

Welcome to the C.N.A. E-Bulletin Vol. 3, No. 15 – March 13, 2007

An electronic publication of the Canadian Numismatic Association
Copyright © 2007, the Canadian Numismatic Association

SPECIAL “SPY COIN” EDITION

INTRODUCTION

Much has been made of the original report about the existence of three so-called “Spy” coins, the U.S. government denying their existence, the retraction of the portion of the report dealing with the existence of the coins and then another update saying that investigations seem to indicate the existence of the coins. No wonder that in a previous bulletin I stated: “It seems there’s no danger of your spare change spying on you after all. Or is there? Or isn’t? Or is?”

Although the final chapter has yet to be written, we present a special “Spy Coin” edition.

SNEAKER WITH GPS TRACKS DOWN WEARER

First, a report claims that three Spy coins exist. Now we read that Quantum Satellite Technology is going to sell a line of sneakers starting next month that will include a tiny Global Positioning System chip. The chip will offer peace of mind to people who might have wandering children, elderly parents or people with Alzheimer’s patients, according to an Associated Press news release.

The technology works...if you pay a monthly fee of \$19.95...when you press a button on the sole to activate the GPS device. The sneakers will sell for \$350 (US). The company claims that out of the 1,000 shoes that will be manufactured and sold over the Internet, 750 have been pre-sold. The technology will also be put into military boots, which, according to a news release, includes “a 2 inch by 3 inch chip.”

Now I know why the Royal Canadian Mint is considering a \$1 million coin. All existing coins are too small to easily incorporate a reasonably priced spy chip. Solution: make a coin large enough to easily hold a chip size 2 inches by 3 inches. Hence the \$1 million coin!

Now you know why you subscribe to this bulletin. It’s because we track down the truth! Just like the lawyers and politicians!

NEW TRACKING CHIP SIZE OF A DUST GRAIN

The following report by Bill Christensen, comes to us via Technovelgy. Its reason for being included here is that, as the article states, it can be incorporated into paper currency and gift certificates...or spy coins.

The world's smallest and thinnest Radio Frequency Identification (RFID) tags were introduced recently by Hitachi. Tiny miracles of miniaturization, these RFID chips measure just 0.05 x 0.05 millimeters. "RFID" refers to small electronic devices that use a tiny antenna to transfer small amounts of data for identification purposes.

The previous record-holder, the Hitachi mu-chip, is 0.4 x 0.4 millimeters. The mu-chip RFID tag looks like a speck of dust on a human fingertip. The "powder type" tags are some 60 times smaller, barely noticeable next to a human hair. To see a photo of the mu-chip in relation to the size of a thumb and a powder RFID next to a human hair, go to:

<http://technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=939#mu>.

The new RFID chips have a 128-bit ROM for storing a unique 38 digit number, like their predecessor. Hitachi used semiconductor miniaturization technology and electron beams to write data on the chip substrates to achieve the new, smaller size.

Hitachi's mu-chips are already in production. They were used to prevent ticket forgery at last year's Aichi international technology exposition. RFID 'powder,' on the other hand, is so much smaller that it can easily be incorporated into thin paper, like that used in paper currency and gift certificates.

Science fiction fans will have a field day with this new technology. In his 1998 novel "Distraction," Bruce Sterling referred to bugged money: "They always played poker with European cash. There was American cash around, flimsy plastic stuff, but most people wouldn't take American cash anymore. It was hard to take American cash seriously when it was no longer convertible outside U.S. borders. Besides, all the bigger bills were bugged."

These tiny RFID tags could be worked into any product. Built into doorways, theft of consumer goods would be practically impossible. These devices could also be used to identify and track people. For example, suppose you participated in a protest or other organized activity. If police agencies sprinkled these tags around, every individual could be tracked and later identified at leisure, with powerful enough tag scanners. To put it in the context of popular culture, you may recall the following scene from the 1996 movie "Mission Impossible." One of the IMF operatives places a tracking tag on the shoulder of a computer programmer. But that, in comparison, was a pretty clunky-looking tag!

ARE SPY COINS PURELY SCIENCE FICTION?

Technovelgy.com publishes articles under the byline "Science Fiction in the News – The predictions of science fiction writers coming true in today's world." They recently published the following article by Bill Christensen under the heading "Canadian Coins Are Bugged Money."

Canadian coins with transmitters have been found in the pockets of American contractors who visited Canada, according to the Department of Defense (DoD). A DoD report titled "Technology Collection Trends in the U.S. Defense Industry" reports on the problem: "On at least three separate occasions between October 2005 and January 2006, cleared defense contractors' employees traveling through Canada have discovered radio frequency transmitters embedded in Canadian coins placed on their persons..."

The report does not specify the kind of technology used. The coins could have been bugged using RFID technology. However, this would only serve to "mark" an individual so he could be discerned in a crowd using an RFID reader. RFID does not have any means of transmitting voice data, which is apparently the case with this bugged Canadian money.

CANADIAN SPY COINS – THE BEGINNING

For those of you who missed the original story, following is the initial report from The Canadian Press:

They say money talks, and a new report suggests Canadian currency is indeed chatting, at least electronically, on behalf of shadowy spies.

Canadian coins containing tiny transmitters have mysteriously turned up in the pockets of at least three American contractors who visited Canada, says a branch of the U.S. Department of

Defense. Security experts believe the miniature devices could be used to track the movements of defense industry personnel dealing in sensitive military technology.

"You might want to know where the individual is going, what meetings the individual might be having and, above all, with whom," said David Harris, a former CSIS officer who consults on security matters. "The more covert or clandestine the activity in which somebody might be involved, the more significant this kind of information could be."

The counter-intelligence office of the U.S. Defense Security Service cites the currency caper as an example of the methods international spies have recently tried to illicitly acquire military technology. The Service's report, *Technology Collection Trends in the U.S. Defense Industry*, says foreign-hosted conventions, seminars and exhibits are popular venues for pilfering secrets.

The report is based on an analysis of 971 "suspicious contact reports" submitted in fiscal 2005 by security-cleared defense contractors and various official personnel. "On at least three separate occasions between October 2005 and January 2006, cleared defense contractors' employees traveling through Canada have discovered radio frequency transmitters embedded in Canadian coins placed on their persons," the report says.

The report did not indicate what kinds of coins were involved. A service spokeswoman said details of the incidents were classified. As a result, the type of transmitter in play — and its ultimate purpose — remain a mystery.

However, tiny tracking tags, known as RFIDs, are commonly placed in everything from clothing to key chains to help retailers track inventory. Each tag contains a miniature antenna that beams a unique ID code to an electronic reader. The information can then be transferred by the reader into a computerized database.

The likely need for such a reading device means the doctored coins could be used to track people only in a controlled setting, not over long distances, said Chris Mathers, a security consultant and former undercover RCMP officer. "From a technology perspective, it makes no sense," he said. "To me it's very strange."

Then there's the obvious problem: what if the coin holder plunks the device into a pop machine? "You give the guy something with a transmitter that he's going to spend - I mean, he might have it for an hour," Mathers said with a chuckle.

Harris speculates recent leaps in miniaturization could allow for a sophisticated transmitter capable of monitoring a target's extensive travels. "I think we can be pretty darn confident that the technology is there for the sorts of micro-units that would be required to embed these things in a coin," he said. "It's a brave new world, and greatly concerning on so many levels."

Passing the coin to an unwitting contractor, particularly in strife-torn countries, could mark the person for kidnapping or assassination, Harris said. "You could almost, by handing a coin to somebody, achieve the equivalent of the Mafiosi's last kiss on the cheek."

The Defense Security Service report says employees of U.S. contractors reported suspicious contacts from individuals, firms or governments of more than 100 countries during the year. Technologies that generated the most interest were information systems, lasers and optics, aeronautics and sensors.

A foreign approach often meant a simple request for information from the contractor. But the report also underscores clandestine means of acquiring secrets from U.S. employees, particularly those traveling abroad. "It is important to recognize copiers and shredders can contain built-in scanners to copy the data." Other common methods include placing listening devices in rooms, searching hotel rooms, inspecting electronic equipment and eavesdropping on conversations.

The report, which first came to light in a U.S. newspaper, has since been posted on the website of the Federation of American Scientists, an organization that tracks the intelligence world and promotes government openness.

CANADIAN SPY COINS – THE RETRACTION

Under the heading "Pentagon caught inventing 'Canadian spy coin' story, the Wonkette website states the following:

The Defense Department finally admitted that its claims that Canadian spy coins were found tracking U.S. defense contractors is just some crazy made-up bull that ended up in an official DoD espionage report last week.

The news, obviously, is that this time the Pentagon actually acknowledged its pointless lies. It usually takes 10 years, thousands of dead U.S. troops and a few failed occupations to get anybody over there to admit any culpability.

The extra-great part is nobody knows where the ridiculous Magical Canadian Coins Hunt U.S. Contractors story even originated - it just showed up in the report with all the other stupid lies.

WHAT GOOD WOULD THEY BE?

What good would spy coins be, even if they did exist? Here is what the Techdirt Website has to say:

There's been a lot of talk lately about the use of RFID chips in various things like tires and sneakers, and how these technologies could be misused to spy on your whereabouts. Of course, what's never clearly explained is how effective such a solution would be. RFIDs tend to have very limited range. Still, with so much talk about using RFIDs to spy on people, is it any wonder that press quickly jumped on the story about the US Defense Department is warning American contractor employees to be careful when they get foreign change. The story claims that a few contractors discovered that the Canadian coins they had, held RFID chips placed inside. However, no one seems to have a good answer to explain what this would be useful for. A reader would need to be quite close to the coins to get a read on the tags, at which point you wonder exactly what the benefit really is. Also, since change tends to be spent or passed around pretty rapidly (with no indication back to whoever put the chips in the coins), it might not be even remotely effective in following an individual. Perhaps the answer is that it didn't really happen. Another news report on the topic claims that there were some concerns, but an investigation of the coins found no transmitters. That source claims the report about the RFID coins was simply false, and never should have been reported. No matter which story is actually true, it seems like lots of people are eager to jump onto any claim of RFID-based spying, even if there's no technological reason to be concerned.

CONCLUSION

Well, that should finish our report on Spy Coins, at least for now. Watch this space for news about some U.S. government department acknowledging that there have indeed been

“incidences” of spy coin discoveries. And if that happens, watch www.whereswilly.com or www.wheresgeorge.com announce that they are tracking coins as well as notes, which makes sense - with governments considering switching to coins for higher denominations, the tracking sites might feel they will be out of business unless they start to track coins!

Okay, enough about the non-existent spy coins!

John Regitko
Your C.N.A. E-Bulletin Editor
Canadian Numismatic Association

The Canadian Numismatic Association is a not for profit organization devoted to serving those who enjoy coin collecting/numismatics by promoting fellowship, communication, education and providing advocacy and leadership for the hobby.

If you have a comment to make, or would like to submit an item for publication, email:
cnanews@look.ca

To subscribe to the E-Bulletin email:
cnanews@look.ca

Back-issues of the C.N.A. E-Bulletin are available from the C.N.A. Website at
<http://www.canadian-numismatic.org/ebulletin.php>

If you have questions about our privacy policy, email:
privacyissues@canadiannumismatic.org

To learn about the benefits of membership or to join the C.N.A. visit our website at:
www.canadian-numismatic.org

For a complimentary copy of The CN Journal, email your name and mailing address to:
cnainfo@look.ca

Any submissions, comments or information sent to us will be shared with subscribers unless indicated otherwise. We reserve the right to edit submissions for publication.