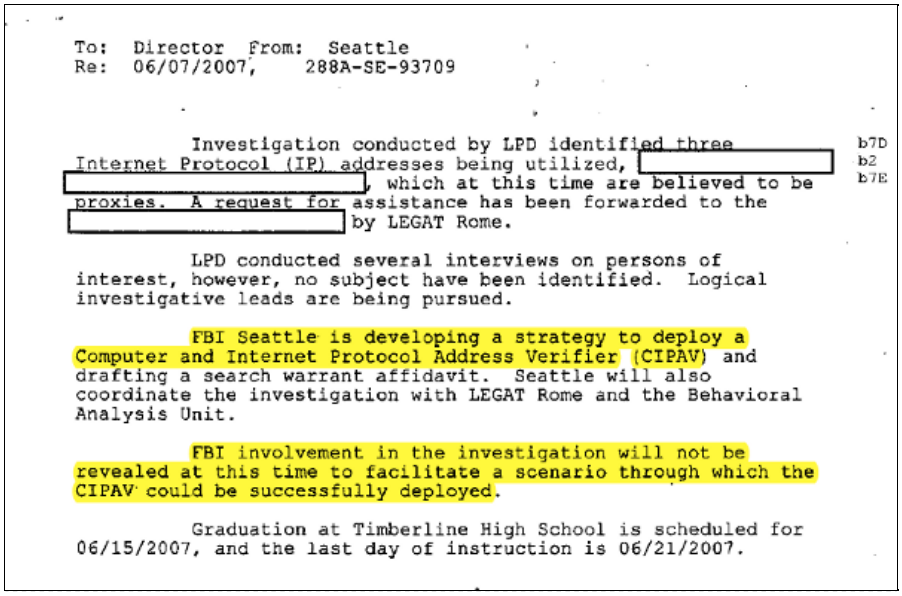
ELECTRONIC FRONTIER FOUNDATION

APRIL 29TH, 2011

New FBI Documents Provide Details on Government's Surveillance Spyware

Commentary by Jennifer Lynch

EFF recently received documents from the FBI that reveal details about the depth of the agency's electronic surveillance capabilities and call into question the FBI's controversial effort to push Congress to expand the Communications Assistance to Law Enforcement Act (CALEA) for greater access to communications data. The documents we received were sent to us in response to a Freedom of Information Act (FOIA) request we filed back in 2007 after Wired reported on evidence that the FBI was able to use "secret spyware" to track the source of e-mailed bomb threats against a Washington state high school. The documents discuss a tool called a "web bug" or a "Computer and Internet Protocol Address Verifier" (CIPAV),[1] which seems to have been in use since at least 2001.[2]



To: Director From: Seattle
Re: 06/07/2007, 288A-SE-93709

Investigation conducted by LPD identified three Internet Protocol (IP) addresses being utilized, [redacted], which at this time are believed to be proxies. A request for assistance has been forwarded to the [redacted] by LEGAT Rome. b7D b2 b7E

LPD conducted several interviews on persons of interest, however, no subject have been identified. Logical investigative leads are being pursued.

FBI Seattle is developing a strategy to deploy a Computer and Internet Protocol Address Verifier (CIPAV) and drafting a search warrant affidavit. Seattle will also coordinate the investigation with LEGAT Rome and the Behavioral Analysis Unit.

FBI involvement in the investigation will not be revealed at this time to facilitate a scenario through which the CIPAV could be successfully deployed.

Graduation at Timberline High School is scheduled for 06/15/2007, and the last day of instruction is 06/21/2007.

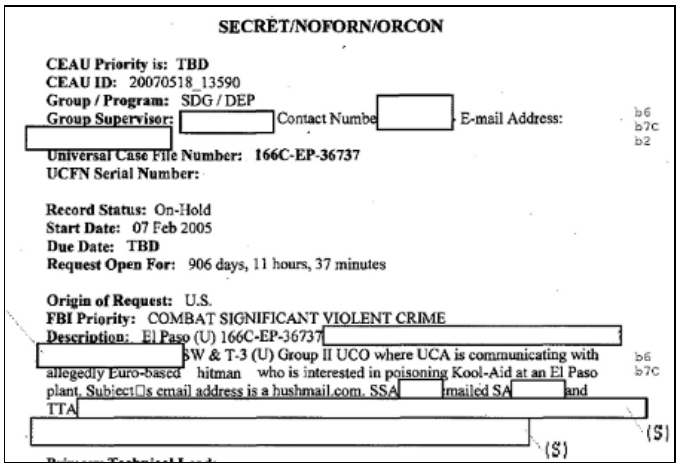
What is CIPAV and How Does It Work?
The documents discuss technology that, when installed on a target's computer, allows the FBI to collect the following information:

- IP Address
- Media Access Control (MAC) address
- "Browser environment variables"
- Open communication ports
- List of the programs running
- Operating system type, version, and serial number
- Browser type and version
- Language encoding
- The URL that the target computer was previously connected to
- Registered computer name
- Registered company name
- Currently logged in user name
- Other information that would assist with "identifying computer users, computer software installed, [and] computer hardware installed"[3]

It's not clear from the documents how the FBI deploys the spyware, though *Wired* has reported that, in the Washington state case, the FBI may have sent a URL via MySpace's internal messaging, pointing to code that would install the spyware by exploiting a vulnerability in the user's browser. Although the documents discuss some problems with installing the tool in some cases, other documents note that the

agency's Crypto Unit only needs 24-48 hours to prepare deployment.[4] And once the tool is deployed, "it stay[s] persistent on the compromised computer and . . . every time the computer connects to the Internet, [FBI] will capture the information associated with the PRTT [Pen Register/Trap & Trace Order].[5]

Where Has CIPAV Been Used and What Legal Process Does the FBI Rely On to Use It?



SECRET/NOFORN/ORCON

CEAU Priority is: TBD
CEAU ID: 20070518_13590
Group / Program: SDG / DEP
Group Supervisor: [redacted] Contact Numbe [redacted] E-mail Address: [redacted] b6 b7C b2
Universal Case File Number: 166C-EP-36737
UCFN Serial Number:

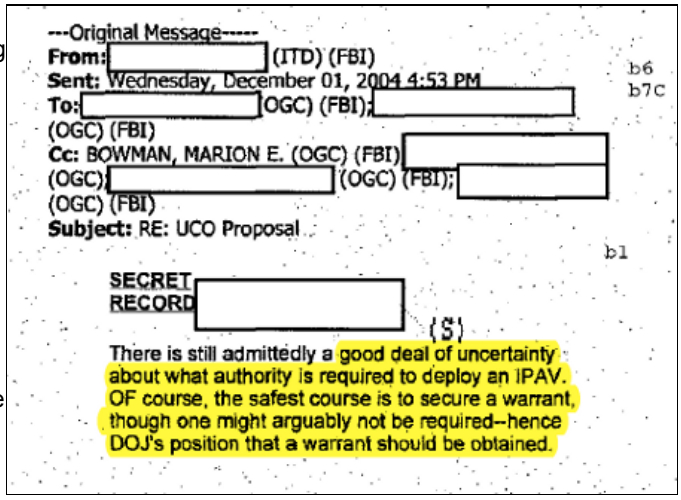
Record Status: On-Hold
Start Date: 07 Feb 2005
Due Date: TBD
Request Open For: 906 days, 11 hours, 37 minutes

Origin of Request: U.S.
FBI Priority: COMBAT SIGNIFICANT VIOLENT CRIME
Description: El Paso (U) 166C-EP-36737 [redacted]
[redacted] SW & T-3 (U) Group II UCO where UCA is communicating with [redacted] b6 b7C allegedly Euro-based hitman who is interested in poisoning Kool-Aid at an El Paso plant. Subject's email address is a hushmail.com. SSA [redacted] mailed SA [redacted] and TTA [redacted]
[redacted] (S)
(S)

It is clear from the documents we received that the FBI—and likely other federal agencies—have used this tool a lot. According the documents, the FBI has used CIPAV in cases across the country—from Denver, El Paso, and Honolulu in 2005; to Philadelphia, California, and Houston in 2006; to Cincinnati and Miami in 2007. In fact, one stack of documents we received consists entirely of requests from FBI offices around the country to the agency's Cryptologic and Electronic Analysis Unit ("CEAU") for help installing the device.[6]

The FBI has been using the tool in domestic criminal investigations as well as in FISA cases,[7] and the FISA Court appears to have questioned the propriety of the tool.[8] Other agencies, and even other countries have shown interest in the tool, indicating its effectiveness. Emails from 2006 discuss interest from the Air Force,[9] the Naval Criminal Investigative Service[10] and the Joint Task Force-Global Network Operations,[11] while another email from 2007 discusses interest from the German government.[12]

The FBI's Crypto Unit appears to have viewed the CIPAV as a proprietary tool. In one email, an agent grumbled, "we are seeing indications that [CIPAV] is being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression without any countervailing benefit)."[13] In another email, an agent stated, "[I] am weary [sic] to just hand over our tools to another Gov't agency without any oversight or protection for our tool/technique."[14] And a third email noted, "[w]e never discuss how we collect the [data CIPAV can collect] in the warrants/affidavits or with case agents. AUSAs, squad supervisors, outside agencies, etc."[15]



---Original Message-----
From: [redacted] (ITD) (FBI)
Sent: Wednesday, December 01, 2004 4:53 PM
To: [redacted] OGC) (FBI); [redacted]
(OGC) (FBI)
Cc: BOWMAN, MARION E. (OGC) (FBI) [redacted]
(OGC) [redacted] (OGC) (FBI); [redacted]
(OGC) (FBI)
Subject: RE: UCO Proposal

b6 b7C b1

SECRET
RECORD [redacted]
(S)

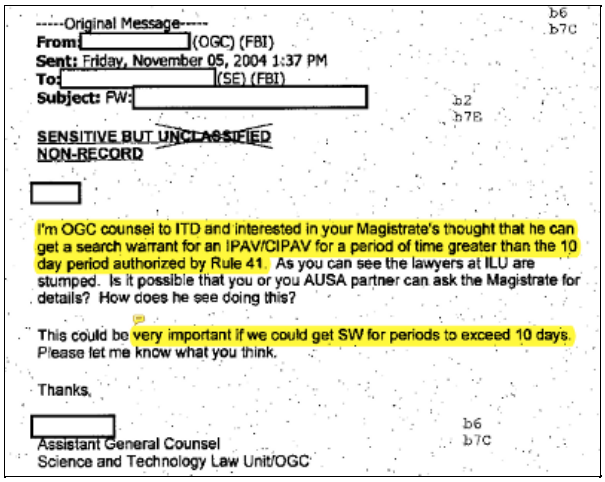
There is still admittedly a good deal of uncertainty about what authority is required to deploy an IPAV. OF course, the safest course is to secure a warrant, though one might arguably not be required--hence DOJ's position that a warrant should be obtained.

It appears from the documents that the FBI wasn't sure what legal process to seek to authorize use of the spyware device. Some emails discuss trying to use a "trespasser exception" to get around a warrant,[16] while others discuss telling the AUSA (government attorney) to cite to the "All Writs Act, 28 U.S.C. § 1651(a)."[17] And one email suggests some agents thought the tool required no legal process at all. In that email, the FBI employee notes he considers the tool to be "*consensual monitoring without need for process*; in my mind, no different than sitting in a chat room and tracking participants' on/off times; or for that matter sitting on P2P networks and finding out who is offering KP."[18]

Eventually, the FBI seems to have sought a legal opinion on the proper use of the tool, both from the Office of General Counsel and from the National Security Law Branch,[19] and ultimately, the agency seems to have settled on a "two-step request" process for CIPAV deployments -- a search warrant to authorize intrusion into the computer, and then a subsequent Pen/Trap order to authorize the surveillance done by the spyware.[20]

What Does This Mean for the FBI's Push for New Back Doors into Our Internet Communications?

Over the past few months, we've heard a lot from the FBI about its need to expand the Communications Assistance to Law Enforcement Act (CALEA), a law that that requires all telecommunications and broadband providers to be technically capable of complying with an intercept order. Federal law enforcement officials have argued that under current regulations they can't get the information they need and want to expand CALEA to apply to communications systems like Gmail, Skype, and Facebook. However, these documents show the FBI already has numerous tools available to surveil suspects directly, rather than through each of their communications service providers. One heavily redacted email notes that the FBI has other tools that "provide the functionality of the CIPAV [text redacted] as well as provide other useful info that could help further the case."[21] Another email notes that CIPAVs are used in conjunction with email intercepts, perhaps using similar spyware-type tools.[22] If the FBI already has endpoint surveillance-based tools for internet wiretapping, it casts serious doubt on law enforcement's claims of "going dark."



-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, November 05, 2004 1:37 PM
To: [redacted] (SE) (FBI)
Subject: FW: [redacted]

b6 b7C b2 b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I'm OGC counsel to ITD and interested in your Magistrate's thought that he can get a search warrant for an IPAV/CIPAV for a period of time greater than the 10 day period authorized by Rule 41. As you can see the lawyers at ILU are stumped. Is it possible that you or you AUSA partner can ask the Magistrate for details? How does he see doing this?

This could be very important if we could get SW for periods to exceed 10 days. Please let me know what you think.

Thanks,

[redacted]
Assistant General Counsel
Science and Technology Law Unit/OGC

b6 b7C

A device that remains "persistent" on a "compromised computer" is certainly concerning. However, if the FBI obtains a probable cause-based court order before installing tools like CIPAV, complies with the minimization requirements in federal wiretapping law by limiting the time and scope of surveillance, and removes the device once surveillance concludes, the use of these types of targeted tools for Internet surveillance would be a much more narrowly tailored solution to the FBI's purported problems than the proposal to undermine every Internet user's privacy and security by expanding CALEA. We will continue to report on both the FBI's use of endpoint surveillance tools and on the agency's push to expand CALEA as more documents come in.

Click here to access full pdf versions of the documents we received or see below for the pages referenced in this post.

---

1. FBI_CIPAV_01 p.26
2. FBI_CIPAV_09 p.3
3. FBI_CIPAV_07 pp.10-11
4. FBI_CIPAV_07 p.50
5. FBI_CIPAV_08 p.67
6. FBI_CIPAV_10
7. FBI_CIPAV_07 p. 45, FBI_CIPAV_08 p.132, 143
8. FBI_CIPAV_14 p.52
9. FBI_CIPAV_08 p.20
10. FBI_CIPAV_09 p.21-22
11. *Id.*
12. FBI_CIPAV_08 p.9
13. FBI_CIPAV_05 p.1
14. FBI_CIPAV 09 p.21
15. FBI_CIPAV_07 pp.11
16. FBI_CIPAV_08 p.29
17. FBI_CIPAV_08 p.149
18. FBI_CIPAV_14 p.36."KP" is likely a reference to "kiddie porn."
19. FBI_CIPAV_14 p.42, 62
20. FBI_CIPAV_08 p.169
21. FBI_CIPAV_08 p.168
22. FBI_CIPAV_08 p.143

Related Issues: *CALEA*, *FOIA Litigation for Accountable Government*, *Pen Trap*, *Privacy*, *Transparency*

Related Cases: *FOIA: Endpoint Surveillance Tools (CIPAV)*, *FOIA: Expanding CALEA and Electronic Surveillance Laws*

[Permalink: http://www.eff.org/deeplinks/2011/04/CIPAV_Post]

Want to learn how you can defend free speech, stand up for privacy, fight for government transparency, support consumer rights, and protect your right to innovation in the digital world? Visit **http://eff.org/fight** to find ways to help.