Recent Case Report

U.S. v. Forrester

(9th Cir. 2007) __ F.3d __ [2007 WL 2120271]

ISSUE

If officers want to monitor a suspect's email and internet activity, can they utilize the expeditious pen register procedure?

FACTS

Federal agents in Southern California suspected that Forrester and Alba were manufacturing large quantities of ecstasy. In the course of their investigation, they obtained a court order requiring Alba's internet service provider, PacBell, to install a "mirror port," which is a pen register analogue that disclosed the email addresses of people with whom Alba corresponded via email, and the addresses of the websites he visited. Some of this information was used to obtain a search warrant that resulted in the seizure of incriminating evidence. Based in part on this evidence, both men were convicted.

DISCUSSION

Forrester and Alba contended that the evidence should have been suppressed because the information about their email and internet activity was obtained unlawfully. Specifically, they argued that the judge who issued the order lacked the authority to do so. The court disagreed.

The court order in this case was issued in 2001 when federal law did not specify a procedure for obtaining email and internet addresses. So the officers had to improvise. It appears they concluded that the undemanding pen register procedure should suffice because the information they were seeking was not significantly different from the phone numbers they could obtain by means of a pen register.[1] In any event, they applied for pen register authorization, and the judge signed the order.

By way of background, a pen register is a device that records the phone numbers dialed from a suspect's phone. Another device, known as a "phone trap" or "trap and trace" device, records the phone numbers of the people who placed calls *to* the suspect.

In recent years, there have been some changes in the technology and law pertaining to pen registers and phone traps. First, as the result of computerization, phone companies

[1] **NOTE**: A court order for the installation and monitoring of pen registers does not require probable cause. Instead, it may be issued if the declarant states that the phone numbers that are likely to be obtained are "relevant to an ongoing criminal investigation." See 18 USC § 3122(b)(2); *Brown* v. *Waddell* (4th Cir. 1995) 50 F.3d 285, 290.

have largely replaced these hardware devices with software applications. And because the software used to monitor dialed numbers is essentially the same as the software used to monitor incoming numbers, the distinction between pen registers and phone traps has become technologically insignificant.

Second, as the result of changes to the federal law in 2001, email and internet addresses are now treated the same as the telephone numbers that can be obtained by means of pen registers. This was because the Patriot Act expanded the definition of "pen register" to include devices and applications that record email and internet activity.[2] Thus, if the court order that was issued in *Forrester* had been issued today, it would have been unquestionably valid.

It is important to understand that the information that can be obtained via the pen register statute is limited to non-communicative records and data; e.g., dates, times, telephone numbers, email and internet addresses. An entirely different—and much more demanding—procedure must be followed to obtain "content," such as the spoken or written words of an email message (including the "subject" line), and a numeric message transmitted to a pager.[3]

Back to *Forrester*. As noted, the issue was whether the laws governing the installation and monitoring of pen registers prior to 2001 could also authorize the monitoring of Forrester's email and internet activity. The court ruled they could for two reasons. First, this type of information is "constitutionally indistinguishable" from the information provided by pen registers; and the United States Supreme Court ruled in *Smith* v. *Maryland*[4] that dialed phone numbers are not private under the Fourth Amendment because they are in the hands of a third party (i.e., phone companies) over whom the suspect has no control.

Thus, the court in *Forrester* reasoned that email and internet addresses are not private either because they, too, are in the hands of a third party; i.e., internet service providers. Said the court:

> [E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are

---

[2] **NOTE**: 18 USC §§ 3127(3) and 3127(4) expanded the definitions of pen registers and phone traps to include devices and processes that record or decode "routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"; i.e., the definitions are no longer limited to devices and applications that record telephone numbers.

[3] **NOTE: "Content" defined**: See 18 USC § 2510(8) ["[W]hen used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."]. ALSO SEE *People* v. *Pons* (1986) 509 N.Y.S. 2d 450, 453 ["The monitoring of [a] telephone pager device is more intrusive than the use of a pen register. The pager device is capable of conveying substantive information by combining digits in various sequences. Both telephone numbers and coded messages may be conveyed."]; *Jessup-Morgan* v. *AOL* (E.D.Mich. 1998) 20 F.Supp.2d 1105, 1108 ["The 'content' of a communication is not at issue in this case. Disclosure of information identifying an AOL electronic communication account customer is at issue."]; *In re application of the USA for an order authorizing the use of a cellular telephone digital analyzer* (C.D.Cal. 1995) 885 F.Supp. 197, 199 [a cell phone's ESN, its own number, or the numbers being called by the cellular telephone are not "content"].

[4] (1979) 442 U.S. 735.

accessed through the equipment of their Internet service provider and other third parties.

Second, email and internet addresses do not constitute "content." As the court observed, "[W]hen the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or the particular pages on the websites the person viewed."

Accordingly, the court ruled that the surveillance of Alba's email and internet activity "did not constitute a Fourth Amendment search and was not unconstitutional."

COMMENT

Forrester is the first case in which a federal court has ruled that internet subscribers cannot reasonably expect that their to/from email addresses and the addresses of the websites they visit will be private under the Fourth Amendment. Still, internet service providers will probably not furnish such information without court authorization because of civil liability concerns. Consequently, a court order will be required. To view and obtain forms that can be used for this purpose, visit Point of View Online (www.acgov.org/da) and click on "Forms and Publications." POV