Clinton administration plan for FBI spying on email

Patrick Martin
2 August 2000

The Clinton administration announced July 17 that it would seek broad powers to compel Internet Service Providers to allow FBI monitoring of email messages, using a powerful software package devised by the police agency and given the ominous title of "Carnivore."

In its familiar style, the White House is packaging this reactionary plan as a "reform," presenting an expansion of wiretapping as an effort to set limits on the FBI and insure civil liberties. Chief of Staff John D. Podesta, in a speech to the National Press Club, declared, "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations."

Conflicting laws currently regulate police surveillance and interception of various modes of private communication in the United States. For example, telephone calls may only be wiretapped by the police with a court order, while there is no legal restriction on the interception of ordinary email. Communications routed over cable modems are effectively immune from interception, since police are required to obtain a court order after a judicial process in which the target of the surveillance has the right to challenge it.

These contradictions are a byproduct of the rapid development of communications technology. Email messages have little legal protection because until recently it was technologically impractical for the FBI to monitor them systematically. Carnivore was only developed in the last 18 months, as a modification of a software program typically used by Internet Service Providers (ISPs) known as a "packet sniffer." It sorts through the stream of data entering an ISP to find the senders and recipients of email to and from the target of surveillance.

Because Carnivore examines every email message handled through a given ISP, it closely resembles a form of telephone surveillance called a "trunk side" wiretap, in which the tap is placed, not on a particular phone, but in a telephone company switching center. Such wiretaps have been illegal in the United States for more than 30 years, since they give police access to all phone calls rather than those of a specific target. Under the Clinton administration plan, the email equivalent of such illegal wiretaps would now be permissible.

Opponents of the legislation have pointed out that there is no way to insure, once Carnivore is installed on an ISP, that the FBI would limit itself to monitoring the email of one targeted individual. The agency would be accountable only to itself. It has refused to release the source code for Carnivore, citing the proprietary interest of the companies which helped develop it, but also because, as one official said, "people might go to work on how to beat the system. We're not interested in getting into that race."

Barry Steinhardt, associate director of the American Civil Liberties Union, criticized the plan to install Carnivore, saying it "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic."

The Clinton administration's posture is that messages sent over the Internet should be treated in the same way as telephone calls. That is, monitoring ordinary email should require a court order (a restriction of police power), while monitoring email over cable lines should be made easier. But in practice, given the different character of email and telephone communication, the proposed measure amounts to a sweeping expansion of police powers.

For instance, current law gives police virtually

unlimited right to “transaction” surveillance of telephone calls. Telephone companies routinely hand over to the police, on request, logs of all calls made from a particular telephone and to whom. This power would now be extended by requiring ISPs to provide police the logs of email messages, when they were sent and to whom, as well as the record of web sites visited.

This power is a much more serious threat to political freedom than telephone logs, which reveal far less about the content of the communication being monitored. A list of web sites visited can tell a great deal about the political beliefs of someone targeted for police surveillance. Moreover, police cannot seek access to the content of phone calls when they learn of them after the fact from a log. Email messages, however, are recorded automatically by the Internet Service Provider. Accordingly, there will be intense pressure to divulge the content of messages once the police learn of their existence.

The email monitoring program would have worldwide implications, since it would apply to all communications that either begin or end in the United States. It would not apply to email messages transmitted entirely outside the country, but these could be monitored if they pass through an ISP based in the US—as do many email messages between European countries, for instance. The FBI recently objected to the takeover of a US-based Internet provider by the Nippon Telegraph & Telephone, citing “national security” considerations. According to one report, “the focus of the FBI's complaint is about preserving wiretap capabilities when an Internet service provider (ISP) is foreign-owned.”

The FBI is also pressuring makers of Internet equipment and software to insure that the next generation of Internet technologies have “wiretap-friendly” features. This amounts to an effort by the agency to assume powers that were specifically barred to it in the Communications Assistance to Law Enforcement Act of 1994, which excluded the Internet from federal police spying.

Congressional reaction to the White House plan was mixed, with most Democrats supporting it. Senator Patrick Leahy of Vermont cited the refusal of some ISPs to execute court orders for wiretapping, declaring, “If an ISP says it will not or cannot execute the order, what is the FBI supposed to do?” There was more opposition among congressional Republicans, citing either privacy considerations or concern that federal monitoring could be a prelude to other forms of regulation of the Internet, or taxation.

Neither party voiced any opposition to the widespread phenomenon of corporate spying on the email and Internet use of workers. An American Management Association survey released last month found that nearly three quarters of all companies conduct such monitoring actively, while one quarter have fired workers as a result.