" and "damaging" speech, the FBI could literally remove such "offensive" terms from our communications. They will hold a virtual big black marker which can be used to block "dangerous" or "threatening" ideas and images from our tender and innocent eyes and minds.

Do you think that the FBI would not dare to snoop where they shouldn't or needn't be snooping? Remember, this is the same FBI that kept extensive files on Martin Luther King, Jr., Marilyn Monroe, and John Lennon, not to mention countless celebrity "communists" and dissidents. Do they still keep those kind of files? You tell me. Would Carnivore help widen the range, scope, and frequency of frivolous violations of privacy such as those? Absolutely. Do you think that your Government would never allow such blatant and reckless behavior from one of its Agencies? This is the same Government that drove the Branch Davidians to their deaths. (The same Government which is trying to pass *three different laws*, all containing [certain duplicate clauses](#), which would outlaw the drug-related information I spoke of above. One of these laws is a *bankruptcy bill*!) The same Government that fed LSD to unsuspecting black military personnel. The same one that corralled Japanese-Americans during World War II, persecuted "communists" in the 50's, beat hippies and burned Vietnam in the 60's and 70's, sold weapons to our enemies in the 80's, and beat the crap out of Rodney King but let O.J. Simpson walk free in the 90's. Our Government does not always follow rules that make sense; nor does it uniformly respect our rights. Not by a long shot.

While Government does seem to be trying to pursue good for all, it has shown itself more than willing to destroy the rights of some, in pursuit of protecting the rights of others. Carnivore will give Government the power to do that in such a way as we have never seen before. Remember, this is the same Government that fed LSD to unsuspecting black soldiers, with the goal of better protecting us. You've been warned.

It Sets a Bad Precedent: What if the FBI said they wanted to monitor all telephone calls, for information about suspected criminals? What if they wanted to intercept all postal mail, to check and see if any of it was related to any of their suspects? What if they wanted to do a "profile" of the average marijuana user, by scanning huge amounts of electronic data, and compiling the marijuana-related communications? What if they wanted keys to everyone's houses,

in case they had to get inside to investigate a crime? Use of the Carnivore system plants the seeds for all of those types of developments, and many more frightening ones. No, the FBI will not be asking for permission to intercept all postal mail anytime soon. But the majority of non-verbal communication already takes place over the Internet, and that portion grows every day. A time will come when postal mail is an insignificant factor in our communications. By that time, the FBI may already have the "keys" to all the rest of our communications, via tools like Carnivore.

It is only a matter of time before our telephone, satellite, and television communications are intricately intertwined with the Internet. The time will come, sooner rather than later, when your ISP will be your phone company and your cable company and your cellphone provider and your long distance provider. Your banking, shopping, and other financial dealings will mostly take place through the Internet. Eventually, your home appliances, your car, your town's streetlights, and even perhaps your medications will all be affected or controlled to a certain degree by the Internet. Like it or not, that is the path that we are heading toward. You will only be able to avoid it for so long- eventually it will be like avoiding use of roads or electricity or telephones- nearly impossible, and only possible by severe estrangement from mainstream society.

Carnivore is a bad precedent because it places Government at the hub of all of this coming technology. It gives the FBI (and by extension, every Government agency) a "backstage pass" into our global communications- and, in almost every case, without our knowledge or consent. (In fact, there is another bill before Congress which would make it a felony to notify you if you are being investigated through a wiretap warrant.) Eventually, all of our communications except for face-to-face conversations will pass by the ears and eyes of the Federal Government. The majority of what we say, watch, and do will be available to federal agents at their discretion. As frightening as it may be, this is the precedent that is being set through continued use and tolerance of the Carnivore ISP spy tool. If it is not stopped, it will grow. As it grows, our right to privacy and freedom shrinks.

Secret plan to spy on all British phone calls

Kamal Ahmed, political editor

Sunday December 3, 2000

The Observer

Britain's intelligence services are seeking powers to seize all records of telephone calls, emails and internet connections made by every person living in this country. A document circulated to Home Office officials and obtained by The Observer reveals that MI5, MI6 and the police are demanding new legislation to log every phone call made in this country and store the information for seven years at a vast government-run 'data warehouse', a super computer that will hold the information. The secret moves, which will cost millions of pounds, were last night condemned by politicians and campaigners as a sinister expansion of 'Big Brother' state powers and a fundamental attack on the public's right to privacy. Last night, the Home Office admitted that it was giving the plans serious consideration.

Lord Cope, the Conservative peer and a leading expert on privacy issues, said: 'We are sympathetic to the need for greater powers to fight modern types of crime. But vast banks of information on every member of the public can quickly slip into the world of Big Brother. I will be asking serious questions about this.' Maurice Frankel, a leading campaigner on personal data issues, called the powers 'sweeping' and a cause for worry. The document, which is classified 'restricted', says new laws are needed to allow the intelligence services, Customs and Excise and the police access to telephone and computer records of every member of the public. It suggests that the Home Office is sympathetic to the new powers, which would be used to tackle the growing problems of cybercrime, the use of computers by paedophiles to run child pornography rings, as well as terrorism and international drug trafficking.

Every telephone call made and received by a member of the public, all emails sent and received and every web page looked at would be recorded. Calls made on mobile phones can already be pinpointed geographically, as can those made from land lines. The police would be able to use 'trawling' computer techniques to look through millions of telephone and email records. Campaigners say innocent people could have such highly personal information accessed. The document admits the moves are controversial and could clash with the Human Rights Act, which gives people a right to privacy, European Union law and the Data Protection Act, which protects the public against official intrusion into private lives. The office of the Data Protection Commissioner, Elizabeth France, has already expressed 'grave concerns'. 'A clear legislative framework needs to be agreed as a matter of urgency,' says the document, which is dated 10 August and is thought to have been sent to Home Office Minister Charles Clarke. 'Why should data be retained? In the interests of justice, to preserve and protect data for use as evidence to establish proof of innocence or guilt. For intelligence and evidence gathering purposes, to maintain the effectiveness of UK law enforcement, intelligence and security agencies to protect society.'

The document is written by Roger Gaspar, the deputy director-general of the National Criminal Intelligence Service, the Government agency that oversees criminal intelligence in the United Kingdom. Gaspar, as head of intelligence for NCIS, is one of the most powerful and influential men in the field. The report says it is written 'on behalf of Acpo [the Association of Chief Police Officers], HM Customs and Excise, security service, secret intelligence service and GCHQ [the Government's secret listening centre based at Cheltenham]'. Gaspar argues telephone companies should be ordered to retain all records of phone calls and internet access. At the moment many telephone and internet service providers keep data for as little as 24 hours.

In the interests of verifying the accuracy of data specifically provided for either intelligence or evidential purposes, CSPs [communication service providers such as telephone or internet companies] should be under an obligation to retain the original data supplied for a period of seven years or for as long as the prosecuting authority directs,' the document says. 'Informal discussions have taken place with the office of the data protection commissioner.

Whilst they acknowledge that such communications data may be of value to the work of the agencies and the interests of justice they have grave reservations about longer term data retention.' The document says the new data warehouse would be run along similar lines to the National DNA Database for profiles of known criminals. It would cost about £3 million to set up and £9m a year to run. The report demands that the Government 'should be prepared to defend our position'. A spokesman for NCIS refused to be drawn on the report. 'I am not going to comment on a classified document that is in unauthorised hands,' he said. Meanwhile a Home Office spokesman said it had received the proposals and was considering them.

Guardian Unlimited © Guardian Newspapers Limited 2001

Judge orders emergency hearing on FBI's Carnivore

August 2, 2000

Web posted at: 2:42 p.m. EDT (1842 GMT)

WASHINGTON (Reuters) -- A federal judge ordered an emergency hearing Wednesday on a privacy rights group's request for the immediate release of details on Carnivore, the Federal Bureau of Investigation's e-mail surveillance tool. The Electronic Privacy Information Center (EPIC), in its application to the judge, accused the FBI and the Justice Department of breaching the law by failing to act on a request for fast-track processing of a Freedom of Information Act query about the snooping system.

In July the FBI told Congress Carnivore is designed to intercept data from the electronic mail of a criminal suspect by monitoring traffic at an Internet service provider. EPIC wants the FBI to disclose how it works. U.S. District Judge James Robinson set the hearing for 3:30 p.m. at the federal courthouse in Washington. Attorney General Janet Reno said last week that technical specifications of the system will be disclosed to a "group of experts." In an open letter, 27 House Republicans and one Democrat urged Reno last week to suspend use of Carnivore until the privacy issues it raised were resolved.

"People should feel secure that the federal government is not reading their e-mail, no matter how worthy the objective," House Republican leader Rep. Dick Armey of Texas and co-signers wrote. The FBI had no immediate comment on the emergency hearing. The Justice Department did not immediately respond to requests for comment on the move to compel release of "all records" on Carnivore. The American Civil Liberties has also filed a FOIA request for details on Carnivore, including the software code. The FBI has likened the system to a traditional wiretap in that both require a court finding of probable cause before surveillance may be undertaken.

At least three bills have been introduced in Congress that would clarify legal standards applying to interception of e-mail. David Sobel, general counsel of the Washington-based privacy center known by its acronym EPIC, said there was no substitute for a full and open public review of the Carnivore system. "Unless the public gets access to relevant information, we will not have a fully informed debate on these issues," he said in a telephone interview.

EPIC filed its initial FOIA request July 12. Six days later it asked the Justice Department to expedite the pending query on the ground that it had become a matter of exceptional news media concern raising questions about "the government's integrity which affect public confidence" -- one of the legal standards that qualifies a request for "expedited processing." Despite a 10-day statutory time limit to answer requests for accelerated processing, Sobel said the Justice Department failed to respond to EPIC's request. The 10 days ran out Friday, he said. "If there was ever a request that qualified for expedited treatment, this is it," Sobel added. Although Carnivore reportedly "sniffs" or scans all traffic at an Internet Service Provider once it is installed by court order, the FBI says only the data or messages relevant to a criminal investigation get stored and reviewed.

All other information it sifts through is discarded, Donald Kerr, director of the FBI lab that developed Carnivore, told Congress at a July 24 hearing. Some lawmakers suggested the tool might infringe on the Fourth Amendment to the Constitution, which protects Americans from unreasonable search and seizure.

Copyright 2000 [Reuters](#). All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.

'Carnivore' Eats Your Privacy

Wired News Report, 10:05 a.m. Jul. 11, 2000 PDT

Telecoms Miffed at FBI Meddling: U.S. to Track Crypto Trails

An FBI spokesman told the paper that the agency typically has about 20 Carnivore computers on hand to use when conducting Internet monitoring in compliance with court orders. But some critics say the practice of intercepting the network traffic of all users, even for a brief period of time, could run afoul of federal privacy laws and even the U.S. Constitution's prohibition on unreasonable searches and seizure. "It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring. You develop a tremendous amount of information," Mark Rasch, a former federal prosecutor, told the *Journal*.

Representative Bob Barr (R-Ga.), a conservative privacy advocate, said, "If there's one word I would use to describe this, it would be 'frightening.'" Not all Internet service providers seem to like the idea of a government computer silently recording their network traffic, especially since Carnivore systems are typically kept in locked boxes, and at least one company is challenging the practice in court. The FBI reportedly dubbed the system "Carnivore" because it has the ability to get at the "meat" of interesting or suspicious communications. The FBI says such automated monitoring is necessary to perform surveillance on packet-switched networks, and successfully persuaded Congress in 1994 to require telephone companies to make their digital networks readily snoopable. The bulk of legal wiretaps are used to investigate drug-related crimes, according to annual statistics published by the U.S. federal court system. FBI Director Louis Freeh has in the past pressed for limits on what encryption technology Americans may use, and the FBI last year unsuccessfully asked the Internet Engineering Task Force to build support for wiretaps into network protocols.