ILLUSTRATION: DAVID ANGEL

Secret service providers

In May, to many people's surprise, the European Parliament rubberstamped legislation which allowed EU member countries to force businesses such as ISPs to retain electronic data about our personal communications for years on end. This is just one of many ways our electronic privacy is being compromised, explains Peter Thomas

The UK Regulation of Investigatory Powers Act created quite a stir when it came into force in October 2000, quickly earning itself the nickname the Grim Ripa. For the first time in history the British government had handed police and security services sweeping powers to snoop on our daily lives.

The act received royal assent on 28 July 2000 and Jack Straw, then Home Secretary said: "The Ripa powers, simply put, are essential to help keep the UK a safe place for everyone to live and work." What's more, the act has recently been extended so that many more national and local government departments are now able to access and act on the information about each and every one of us.

Frightening tales then emerged claiming that GTAC (the Government Technical Assistance Centre) will link MI5's headquarters in London directly to every ISP in the UK. John Abbott, director-general of the National Criminal Intelligence Service, was quick to deny this: "Conspiracy theorists must not be allowed to get away with the ridiculous notion that law enforcement would, or even could, monitor all emails.

"The bill does not require all internet service providers to install a black box linked to the Security service which will monitor all internet traffic. This allegation is completely false. The bill does not say it, the intercepting agencies are not asking for it and reports of black boxes by the press are confused and inaccurate." So that's all right then. Or is it?

Nowhere to hide

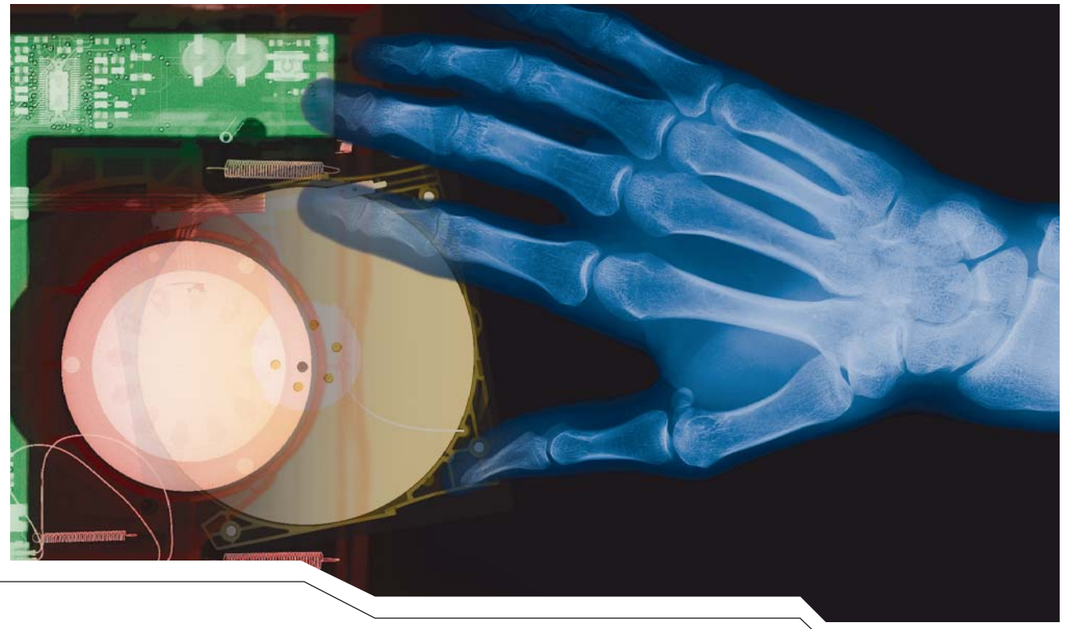
The fact that we need this kind of legislation in the first place has brought home how, in the digital age, we can no longer assume that our privacy is sacrosanct and that we are able to spy on each other in many different ways.

We have come to wonder whether perhaps our private lives aren't so private after all. Are we right to be nervous or is it all media hype? Is our personal data safe as it crosses the internet or are we all going to have to get used to being snooped on? What methods can other people use to spy on our every move? What is this 'spyware' that everyone keeps talking about anyway?

Put simply, spyware is any software that employs a user's internet connection in the background (the so-called 'backchannel') without their knowledge or explicit permission. Spyware shows up in the most unlikely places. If you've downloaded anything from the internet or installed more than just a few programs from the web, there's a strong possibility you're being spied on every time you go online. You probably have spyware hidden away on your PC, reporting back to headquarters – to the marketing companies who collect this data without your knowledge or permission – every day you are online.

No such thing as a free lunch

Spyware works like this: you download a program that is just what you've been looking for – a download manager, maybe, or an MP3 jukebox. You don't have to pay anything for it. It either masquerades as a freeware program or is presented as



Only three percent of consumers read online privacy statements when they visit new sites to buy goods. Either people feel so safe that they don't care about the small print, or they simply can't be bothered

adware – a program that shows you advertising while it runs.

When you install the downloaded file, the installation software also places a hidden program somewhere on your computer. To our knowledge all the spyware currently in use works only on Windows PCs. This doesn't mean the bad guys are picking on Windows; it's just that Windows is the obvious target since most PCs are running one Windows version or another.

The hidden program monitors your activities in whatever way the spyware authors want. But the companies that create and plant spyware on your PC say they're grossly misunderstood. They say they always get permission. In other words, whenever you install a spyware-enabled program you're shown a statement that asks if it's okay if someone spies on you.

This may be true but, if it is, it's news to us – unless the statement is hidden away in the licence document that pops up before the download begins. Most people are so keen to get on with things that they usually click the ok button without reading the document.

An apathetic bunch

A Harris Interactive survey discovered that only three percent of consumers bother to read online privacy statements when they visit new sites to buy goods. This means either that people feel so safe when shopping online that they don't care about the small print or that they simply can't be bothered – after all, they are shopping online in the first place because they want to save time and money and don't want the hassle of ploughing through half a page of legal waffle. This just will not do.

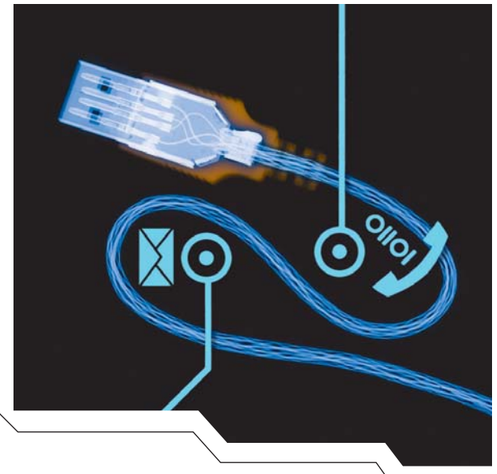
Everyone runs the risk of finding their personal data has been sold to a third party unless they take steps to study a website's privacy policy and to vote with their mice if they don't like what they read. E-traders take note: what consumers need is a clearly worded statement, placed in a prominent position, preferably by the digital 'till', so they can see what it is they are agreeing to before clicking on that 'Submit order' button.

Careful what you say about the boss

All over Britain, company employees are becoming accustomed to seeing notices like this posted on the company intranet, or being sent to them by email: "As required by UK legislation, the company draws to the attention of all users of the company's networks the fact that their communications may be intercepted as permitted by legislation.

"The legislation allows the company to intercept without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance and detecting crime or unauthorised use. The company does not need to gain consent before intercepting for these purposes, although staff should be advised that interceptions may take place."

Snoopers can read every email, instant message and document you send and receive, even if you deleted or never even saved what you typed



Right now, your boss, the police or a government department could be secretly reading every word you type – even the ones you deleted – while surreptitiously taking your picture. Sounds alarming? Well it should.

The latest versions of spy software can snap pictures from a webcam, save screenshots and read keystrokes in multiple languages. Snoopers can read every email, instant message and document you send and receive, even if you deleted or never even saved what you typed. Spy software can be downloaded from the web and costs about the same as a meal for two in a restaurant.

These programs run in what's called 'hidden in plain sight' mode. They change their name every so often and files containing the information they gather are given arbitrary old dates to make them difficult to find. The monitor can choose to have a user's every move sent to an email address or the program can be instructed to look for keywords such as 'boss', 'pornography' or 'terrorist' and only send records when it finds those prompts.

Software like this was virtually unknown a couple of years ago. Now it's become a lucrative niche market, attracting plenty of competitors and at least one product that aims to track down the snooping software itself. FBI investigators recently used this type of software to snag suspected Russian computer hackers, one of whom was subsequently convicted on 20 counts including conspiracy, various computer crimes and fraud.

Corporate employers are using such software to catch employees who send out their CVs to prospective employers, download pornography or spend their time playing online games. Many UK companies will not admit to snooping on their staff, but it's thought that the practice is becoming widespread.

In most cases, snooping software is not illegal but, morally, there are some very important issues to be addressed with employers tracking the personal habits of their employees.

Loyalty will get you everywhere

It has been said that there are three types of people who need have no fear of their personal habits being recorded and stored in databases: the very poor, who have little or no access to credit or debit cards or to the internet; the Luddites, who don't believe in all this new-fangled technology; and the very rich and famous. The rich are safer in one respect, because they tend not to use personal credit cards and don't freely disclose their email address. The rest of us had better accept that we have little remaining privacy and that which we do have is under attack.

Imagine you have a supermarket loyalty card which is swiped every time you buy the groceries. Linked to your personal details is a database showing everything you have bought since you got the card. This allows the supermarket to build a profile of your eating habits – your lifestyle even. Next time you're driving in the vicinity of the supermarket the company fixes the position of your car, using that nifty satellite navigation device that the salesman persuaded you to add on. Soon, your mobile phone bleeps and a satellite text message appears – it's from the supermarket, telling you they've got a fresh consignment of those salmon steaks you buy so often.

Can it happen? Yes it can and it may well be happening to millions of us unless legislators get to grips with the whole business of unsolicited text messages. The point of all this is to illustrate just how easy it is to use technology to track our every move and it's being done on the internet.

Crumbling cookies

Cookies – those little text files that accumulate in your Temporary Internet Files folder – are used by almost every website you visit. The humble cookie has suffered from a bad press over the years – much of it unjustified.

A cookie is simply an HTTP (hypertext transfer protocol) header that consists of a text-only string that gets entered into the memory of a browser. This string contains the domain name, path, lifetime and value of a variable that a website sets. If the lifetime of this variable is longer than the time the user spends at that site, then this string is saved to file for future reference.

So far so good, but what does it do? A cookie can do many things, but what it can't do is transmit a virus or send private information from your hard drive to a third party. It's a text file and, as such, is incapable of action.

Every move you make

US Senator John Edwards introduced legislation in October 2000 that would force software manufacturers to notify consumers when their products include spyware. Under the Spyware Control and Privacy Protection Act, manufacturers that build spyware into their products must give consumers clear and conspicuous notice at the time of installation that the software contains spyware. Such a notice would describe what information would be collected and to whom it would be sent. The spyware would then be forced to lie dormant unless the consumer chooses to enable it.

Balanced information

It's easy to become paranoid in such circumstances and, if you allow it to happen, you'll soon be swamped in a tide of suspicion and doubt. The internet is a reflection of society, and is no better or no worse than any other arena when it comes to malpractice and plain dishonesty.

Oddly enough, there are some people who like to spend their day trying to find other people's computers that are open to them – and without proper safeguards any computer is wide open. The intruder will gain access to all the data stored on your computer and can delete, copy or edit any file you have. Once access is gained, the intruder can run various applications on your computer. They even attack other systems, making it look like you were the attacker.

Coming at you from every angle

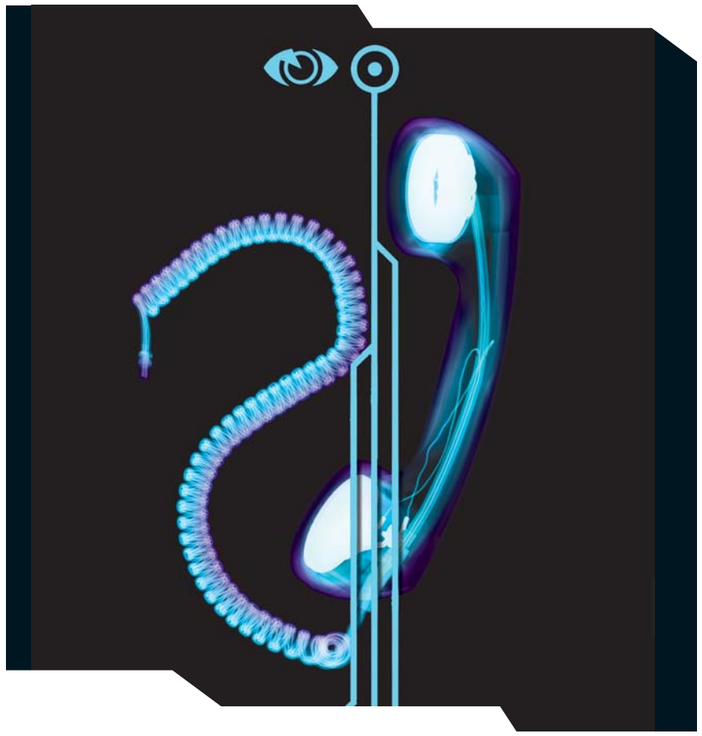
There are several ways your computer can be made vulnerable: Trojan horses, security holes in your software, harmful data streams and weaknesses in your operating system (NetBios settings).

A Trojan horse, like the Greek 'gift' to Troy, looks like a useful and innocent program but actually contains a means of attacking your system. A Trojan allows an attacker to perform almost the same actions on an infected computer as its owner. They can copy, view and delete information from the hard drive, run applications, change configuration settings, control the infected computer's hardware and much more. Once a cracker gains access to a system, all manner of maliciousness is possible. But the threat can also come from your own system.

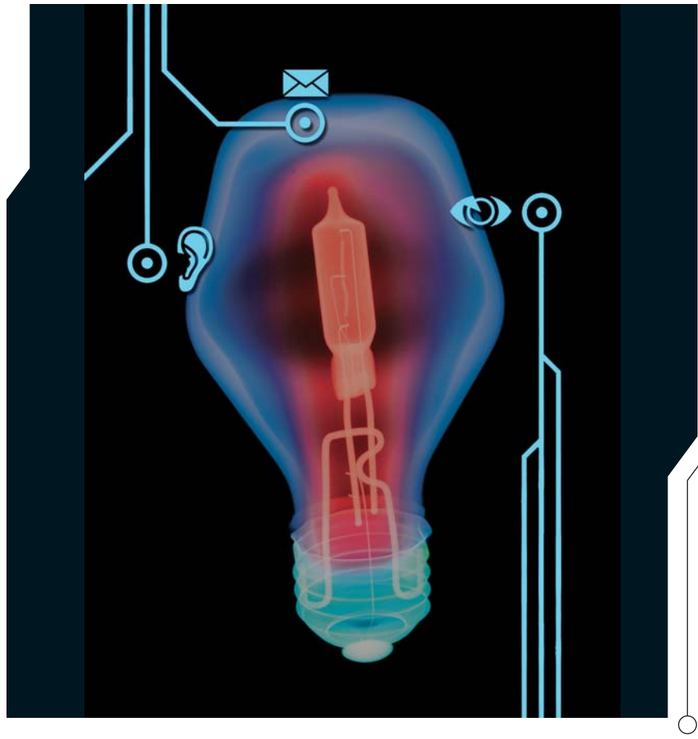
Some internet applications, such as browsers and internet pagers, have security holes that can be taken advantage of by attackers to access data stored on your hard drive. Depending on your application configurations, your computer can distribute confidential information about your system and your online operations.

Another threat comes from software that attackers use to send harmful data streams designed to disrupt your system and impair its efficiency on the internet. A computer receiving this data through its different ports might lose control and hang. Beyond the bother of having to reboot your computer, current downloads are lost, phone calls are interrupted and so on.

Finally, attackers can take advantage of the free and open access made available by how your operation system is configured. For example, if your computer uses Microsoft Windows its NetBios settings can be set so your files are made available to attackers.



The internet is a reflection of society, and is no better or no worse than any other arena when it comes to malpractice and plain dishonesty



Once access is gained [to your PC] the intruder can run various applications on your computer and even attack other systems making it look like you were the attacker

Better practice

Antiviral and firewall software will perform part of the task of keeping intruders away from your data, but it's the snoops you inadvertently invite on to your desktop you need to be proactive in repelling.

First, uninstall any programs you don't use and check any you do use against an online spyware database such as www.spychecker.com or download Spy Chaser from http://camtech2000.net/pages/spychaser.html. Downloaded software often contains spyware of some description. Uninstalling this and buying the full version will often give you the option of not installing those specific components.

Relatively well-known anti-spyware programs such as Lavasoft's AdAware 5.83 (www.lavasoft.nu) and OptOut (http://grc.com/optout.htm) can be downloaded and used to scan your hard drive, Registry and memory for malicious software and assist in its safe removal. However, as highlighted by readers in our online forum, AdAware itself has recently been targeted by those keen to propagate spyware. Users reported finding AdAware being uninstalled without their knowledge.

There are also one or two commercially available products such as Sunbelt's PestPatrol (www.sunbelt-software.com) that specialise in rooting out spyware while, on the flip side of the privacy and control debate, businesses can invest in products such as SpectorSoft's $99.95 Spector Pro 3.1 (www.spectorsoft.com). Such products go further than simply providing access to network-based email conversations – they can monitor every keystroke made (even deleted characters), providing records of web-based emails, instant message conversations and online chat.

Safety system

To safeguard your computer while online, it is not enough just to install protective software and improve your system configuration settings. To be secure you have to learn and practice the following fundamental safety procedures.

- Get the knowledge Learn the security policies of your ISP (internet service provider) and/or other respected sources.
- Be wary Do not open email attachments from anonymous or unknown sources.
- Be selective Do not download suspicious files from the internet and do not execute them on your computer.
- Don't be too trusting In a networking or workgroup situation only allow people you know and trust to use your computer.
- Set up security features Configure your web browser for safe internet operation. Have your browser ask or prompt you for confirmation each time it is offered a Java or ActiveX applet. Approve these only when you are visiting trusted sites.
- Protect yourself Purchase software to protect your computer, such as antivirus programs, anti-Trojan horse software and a decent personal firewall like Outpost, available as a free download from www.agnitum.com.

Do all of this and you'll be about as safe as it's possible to be in normal circumstances. There's no cast-iron guarantee but, with some common sense, you should be free to enjoy your computing without too much interference. ■