TAIPEI TIMES

SUNDAY FEATURES

SUNDAY, SEPTEMBER 28, 2008

Who has your old phone's data?

Millions of mobile phones are lost and discarded every year, yet their owners give little thought to the sensitive information they contain

BY **PETE WARREN**
THE GUARDIAN, LONDON

Three years ago, Graham Clements — the European managing director of the UK subsidiary of the Japanese packaging multinational Ishida — decided to get rid of his BlackBerry and passed it on to his IT department for recycling. At the start of this month, that BlackBerry was one of the top items on the agenda at the first board meeting that Clements had called since his return from holiday — because it, and the data on it, had come back to haunt him.

Instead of being recycled, the BlackBerry, like millions of other mobile devices every year, had been passed on to a company to be sold. On Clements's device were business plans, details of customer relationships, information on the structure of the company, details of his bank accounts and details about his children.

And Clements isn't alone. It's almost impossible for the average person to wipe a mobile phone clean: unlike a PC, which has an open architecture, mobile phones are closed books in terms of where data resides. "It has taken us over a year to get talks going with Nokia that now allows us to wipe their phones," says Jon Godfrey, director of Sims Lifecycle Services, which recycles mobiles. "We have to go through a different process with each manufacturer. To wipe it, you have to be able to access all the memory — and manufacturers don't want you to do that for all sorts of commercial reasons."

Yet, in the UK for instance, every six months 63,000 phones and around 6,000 PDAs are left in cabs in London alone. At the city's Heathrow airport, 10 phones are handed in every day; one in four has no security and can be turned on by staff. Furthermore, the security of the data on those devices is the responsibility of the person who put it on the phone. It is not illegal to read it; it is up to you to protect it.

The case of Clements is not unique. That BlackBerry was among several that were recovered from mobile phone recycling companies as part of a study into data loss on mobile devices by BT (formerly British Telecom), Glamorgan University, Australia's Edith Cowan University and Sim Lifecycle Services. It was intended to demonstrate just how much data a mobile device can collect about you. For as Clements discovered, we very quickly create intensely personal relationships with these devices.

Just how personal those relationships can be was shown by one BlackBerry recovered in Australia. It revealed that its owner, a businessman, lived in an upmarket part of Sydney. It also contained the details of his various businesses, including bids and contracts under negotiations, uncomplimentary comments about employees, an extensive list of contacts and a complete log of phone calls and diary commitments. It even held extensive and lurid exchanges between the man and a woman he was conducting a clandestine affair with.

With government departments losing laptops and discs teeming with information seemingly every week, it is easy to forget how much data is held on our PDAs and phones. The problem is that very few of us take any care to secure them against loss or theft.

Over the next few years, the phone industry hopes to tempt us with new devices that will be able to hold huge amounts of information, while the financial services industry aims to turn mobiles into payment devices that incorporate credit cards. Nearly all of them are designed so they can be linked to a computer to exchange and back up data or music. When they do, virtually by default, they will exchange information from your address book and your diary.

Is that safe? No. Two years ago CESG, the technical wing of the UK government's eavesdropping organization GCHQ, which is responsible for advising the government on technology vulnerabilities, was privately briefing that mobile phones cannot be wiped. Now, according to CESG, some measures can be taken, though its spokesman was not prepared to share precisely what those measures are. CESG says: "The government needs assurance that information has been properly erased in all forms of electronic device. Guidance is provided to departments on the most appropriate ways of achieving this. The advice provided to government departments is classified and we are not able, or prepared, to provide detail."

However, as Clements points out, this is exactly the sort of information that is needed. He says: "So what are people meant to do with things when they have finished with them?"

According to Godfrey at Sims Lifecycle Services, a discarded, unwiped phone or PDA is "a perfect tool for social engineering, and it's only going to get worse" as the storage capacity of mobile devices increases.

He says: "The point of this work is really to bring that across to people the risks that mobile phones present to their personal data." Of the devices in the survey, 7 percent had enough personal data on them for the individual concerned to have their identity stolen, and 7 percent would have allowed a corporate fraud to have taken place. Another 2 percent still had SIM cards in them, while 27 percent of the BlackBerrys in the survey had company data and 16 percent carried personal information.

Of the 161 devices in the survey, many were first-generation GSM phones, and only 82 could be made to work. But as Andy Jones, head of information security research at BT's research center, points out, that alone is significant. "The life expectancy of a mobile device is only slightly longer than that of a butterfly," he says. "People only hold on to their own phones for around 12 months; corporate devices go for 24 months.

"But when they are finished with, the devices are not generally considered to have any intrinsic value to the organization. When they reach the end of their effective life, they do not appear to be given any consideration with regard to the data that they may still contain."

Says Andrew Blyth of Glamorgan University's computer forensics department: "There are no tools out there at the moment that let you destroy the data on mobile phones, so I think that people need to take the appropriate measures to protect their personal data."

Craig Valli, of Edith Cowan's school of computer and information science, says that many of the BlackBerry devices he analyzed represented a significant risk. "Loss of these devices could have resulted in a number of secrets and sensitive information being revealed, the end result of which could have been significant criminal activity." In fact, BlackBerrys do have a remote erase routine, but it is not standard across the industry.

Most of us leave old phones in drawers or cupboards at home until they are given to charities, which pass them on to recycling companies that pay them for the devices. And then we forget about them, until — as in Clements's case — they turn up three years later. But he was lucky. Most of the phones from recycling companies are destined for Africa and Asia — areas that are rapidly gaining a reputation for ID theft. Do you know where your last mobile phone is now? And whether it was wiped clean before you got rid of it?

Below: A pedestrian talks on a cellphone on Tuesday in London. PHOTO: AP
Left: Mobile devices such as Google's G1, which hold large amounts of information about our business and personal lives, are potential gold mines for identity thieves. PHOTO: AFP