Consumers vulnerable to phone data theft

January 16 2006

The political site AMERICAblog announced Thursday that for only $89.95 it had purchased the cell-phone records of 100 calls over three days in November 2005 made or received by former presidential candidate General Wesley Clark.

Blog publisher John Aravosis wrote he had bought Clark's phone records from the Web site Celltolls.com and his own from Locatecell.com for $110 to address failed privacy protections.

The blog's actions came after the Chicago Sun-Times published a Jan. 5 article by reporter Frank Main in which the paper conducted a similar investigation. The story followed after the FBI informed law enforcement nationwide including the Chicago Police Department, warning officers' phone records may be purchased online, according to Main's article.

While no legislation is in place, dozens of online companies selling phone records exist, where buyers could purchase phone records with a credit card and a cell-phone number.

According to the blog, the attempted purchasing of other cell-phone records included ABC's George Stephanopoulos, the Washington Post's Dana Milbank and the New York Time's Adam Nagourney; however, Locatecell was unable to provide those records.

"The only question now remaining is why President Bush, our leaders in Congress, and our wireless phone companies (at the very least T-Mobile

and Cingular, whose customers' records are available online to anyone) have known about this problem for at least six months but have yet to fix it," according to the AMERICAblog post.

T-Mobile said in a statement, "We are not affiliated with any party that sells call records, we do not sell call records, and anyone that purports to offer this service is engaging in an unlawful activity."

The company, which says it supports pending legislation to ban and criminalize the sale of phone records, has taken safeguarding its customers' privacy seriously by encouraging customers to utilize a security password as an additional layer of security on their account.

Cingular spokesman Mark Siegel says the company is aware of the problem and has taken safeguards to protect customers like others in the industry. Cingular's wireless service only gives out records in two circumstances: owners of the account and law enforcement, he said.

"This is something we take seriously," he said. "No one is entitled to those records under false pretenses."

As Siegel explains, there are already several safeguards in place against unauthorized access, as well as technical safeguards and a center that specifically deals with law-enforcement officials obtaining records through subpoenas or court orders.

Last year both Verizon Wireless and Cingular Wireless sued online data-broker sites.

"We are suing these data brokers who could potentially danger our customer's privacy," Siegel said. "We would be supportive of legislative that criminalizes this activity."

And in a statement Friday, Cingular announced it had obtained a temporary restraining order from the U.S. District Court in Atlanta against Data Find Solutions Inc. and 1st Source Information Specialists Inc. after filing a civil lawsuit alleging these companies unlawfully obtained and disseminated Cingular customer records by posing as customers seeking information about their own accounts.

Cingular believes Data Find Solutions "previously owned and operated several Web sites that advertise the sale of phone records, including locatecell.com and celltolls.com, and that 1st Source Information Specialists, Inc. currently owns and operates these Web sites."

However, criminalizing and suing these online data brokers are not enough, says Chris Hoofnagle, senior counsel to the public interest research center Electronic Privacy Information Center.

Bellsouth, Verizon, Verizon Wireless, SBC and the CTIA are in favor of enforcement actions but are against heighten security, according to the EPIC.

In fact, the EPIC filed a petition with the Federal Communications Commission for heighten security safeguards to protect phone records last year, only filing a complaint with the Federal Trade Commission to investigate data broker companies a month before.

"It's identity theft," Hoofnagle said. Instead, his organization would require telephone carriers to enhance security measures when releasing records since many times they only require the billing address and one other piece of information.

For example, Hoofnagle suggests that phone companies could send a customer's cell phone a text message notifying that their records are being released and to contact them immediately if that was wrong.

According to the EPIC, data brokers can get ahold of records in three ways: The most prevalent is pretexting, in which a person impersonates an account holder through gaining access to "commercial data broker" services that will allow them to obtain everything from Social Security numbers to date of birth. Records can also be accessed by hacking into online account administration tools and using insider information.

Hoofnagle also emphasizes the issue's importance since the privacy concerns include personal information stolen from screen names or dating services.