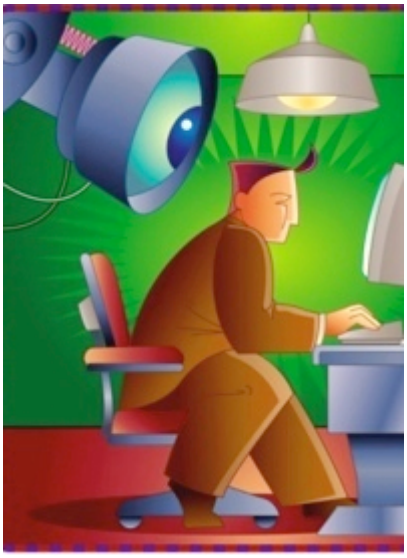
Court Rules Judges May Require Warrants for Cellphone Records



The U.S. Court of Appeals for the Third Circuit, seated in Philadelphia, ruled on September 14 that under the provisions of the Stored Communications Act (SCA), government agencies may compel communication services such as cellphone or computer services to provide consumer information, but only under controlled conditions, which may include warrants or court order.

In the ruling of the court:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity —
>
> > (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
> > (B) obtains a court order for such disclosure under subsection (d) of this section;
> > (C) has the consent of the subscriber or customer to such disclosure;
> > (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title).

The ruling (downloadable PDF) was delivered in response to an appeal from the United States District Court for the Western District of Pennsylvania filed by the United States Department of Justice Office of Enforcement Operations in Washington, D.C. (referred to as the "Government" in the ruling).

According to the language of the ruling, "The United States ('Government') applied for a court order pursuant to a provision of the Stored Communications Act, 18 U.S.C. § 2703(d), to compel an unnamed cell phone provider to produce a customer's 'historical cellular tower data,' also known as cell site location information or 'CSLI.'"

Basically, therefore, the government wanted to know a cellphone customer's general whereabouts determined by which cellphone tower his signal had been bounced off.

However, the Western Pennsylvania judge had denied the government's application, writing (in the words of the appellate court ruling) "an extensive opinion that rejected the Government's analysis of the

statutory language, the legislative history, and the Government's rationale for its request."

Whereupon "the government" appealed the ruling to the District Court in Philadelphia. The court (again in the court's own language) received "amici [friend of the court] briefs in support of affirmance of the District Court from a group led by the Electronic Frontier Foundation and joined by the American Civil Liberties Union, the ACLU-Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology (hereafter jointly referred to as "EFF") and from Susan A. Freiwald, a law professor who teaches and writes in the area of cyberspace law and privacy law."

In its ruling, the appellate court noted: "The growth of electronic communications has stimulated Congress to enact statutes that provide both access to information heretofore unavailable for law enforcement purposes and, at the same time, protect users of such communication services from intrusion that Congress deems unwarranted."

In turning down "the government's" appeal, the appellate court noted, in part: "In submitting its request to the [judge] in this case, the Government did not obtain either a warrant … or a subpoena …, nor did it secure the consent of the subscriber…. Instead it sought a court order."

Expanding on the final phrase, the appellate court defined the "requirements for a court" that a government entity must seek in order to obtain communications records.

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity*offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.* [Emphasis in original.]

A writer for*Computerworld* Kevin Bankston, in a September 9 article, quoted an attorney with the Electronic Frontier Foundation, an advocacy group that had filed an amicus brief in the case:

> "The SCA allows the government to obtain cell location data without a warrant. This ruling holds that under the statutes, courts have the discretion to instead require the government to show probable cause and get a warrant [when needed]."

"This decision gives the front-line judges new tools to exercise oversight and to raise the bar when the government seeks cell phone location data," Bankston said.

An summary of the ruling in the *Philadelphia Inquirer* said:

> A federal appeals court in Philadelphia ruled Tuesday that the government may need a warrant when trying to obtain phone records that show a person's location.

It was not a clear victory for privacy advocates, but it kept open a door that law enforcement had wanted to slam shut.

The *Inquirer* also noted that the government wanted to obtain the phone records if they were "relevant and material to an ongoing investigation." However, U.S. Magistrate Judge Lisa Pupo Lenihan rejected the government's request and insisted that a warrant was needed.

The appellate opinion, written by Judge Delores K. Sloviter, noted that Lenihan had an "impressive level of support" in the Western District of Pennsylvania from other magistrate judges who routinely issue warrants and that a U.S. district judge also sided with Lenihan, and the government appealed to the Third Circuit.

While most media reports about the ruling defined it as a shot across the bow of over-zealous government agencies that have attempted to circumvent the Fourth Amendment's privacy standards — and therefore, a partial victory for civil libertarians — at least one media account viewed the decision as a glass that was not half full, but half empty.

A report from CNET News' "PrivacyInc" was headlined "Court allows warrantless cell location tracking" and reported: "A three-judge panel of the Third Circuit said (PDF) tracking cell phones 'does not require the traditional probable-cause determination' enshrined in the Fourth Amendment, which prohibits government agencies from conducting 'unreasonable' searches."

Referring to Judge Lenihan's earlier ruling that the government had appealed, CNET News reported: "Lenihan had required the Justice Department to demonstrate 'probable cause,' a standard used in search warrants. But the three-judge panel rejected that idea, saying Lenihan 'erred' and the relevant requirement is a 'lesser one than probable cause' that is less privacy-protective."

The government's ability to monitor cellphone usage poses a threat beyond the mere invasion of privacy, however. There were reports during the early stages of the U.S. invasion of Iraq in 1993 that the U.S. military had used cellphone signals emanating from a unique model phone used by Saddam Hussein's elite inner circle to direct smart bombs against specific targets.

The language of the Fourth Amendment, as with the other amendments comprising the Bill of Rights, was not designed to shield criminals. The memory of the loss of rights existing among free Englishmen since the days of the Magna Carta under the British occupation of the American colonies was fresh in the minds of our Founding Fathers.

From their experience, free citizens had learned to fear oppressive government more than a few wayward criminals. And if things became too bad, the right to keep and bear arms, enshrined in the Second Amendment, could be used by free men to defend themselves against both threats.