CNET News
Politics and Law
February 3, 2010 4:00 AM PST

Police want backdoor to Web users' private data

by Declan McCullagh

Anyone with an e-mail account likely knows that police can peek inside it if they have a paper search warrant.

But cybercrime investigators are frustrated by the speed of traditional methods of faxing, mailing, or e-mailing companies these documents. They're pushing for the creation of a national Web interface linking police computers with those of Internet and e-mail providers so requests can be sent and received electronically.

CNET has reviewed a survey scheduled to be released at a federal task force meeting on Thursday, which says that law enforcement agencies are virtually unanimous in calling for such an interface to be created. Eighty-nine percent of police surveyed, it says, want to be able to "exchange legal process requests and responses to legal process" through an encrypted, police-only "nationwide computer network." (See **one excerpt** and **another**.)

The survey, according to two people with knowledge of the situation, is part of a broader push from law enforcement agencies to alter the ground rules of online investigations. Other components include renewed calls for laws **requiring Internet companies to store data** about their users for up to five years and increased pressure on companies to respond to police inquiries in hours instead of days.

But the most controversial element is probably the private Web interface, which raises novel security and privacy concerns, especially in the wake of a recent inspector general's **report (PDF)** from the Justice Department. The 289-page report **detailed** how the FBI obtained Americans' telephone records by citing nonexistent emergencies and simply asking for the data or writing phone numbers on a sticky note rather than following procedures required by law.

Some companies already have police-only Web interfaces. Sprint Nextel operates what it calls the L-Site, also known as the "legal compliance secure Web portal." The company even has offered a course that "will teach you how to create and track legal demands through L-site. Learn to navigate and securely download requested records." Cox Communications makes its **price list** for complying with police requests public; a 30-day wiretap is $3,500.

The police survey is not exactly unbiased: its author is Frank Kardasz, who is scheduled to present it at a **meeting (PDF)** of the Online Safety and Technology Working Group, organized by the U.S. Department of Commerce. Kardasz, a sergeant in the Phoenix police department and a project director of Arizona's **Internet Crimes Against Children** task force, said in an e-mail exchange on Tuesday that he is still revising the document and was unable to discuss it.

In an incendiary October 2009 essay, however, Kardasz wrote that Internet service providers that do not keep records long enough "are the unwitting facilitators of Internet crimes against children" and called for new laws to "mandate data preservation and reporting." He predicts that those companies will begin to face civil lawsuits because of their "lethargic investigative process."

"It sounds very dangerous," says Lee Tien, an attorney with the **Electronic Frontier Foundation**, referring to the police-only Web interface. "Let's assume you set this sort of thing up. What does that mean in terms of what the law enforcement officer be able to do? Would they be able to fish through transactional information for anyone? I don't understand how you create a system like this without it."

Kardasz's survey, based on questionnaires completed by 100 police investigators, says that 61 percent of them had their investigations harmed "because data was not retained" and only 40 percent were satisfied with the timeliness of responses from Internet providers.

It also says: "89 percent of investigators agreed that a nationwide computer network should be established for the purpose of linking ISPs with law enforcement agencies so that they may exchange legal process requests and responses to legal process. Authorized users would communicate through encrypted virtual private networks in order to maintain the security of the data."

Some of the responses to other questions: "AT&T is very prompt." "Cox Communications seems to be the worst." "Places like Yahoo can take a month for basic subscriber info which is also a problem." "AT&T Mobility does not keep a log at all." "MySpace give (sic) me the quickest response and they have been very pro-police."

Hemanshu (Hemu) Nigam, MySpace's chief security officer, said in an interview with CNET on Tuesday that: "You can be very supportive of law enforcement investigations and at the same time be very cognizant and supportive of the privacy rights of our users. Every time a legal process comes in, whether it's a subpoena or a search order, we do a legal review to make sure it's appropriate."

Nigam said that MySpace accepts law enforcement requests through e-mail, fax, and postal mail, and that it has a 24-hour operations center that tries to respond to requests soon after they've been reviewed to make sure state and federal laws are being followed. MySpace does not have a police-only Web interface, he said.

Creating a national police-only network would be problematic, Nigam said. "I wish I knew the number of local police agencies in the country, or even police officers in the country," he said. "Right there that would tell you how difficult it would be to implement, even though ideally it would be a good thing."

Another obstacle to creating a nation-wide Web interface for cops--one wag has dubbed it "DragNet," and another "Porknet"--is that some of its thousands of users could be infected by viruses and other malware. Once an infected computer is hooked up to the national network, it could leak confidential information about ongoing investigations.

Jim Harper, a policy analyst at the free-market **Cato Institute**, says that he welcomes the idea of a police-only Web interface as long as it's designed carefully. "A system like this should have strong logins, should require that the request be documented fully, and should produce statistical information so there can be strong oversight," he says. "I think that's a good thing to have."

Declan McCullagh is a contributor to CNET News and a correspondent for CBSNews.com who has covered the intersection of politics and technology for over a decade. Declan writes a regular feature called Taking Liberties, focused on individual and economic rights; you can bookmark his CBS News Taking Liberties site, or subscribe to the RSS feed. You can e-mail Declan at declan@cbsnews.com.