Washington Post

July 8, 2005 Friday

Online Data Gets Personal: Cell Phone Records for Sale

By Jonathan Krim, Washington Post Staff Writer

They're not just after your credit card or Social Security numbers.

Fueled by the ease of online commerce, snoops are on the trail of other personal information, too. One of the hottest markets: records of phone calls, especially from cell phones.

A tool long used by law enforcement and private investigators to help locate criminals or debt-skippers, phone records are a part of the sea of personal data routinely bought and sold online in an Internet-driven, I-can-find-out-anything-about-you world. Legal experts say many of the methods for acquiring such information are illegal, but they receive scant attention from authorities.

Think your mate is cheating? For $110, Locatecell.com will provide you with the outgoing calls from his or her cell phone for the last billing cycle, up to 100 calls. All you need to supply is the name, address and the number for the phone you want to trace. Order online, and get results within hours.

Carlos F. Anderson, a licensed private investigator in Florida, offers a similar service for $165, for all major telephone carriers.

"This report provides all the calls with dates, times, and duration on the billing statement," according to Anderson's Web site, which adds, "Incoming Calls and Call Location are provided if available."

Learning who someone talked to on the phone cannot enable the kind of financial fraud made easier when a Social Security or credit card number is purloined. Instead, privacy advocates say, the intrusion is more personal.

"This is a person's associations," said Daniel J. Solove, a George Washington University Law School professor who specializes in privacy issues. "Who their physicians are, are they seeing a psychiatrist, companies they do business with . . . it's a real wealth of data to find out the people that a person interacts with."

Such records could be used by criminals, such as stalkers or abusive spouses trying to find victims.

Unlike Social Security numbers, which are on many public documents that have been scooped up for years by data brokers, the only repository of telephone call records is the phone companies.

Wireless carriers say they are aware that unauthorized people seek to get their customers' call records and sell them, but the companies say they take steps to prevent it.

"There are probably 100 such sites" known to security officials at Verizon Wireless that offer to sell phone records, said Jeffrey Nelson, a company spokesman, who said Verizon is always trying to respond to abusive practices. He said that the company views all such activity as illegal and that "we have historically, and will continue to, change policies to reflect the changing nature of criminal activity," though he declined to be specific.

Mark Siegel, a spokesman for Cingular Wireless, said his company constantly is on guard against people trying to get at customer information. But he called the acquisition of call records "an infinitesimally small problem" at his firm.

Some experts in the field aren't so sure.

"Information security by carriers to protect customer records is practically nonexistent and is routinely defeated," said Robert Douglas, a former private investigator and now a privacy consultant who has tracked the issue for several years.

Experts say data brokers and private investigators who offer cell phone records for sale probably get them using one of three techniques.

They might have someone on the inside at the carrier who sells the data. Spokesmen for the telephone companies said strict rules prohibiting such activity make this unlikely. But Joel Winston, associate director of the Federal Trade Commission's Financial Practices Division, said other types of data-theft investigations have shown that "finding someone on the inside to bribe is not that difficult."

Another method is "pretexting," in which the data broker or investigator pretends to be the cell phone account holder and persuades the carrier's employees to release the information. The availability of Social Security numbers makes it easier to convince a customer service agent that the caller is the account holder.

Finally, someone seeking call data can try to get access to consumer accounts online.

Telephone companies, like other service firms, are encouraging their customers to manage their accounts over the Internet. Typically, the online capability is set up in advance, waiting to be activated by the customer. But many customers never do.

If the person seeking the records can figure out how to activate online account management in the name of a real customer before that customer does, the call records are there for the taking.

Federal law expressly prohibits pretexting for financial data – which at one time was a primary means of stealing credit card and other account information – but does not cover telephone records, which are covered by a patchwork of state and federal laws governing access to personal information.

Some privacy advocates argue that the federal pretexting law needs to be broadened.

At the very least, "there need to be audit trails to detect employee access to this personal information and a data retention schedule that mandates deletion of records" after a certain period of time, said Chris Jay Hoofnagle, West Coast director of the Electronic Privacy Information Center.

The center filed a complaint with the Federal Trade Commission yesterday against one data broker, Intelligent e-Commerce Inc. of Encinitas, Calif., saying it misrepresented its right to obtain the information. The firm, which operates the Web site www.bestpeoplesearch.com, advertises a variety of personal data for sale, including cell phone records.

The company, which says on its Web site that it uses a licensed private investigator to get the information, said through its lawyer that it seeks to comply with all local, state and federal laws. Attorney Larry Slade said he does not know how the company acquires the phone records.

Phone companies view all these tactics as illegal, even if they are used to help track down criminal activity. Instead, carriers say, they require court orders before releasing customer records.

If someone uses pretexting to gain access to records, "these people are acting criminally, posing as someone they are not," Nelson said. He added that Verizon is preparing legal action against one data provider.

The FTC views pretexting as a deceptive practice even without a specific ban on its use for telephone records, Winston said.

But he said the agency has never taken such a case to court and does not know how widespread the problem is. He said the FTC must focus its resources on the practices of data thieves that can cause the most damage to large numbers of consumers, such as financial fraud.

Many of the vendors of call records are unregulated data brokers, such as Data Find Solutions Inc. of Knoxville, Tenn., which operates Locatecell.com. Company officials did not return calls seeking comment.

At the Florida office of private investigator Anderson, a man who answered the phone and identified himself only as Mike said, "I don't really think we're going to reveal our sources" of phone records. "There's a lot of ways of doing it."

At Reliatrace Locate Services of Wisconsin, a man who declined to give his name said only that his firm buys the data from another firm.

There is active debate within the private investigator community about the propriety of getting phone records. In at least one online discussion group for the industry, some members defended the practice as legitimate while others said it was illegal, according to transcripts provided to The Washington Post.

“I do not know of any legal way to obtain a person’s telephonic history,” Robert Townsend, head of the National Association of Legal Investigators, said in an interview. Townsend added that he thinks only a small minority of licensed investigators engage in the practice of acquiring and selling the data.