Publication: Irish Examiner
Date: Tuesday, October 3, 2006
Page: 16
Extract: 1 of 3
Circulation: 57.331
Author: Pól Ó Conghaile
Headline: SO, WHO ELSE IS LISTENING ...?

SO, WHO ELSE IS LISTENING ...?

In the first of a two-part series on our rights to privacy, **Pól Ó Conghaile** examines how easy it is to eavesdrop on other people's voicemail or read their texts

IT'S official: there are more mobile phones than people in Ireland. By the end of 2005, according to the Commission for Communications Regulation (ComReg), 4.27 million subscribers accounted for a penetration rate of 103%.

And, boy, do we use 'em. In the first quarter of 2006, Irish people consumed 1.5 billion voice minutes and sent almost 1.3 billion text messages.

Given such market saturation, and what seems like absolute dependence on mobile phones, are consumers paying enough attention to their security?

Recent allegations that a News of the World journalist hacked into a British royal family member's voicemail suggests the technology may be more vulnerable to privacy invasion than we think.

British Labour MP David Blunkett and Victoria Beckham may also have been victims of tabloid hacking, it has emerged.

Before that, in 2002, unwitting voice messages led to the uncovering of the affair between celebrity Swedes Sven-Goran Eriksson and Ulrika Jonsson.

"If you put a team of codebreakers together, you might eventually crack it, but most four-digit codes that have been encrypted are quite difficult to break into," says Tommy McCabe, director of the Irish Cellular Industry Association (ICIA).

There is no great science involved in accessing private messages through compromised personal PIN codes, however. If the owner does not change the default setting standard (typically 0000), his or her mailbox is open to abuse.

Such action could be deemed criminal under the Postal and Telecommunications Act 1983. However, because the act refers to messages "being transmitted", barrister TJ McIntyre suggests stored messages "do not enjoy adequate protection".

Mobile phone operators are careful to warn customers to change their PINs, both in their literature and the first time voicemail systems are accessed.

"It's the same as getting a suitcase with a 000 combination lock on it," says a Vodafone spokesperson. "Anybody can open it until you set that PIN."

Despite the companies' efforts and the "robust" security of their mailbox systems, anecdotal evidence suggests there is no shortage of less scrupulous users.

When TV presenter John Leslie faced allegations of rape in 2003, for instance, a journalist attempting to access Leslie's voicemail found he was still using the factory PIN. The reporter reset it with a new number and Leslie was frozen out of his own messages.

In Ireland, in July, four people lodged allegations that their mobiles had been illegally accessed by a property magnate. The matter was investigated by gardaí.

"If anything, it's carelessness on behalf of the user," McCabe confirms. "They leave their four-digit code lying about, or use their date of birth, or 2006, and people poke through their rubbish bins or put two and two together."

"If you don't change a password, and somebody gets unauthorised access to your mailbox, I would call that social engineering," says Bernard Tyers of civil rights group Digital Rights Ireland (DRI).

Social engineering differs from hacking, Tyers explains, as it involves gaining unauthorised access "in an untechnical way" and is the easiest fraud of this nature.

Publication: Irish Examiner
Date: Tuesday, October 3, 2006
Page: 16
Extract: 2 of 3
Circulation: 57.331
Author: Pól Ó Conghaile
Headline: SO, WHO ELSE IS LISTENING ...?

While technically it may be possible to bug voice traffic between phone and network, for example (as happened with the late Princess Diana and James Gilbey in the infamous "Squidgy" tapes of 1989), a much simpler con is to impersonate a phone company representative, or tap the mailbox of a naïve user whose PIN remains set on default.

In such an event, quite aside from sensitive voicemails, one stands to unearth a detailed set of information — ranging from numbers dialled and time of calls to a record of location as one's phone moves from cell to cell.

That's a vast amount of data on any private life — and concerns about its use are mounting, particularly given Government plans to expand data retention laws requiring its storage, and that of similar information relating to emails and internet surfing.

"In an ideal world, once the bill is paid such data should be deleted," the data protection commissioner told a forum on the retention of communications traffic data in 2003.

"However, if you can no longer feel secure that your telephone, web surfing and electronic communications are, in fact, private, then that signals a major change in the nature of the society in which we are living."

Data protection legislation currently provides that such information can be kept only for lawful purposes (such as billing) and for no longer than necessary.

But how long is necessary?

Three years, according to the Criminal Justice (Terrorist Offences) Act 2005, which provides for such data to be made available to gardaí on request.

No more than one year is acceptable, counters the data protection commissioner, who points out that access restrictions for gardaí have not been imposed, leaving customers vulnerable to marketing, snooping, blackmail and surveillance.

"Does the State want to keep data on everyone just in case we might become a criminal, or does the State wish to treat us all as criminals?"

It is common knowledge that mobile phones can be tracked by telecommunications base stations when they are switched on — a feature which lead to major breakthroughs in criminal investigations such as the Omagh bombing and the Robert Holohan manslaughter case.

Less well-known, though — and further cause for concern regarding privacy rights — is that commercial mobile phone tracking services are increasingly available.

In Britain, traceamobile.co.uk offers "peace of mind by discreetly tracking the location of [the] mobile phone[s]" of children, older people, even hikers and climbers. When the phone is turned on, movement can be monitored online with an accuracy of between 50 and 500 metres.

In Ireland, Top Security plans to introduce the first phase of a commercial tracking service, according to group marketing and PR manager Helene Devlin.

The plans have proved controversial. Although Devlin won't be drawn on potential customers, it has been suggested that tracking products aimed at businesses or parents could be abused by anyone with access to the subscriber's phone for a short period.

"Mobile phone tracking services have clear potential for abuse and comprehensive safeguards need to be in place to ensure the tracked person has given full, ongoing, informed consent to being tracked," says a DRI statement.

Clearly, striking a balance between privacy, security and the right to make a profit is a sensitive endeavour — and mobile phones remain at the cutting edge of that process, particularly as they wriggle and evolve into complex multimedia devices.

"Seen a celebrity when you are on holiday? Caught someone somewhere they shouldn't be?" asks thesnitcherdesk.com, one of a number of websites which acts as a middleman for punters who want to flog opportunistic mobile phone photos to tabloid newspapers.

Open source or citizen journalism appeared to be flourishing in the wake of the London bombings last year, but with news agendas pitching rapidly from crime to celebrity, the defence of public interest appears increasingly under threat.

Witness recent pictures of Kate Moss or Liam Kelly allegedly snorting cocaine, for example, or Prince Harry fondling a fellow party-goer. Are such photographs in the public interest, or an invasion of a person's reasonable expectation of privacy?

With the majority of handsets now integrating cameras, the question is increasingly pertinent — and not just for celebrities.

What if a disgruntled ex-partner or mischievous friend took a compromising picture and posted it online, for example?

"The industry has certainly looked into it," says Tommy McCabe of the ICIA.

"There is no law banning cameras or camera phones anywhere, but any individual or organisation, such as a school or swimming pool, can say no mobile phones are allowed in there."

"There's no real definite answer," says the DRI's Bernard Tyers. "It's supposed to be looked at under Michael McDowell's Privacy Bill ... if that ever comes to fruition."

In the meantime, concerned celebrities and other citizens could look elsewhere for a solution: in South Korea, legislation requires camera phones to emit an audible noise or flash when taking pictures. If your privacy is compromised, at least you'll be the first to hear about it ...

Publication: Irish Examiner
Date: Tuesday, October 3, 2006
Page: 16
Extract: 3 of 3
Circulation: 57.331
Author: Pól Ó Conghaile
Headline: SO, WHO ELSE IS LISTENING ...?

"It's the same as getting a vanity case or suitcase with a 000 combination lock on it. Anybody can open it unless you set that PIN"