

This article takes a closer look at the issue of invasion of privacy when talking or surfing on the wireless web. It investigates the reasons why 'Big Brother' may be watching you, where he's snooping and how he keeps track of your every 'cyber journey'. Runs to 1592 words.

For sale to printed and web publications. Please email for a quotation. This article is subject to copyright. Unauthorised reproduction prohibited.

I Know What You Did Last Night

Well, I don't really, so don't panic, your secret is safe with me but if you did do a bit of casual Web surfing, chances are someone; somewhere knows what you looked at and where you went on the wired Web. As this article reveals, going totally mobile won't waylay the watchers either as the science of snooping keeps pace with wireless innovation.

I don't know about you but I like cookies, especially chocolate chip flavour but a less palatable variety stick to your hard disk instead of your teeth. That's because a 'Cookie' is also a tiny piece of code websites place on your hard drive when you pay them a visit that can send back to their originators all manner of stats about your browsing habits, from how much you spent on your subscription to Wireless World (and you DO subscribe don't you?) to making a note of the hundreds of sites you visited in the last month.

Some are innocuous little things that make your surfing easy by remembering your user name and password for that particular site, but others are more sinister and could pose a threat to your privacy. Internet advertising giant and cookie lover DoubleClick recently got a legal wrap over the knuckles when it bought a marketing company that maintained a database of names, addresses and retail purchasing habits of 90 percent of U.S. households and began profiling Web users.

Think you're safe from spies while surfing on the bus to work? Think again. The next generation of wireless browsers are aimed at providing PC-like Web browsing on IP-based 3G phones and as such can also support Cookies, a prospect that must have the marketing men at NetGenesis salivating as a whole new mobile demographic opens up for possible exploitation.

NetGenesis Corp recently introduced Wireless InfraMarketing - 'habit tracker' software that promises to tell e-businesses everything they need to know about your surfing proclivities. Advocates of privacy have long decried this practice, especially when the information could be sold to third parties who then may bombard your cellphone with sales messages. NetGenesis defends itself by saying its software is intended to help businesses design more effective Web sites and marketing strategies that specifically target mobile Web users but defenders of anonymity decry it as yet another electronic Peeping Tom.

But maybe I'm just being paranoid. According to the latest surveys, users are becoming more tolerant of Cookies because of the convenience and personalisation they offer and so are prepared to give up privacy in return for not having to use too many brain cells when surfing.

"So many sites have log-ins and passwords. You're up to your eyeballs, and people really want those cookies," said Mark Peacock, an analyst at Deloitte Consulting. John Ragsdale of Giga Information Group has a somewhat more cynical view; "the technology is used more at the expense of the consumer than to benefit the consumer.....It is pretty shocking to look at your Cookie file and find out how many companies are watching you," he said.

This trade off between privacy and convenience may be inevitable, especially so when global positioning technology is steadily making its way into cell phones and other handheld devices. The upside is that users will benefit from location based services that, for instance, find the nearest branch of your favourite coffee shop in an unfamiliar city and direct the ambulance to within 100 metres of your horizontal position on the pavement when you start choking on the chocolate chip cookie you had with your latté.

Well that's the excuse they are using in the U.S. where communications authorities are leaning hard on wireless carriers to adopt location-based technology sooner rather than later in order to improve response to emergency calls made from mobiles but civil rights campaigners also point out that any gadgetry aimed at providing in-situ services to consumers could also turn every cell phone or handheld into a potential tracking device for advertisers and governments.

Still smarting after the blow of September 11, the Bush administration is expected to recommend the appointment of a 'Privacy Czar' as part of its impending National Strategy for Securing Cyberspace, itself part of a Homeland Security Bill that seeks to greatly expand the U.S. government's electronic surveillance capabilities under the guise of needing to examine data traffic for possible security threats. The potential to track every mobile user via their handset could be every CIA agent's dream come true.

Whilst location-based services are still in their infancy, so touchy is the subject of possible invasions of privacy that telecoms giant AT&T rolled out the 'big guns' to assuage concerns over its recently launched version of the genre.

AT&T President John Zeglis put privacy at the top of his list not only in wireless but in the entire telecommunications industry-during his speech at

the SuperComm 2000 trade show held recently. In an address devoted almost entirely to the wireless Internet, he listed privacy as one of the top three issues facing the sector, along with availability of services and quality customer experience. André Dahan, President of Mobile Multimedia Services at AT&T also tried to assure doubters when he said "We have a comprehensive privacy policy and our customers' information -- including their geographical location -- is theirs to share with whom they want." According to Dahan users have the option of setting their handsets to 'invisible', under the AT&T plan.

Much as with the wired Net, potential users of GPRS and its ilk seem unconcerned by potential Big Brother surveillance implications. According to a survey of 700 wireless households, the bulk of respondents are receptive to the concept of location-based services and keen to use the service for emergencies, travel, driving information and obtaining information about nearby businesses.

Of course, this public apathy may be music to the ears of any jittery government hoping track your every move on the pretext of you either being a potential terrorist or, in their view, an 'undesirable'. Such an Orwellian vision of the future may not be as far fetched as you think.

According to a report from the human rights group Reporters Without Borders, all over the globe, governments of every political persuasion are watching the wired Internet watchers under the guise of "combating global terrorism".

Whilst it may be no surprise to learn that the more politically or religiously hard line countries such China, North Korea, Vietnam and Saudi Arabia keep a close eye on the how, what, where and when of their citizens surfing habits, in

the wake of the World Trade Centre attacks, increasingly paranoid Western democracies are also stepping up Net surveillance.

For instance, a Canadian anti-terrorist law adopted last December, "clearly undermines the confidentiality of exchanges of electronic mail." the report claims whilst in France a law was recently passed requiring ISPs to maintain records of email exchanges for one year and to enable easier decoding of encrypted messages. In addition the report claims that the governments of Spain, Britain, Germany, Italy, Denmark and, of course, the U.S. have all stepped up their Net surveillance capabilities. The report pointed to technology being developed by the FBI called "Magic Lantern," which will allow investigators to install over the Internet and without a user's knowledge, eavesdropping software capable of recording every keystroke on a PC. How long before they turn their attention to the wireless environment too?

Whilst the exponential expansion of wireless communications is seen as a boon for the general population, there is no reason not to suppose that governments around the globe now see the possibilities of free and unfettered exchange of information over wireless networks as an equal, if not bigger threat to their interests than the wired Web and will devise, if they have not done so already, ways and means of recording your every mobile conversation or action, be you terrorist or tourist.

But it's not just 'Big Brother' keeping eyes on you, so, it would appear, are your fellow citizens. Take for example the recent much publicised incident in the US where a group of friends of Middle Eastern origin had their completely innocent mobile conversations overheard by 'patriots' who put two and two together and came up with a dastardly terrorist plot that led to the boys ending up face down on the public highway with police guns pointed at their heads. Next time you go see a movie and phone your friend to say "the PLOT was

TERRORble, it will BOMB at the box office", do it very, very quietly because walls really do have ears.

So it seems the old phrase 'you don't get something for nothing' applies as much to your ultra-convenient wireless life as to the rest of existence. Either you will see eroded anonymity as a fair price to pay for your 'do it anywhere' lifestyle or an infringement of your right to privacy but like it nor not, either state or commercial snooping seems inevitable - that's just the way the cookie crumbles.

© [Read My Stuff](#) 2005