Not so undercover: what US$29.95 can buy

By Rashunda Tramble for ISN Security Watch (16/3/06)

Imagine you are an undercover operative working for your government. You believe that your real identity, your family, and your entire life are protected by your employer.

Now imagine opening up a major national newspaper and finding out that your cover can be blown for less than dinner for two.

This week's Chicago Tribune report on the availability of information about covert CIA operatives on the internet set off alarm bells in the US administration.

The Tribune story, published on Sunday, outlined its search of a commercial online data service. Through that service, the Tribune found information for internal agency numbers, supposed secret locations, and over 2,600 employees. An undisclosed number of the employees on the list were working covertly.

In one instance, the newspaper found out an operative's name, age, marital status, where the person grew up, and her current address.

It even discovered how many bedrooms her house had.

The paper also uncovered that one of the operatives facing charges in Italy for kidnapping a Muslim cleric in Milan had a criminal background in the US.

Also found: the names of operatives working in US embassies in Europe.

Included in the investigation was information about what is reportedly the CIA's training facility at Camp Peary, Virginia, which is also known as "The Farm". The US government has never acknowledged its existence.

As a test, a reporter entered "Camp Peary" into the search engine Google and found hundreds of entries. They included a newspaper article from 1994 about expansion plans at the facility, information about a landing strip, and a reference to a movie starring Al Pacino and Colin Farrell.

The Tribune did not disclose any names or exactly which service they used to find the information in the article itself, but did say that the all of it came from public records. Tax records, legal judgments, real estate transactions, and the like, were used.

Most of the details were purchased through a fee-based data mining service, not a free one such as Google or Yahoo. Services such as these are one-stop clearinghouses for private information, information that one would normally have to pore through thousands of records to find.

LexisNexis and ChoicePoint are examples of services that may have been used by the newspaper.

A basic background check on ChoicePoint costs US$25.95.

So theoretically, the information the Tribune found is not freely available online. Even with that, the fact that personal details of CIA employees and facilities could be found, especially so easily and at such a low price, reportedly alarmed the agency's director, Porter Goss.

A spokesperson for the CIA was quoted as saying that "cover is a complex issue that is more complex in the internet age".

“There are things that worked previously that no longer work,” chief spokesperson Jennifer Dyck told the paper.

When the Tribune asked a senior official how such potentially damaging details could be that easy to find, the official had no explanation. However, he did say it was the covert person’s responsibility to keep their details private.

“If someone filled out a credit report and put that down, that’s just stupid,” the paper quoted the official as saying.

Perhaps he was referring to when work colleagues of the Milan operative involved the cleric kidnapping case registered at hotels under their true names.

Private data is not private

Gary Chapman, associate director of the Telecommunications and Information Policy Institute at the University of Texas and a former Green Beret, told ISN Security Watch there were quite a few fee-based services around that compile information “that most people regard as a violation of privacy”.

“Revealing information about CIA covert operatives would seem to be an egregious and disturbing violation of information confidentiality, but there are almost innumerable other examples that the public might find equally shocking,” he said.

According to Chapman, it is one thing to find government information on the internet or on a paid search service. It is another to find that your information is ripe for the picking.

“Some people can use data aggregation to find out all kinds of things about someone else, such as their credit information, where their house is, how much they're worth, their sexual preference, their former employers. Unleashing a skilled data sleuth on the identity of someone will often produce pages and pages and pages of information, which is usually shocking to anyone who doesn’t quite understand what’s possible these days.”

Fred Baker, chairman of the board of trustees for the Internet Society and former chairman of the Internet Engineering Task Force, says the internet is not responsible for the exposure.

Baker compares the situation to the inner workings of a house. “One might just as easily say that the plumbing system of a house or city is at fault if fluorine is found in someone’s home,” he told ISN Security Watch.

“The fluorine was probably carried in water through the plumbing system, but the fact that it is or isn’t there is not because there was plumbing, but either because someone put it there or something went wrong.”

Baker said the internet was neither the leak nor the threat.

“The internet is the plumbing that carries information around. The threat, to the extent that there is one, is from the people who intentionally or otherwise publish information, and from other people who go looking for it.”

When asked if he thought the Tribune should not have published the report, Baker said the CIA could assume that intelligence services who were interested in the information probably already had it in their hands.

But that is not to say that the report could not have serious repercussions.

The effect on national security

He said that when commenting on the issue of privacy, “liberal activists” state that just because the tapping or the observing could be done, does not mean it should be done.

Take the issue of lawful interception, or wiretapping, for example. The Bush administration came under fire recently for eavesdropping on communications made to and from the US to suspected al-Qaida sympathizers overseas.

Pertaining to the CIA case, according to Baker, the Tribune should be held up to the same standard; just because the newspaper could search for the information does not mean it should have.

He said the newspaper could have turned over what they found to the CIA. If the Tribune had just done the investigation and, when they realized what they had, given the data to the CIA without publishing it, they would have done those searching for terrorists such as Osama bin Laden a service.

“So doing the analysis isn’t bad, it is doing it and then using it in a manner that compromises people who daily put their lives on the line in the defense of people like the reporters at the Chicago Tribune that is problematic.”

Baker doubted that anything of value has been gained by publishing the report and “could imagine lives being lost as a result”.

But will the revelations really have an effect on national security?

Chapman says the question is difficult to answer because of the host of problems the US is having in terms of national security right now.

“If a particular covert operation were revealed because of information available online, would this have a more deleterious impact on national security than what we’ve done and continue to do in Iraq, which is obviously reported in the general press every day?” he said.

“If we were revealed to be conducting covert operations in Iran, would this surprise anyone?”

Chapman said public knowledge of covert information may be damaging to the people directly involved. He referred to an example documented in the book Masters of Chaos by Linda Robinson. Retired General Wesley Clark, who during a CNN broadcast at the start of the Iraq war in 2003, said that if he were Saddam Hussein, he would block a particular route into Baghdad.

The general said this at the exact time US Special Forces troops were entering that area.

“But do such mistakes or revelations damage national security? Doubtful.” Chapman added: “We’re not in a Cold War with a military equal or competitor, like in the days of the Soviet Union. Terrorists have little or nothing in their arsenal that can damage US national security.”

The big picture

The former Green Beret said he did not believe that the information available online about CIA activities was trivial, but suggested that the situation be put into perspective.

“Over 2,000 American soldiers have died in Iraq and thousands more have been tragically and horrifically wounded. The internet was not involved in that terrible tragedy, nor will the surviving troops be affected significantly by revelations about CIA activities that were previously covert.”

Chapman added that if the government continued to look outward for threats to national security, it may be in for a big surprise.

“The real story is that the US is running its own national security into the ground via its own actions, and the policies of our government. Americans have more to fear from the incompetence of our own leaders than the competence of some hacker or info-geek who happens to ferret out some information that the US would prefer to remain secret,” he said.

As for how the agency is dealing with the fact that some activities are no longer covert, according to the Tribune CIA director Goss is “committed to modernizing the way the agency does cover in order to protect our officers who are doing dangerous work”.

The spokesperson declined to give the paper details because the CIA did not want the “bad guys to know what we’re fixing”.

For the sake of the CIA’s covert employees, hopefully the “bad guys” will not log on to find out.

Rashunda Tramble is an editor for ISN Security Watch in Zurich.