Guess Who's READING YOUR EMAIL?

It's legal, it's happening and these spies can wreck your life BY NICK MORGAN

STEVE FOWLER is the managing director of Universal Balancing, an international engineering company based in Bristol. In a field that uses cutting-edge technology, industrial espionage is a concern and a year ago the company installed a program called Spector 360 on most of their computers. The software, made by SpectorSoft, can track and block the websites a user tries to

visit and log his or her every keystroke. All Universal Balancing employees know that their desktop activity is open to scrutiny. Fowler reads reports of their PC use. If he feels something isn't right, he'll take a closer look.

"I can see screenshots of the pages they visit on the Internet," he says. "I can see what they're typing, when, and whether it's business-related or personal. The software can also block USB memory sticks and other portable media. So no one can bring anything, including viruses, into the company or take out sensitive information."

I T'S A FACT OF LIFE in the 21st-century workplace that the boss may be watching, especially if you use a computer. A 2006 survey by the Federation Against Software Theft found that three out of four companies regularly track the websites their employees visit. Other studies show that more than half use surveillance software to scour office email (looking for keywords such as "sex"). In the public sector alone, some 1,700 workers have been sacked or disciplined for Internet or email misuse in the last three years.

As the use of monitoring software grows, more of the activity that many of us consider innocent is getting caught in the net. Who hasn't opened an email to find a message from a friend passing on a funny YouTube clip, a racy joke or a link to a must-see blog? No big deal, right?

That's what staff at Swansea College

may have thought until 67 of them were investigated for "misuse of emails" in 2006—and six lost their jobs. Their crime? The college remains tight-lipped, but it appears to amount to little more than the sending of rude jokes and images from work computers. Because the college had a formal policy regarding the use of IT in the workplace, the staff had no viable defence.

THERE ARE PLENTY of valid reasons for companies to monitor their workers' computer use. Productivity is one. A survey last June by online price comparison company Foundem.com discovered that employees waste at least 90 minutes a day online sending personal emails, shopping, visiting social networking sites, paying bills, job-hunting, dating and looking at pornography. This tots up to 43 lost working days every year, at an annual cost to employers of £124 billion. It's not surprising that 50 per cent of HR professionals say they have encountered or had to discipline staff for time-wasting on the Internet.

Improper computer use can also cause legal trouble. Downloading pirated music, films or software on to a work computer infringes copyright and could result in a court case. Viewing pornography or sending sexually suggestive emails can lead to sexual harassment charges.

No business wants to end up like City law firm Charles Russell: in 2002 secretary Rachel Walker, who is black, handed in her notice, then saw an

email from solicitor Adam Dowdney to partner Clive Hopewell talking about her replacement. "Can we go for a real fit busty blonde this time? She can't be any more trouble and at least it would provide some entertainment!!" Hopewell replied, "I was about to say the same!" By committing their comments to email, the two lawyers had made a damning record and the firm settled before the case went to tribunal, reportedly paying Walker £10,000.

Security is another concern. For example, porn, gambling and gaming

data theft are memory sticks, MP3 players and emails.

"Over half the big companies in the UK are vulnerable to data theft," says Alyn Hockey, director of product management at Clearswift, a web security company whose clients include Britannia Building Society, AT&T and Marks & Spencer. Hockey recalls installing the company's MIMEsweeper system on the network of a vehicle manufacturer. The software quickly caught a junior designer trying to steal the concept designs for a new car. This

When bosses have access to every single email you write,
IT MUST BE TEMPTING SOMETIMES TO ACT LIKE BIG BROTHER

sites can harbour viruses and "malware", malicious programs that load on to a computer secretly and allow outsiders to damage a network or steal information.

Companies also have competitive reasons to keep tabs. Seventeen per cent of middle managers—and almost one in three departing directors— admit to having stolen confidential corporate information when they've left a job. The YouGov study carried out for IT company Hummingbird found that the favoured methods of

worker, Hockey says, had security clearance to see designs but when he tried to email them outside the company a virtual wall sprang up to block the action and an email was immediately sent to IT staff informing them that an illegal act had taken place.

It's not just industrial espionage that puts companies at risk. Sometimes workers leak sensitive information by accident. "It's good people doing stupid things," says Mark Murtagh, product director of Websense, another web-security firm that has worked

with Harvey Nichols and Everton Football Club.

One client, an international bank, had an employee who copied a large customer database off the secure central server and put it on to his individual work laptop. This database included thousands of records detailing customers' personal information including amounts held in accounts and other identifiable information.

This was a security breach in its own right—but he then downloaded a piece of peer-to-peer (file sharing) software. This was accidentally configured to share everything on his computer with everyone on the Internet. Fortunately Websense software picked up the incident, stopping the data being made available online to millions.

Companies are using two types of spying software: network-based programs that monitor all traffic passing through a system and programs that sit directly on an employee's desktop.

Clearswift's MIMEsweeper is an example of the first type. The software can search all correspondence for any sign that employees are accidentally or maliciously communicating sensitive data and block it. MIMEsweeper also claims it can examine the tone of an email to detect job dissatisfaction. Someone who sends a message saying "I hate my job" or "You're not going to believe what my idiot boss did today" could be poised to upload company files in anticipation of leaving the job.

US company Vericept makes products to monitor other web activities too. Paul Pilotte, a senior product manager at the company, says Vericept Protect helped one client fend off a harassment suit filed by a senior employee who claimed someone had left printouts from an adult website in her office. The company planned to give her a large severance package until it used the Vericept tool to examine her Web use. That search, Pilotte says, found that the employee had printed the pages herself. On another occasion, Vericept helped catch a worker who had installed a keylogger on a manager's computer to extract passwords.

One product that monitors an individual desktop is eBlaster. It can record everything a person types, from bank passwords to the names of illnesses searched on NHS Direct. It also logs and monitors emails sent and received (including those in personal Yahoo!, Hotmail and Gmail accounts), instant-message chats and the names of documents opened or printed.

Andrew Parker, IT manager for Waring and Netts, an architectural design and management company with offices in Leeds and Newcastle, uses Omniquad Mailwall Remote for their email system. He says, "When anybody in the company sends an email, it goes through a system that checks for inappropriate content and malware, then archives the email. No one needs to sit there reading emails, but employees know that everything they send is being filtered and monitored."

Most big companies are like Waring

The Future of
EMPLOYER SNOOPING

Some companies are going beyond the desktop to monitor their employees.

Radio frequency ID chips in swipe cards serve the same function as time-clock punching-in cards, allowing employers to know when workers enter or leave the office and even track their movements inside a building—letting your boss know, say, how much time you take for a cigarette break. One downside: cards can be lost or used by colleagues. In 2006 CityWatcher.com, a video-surveillance firm, dealt with that flaw by implanting RFID chips in the arms of willing workers authorised to enter a secure room holding US government surveillance videos.

Mobile phones can serve a similar function outside the office, transmitting signals that alert supervisors when a worker leaves a particular building and mapping his or her movements on a computer screen. Using a mobile phone to draw a map of someone's movements is easy and affordable. TrackaMobile.net runs a system that costs as little as 25p a search.

Geofencing technology produced by a company called Xora can be incorporated into mobile phones. Once installed, it can send email alerts when an employee, for example, loiters too long in one place. Employers can also designate specific areas—bars, sports venues, home addresses—as off-limits during work hours. Phones can then send an alert if a worker strays into the prohibited locations.

Biometric devices, such as fingerprint readers, were the stuff of futuristic spy thrillers 20 years ago. Now they're increasingly deployed by private companies and government agencies to control building access. Scans of workers' fingerprints, irises or retinas can be used in conjunction with, or in place of, electronic badges. US company Wasp Barcode Technologies makes a biometric attendance-tracking system that requires all employees to place a finger on an electronic reader instead of punching in with a time card. It prevents a worker who's bunking off from getting a friend to clock in for him. Unlike the RFID chip in an electronic ID badge, a biometric marker can't generally be tampered with.
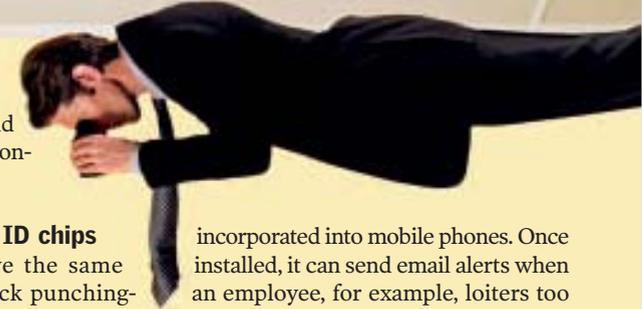
and Netts: they monitor overall email traffic and only target a worker if a problem pops up. But when bosses have access to every single email you write it must be tempting, sometimes, to play Big Brother.

That is what happened at Carmarthenshire College in West Wales, following a "clash of personalities" between PA Lynette Copland and her boss, the deputy principal. Over an 18-month period Copland was monitored extensively. "The surveillance became apparent when staff at the college contacted my stepdaughter to ask about our relationship," she says. "I found out that my phone calls, emails, visits to other campuses were being monitored. It seemed my boss was looking for a chance to undermine me. It was a totally soul-destroying experience."

Copland took her case to the European Court of Human Rights, arguing that she had a reasonable expectation of privacy at work. She won and last April was awarded over £6,000. She has since returned to her job.

"The crucial aspect was that the college did not have a specific policy about monitoring communications," says Ben Doherty, a solicitor with e-policy specialists Pinsent Masons. "So it was reasonable for employees to believe that their personal communications would be private."

The case is a warning to other British companies, many of whom are still not communicating their computer policies adequately.

"The laws surrounding surveillance at work are complex," points out Dr Kirstie Ball, who lectures in surveillance at the Open University Business School. "Yet this latticework of regulation does provide workers with certain rights and protection. Under Britain's data protection laws, if an organisation wants to monitor its staff for productivity, it must at least inform them that they're being watched."

THIS PROTECTION doesn't apply, however, to Britain's army of bloggers, some of whom are learning the hard way that what they say about employers on websites can have consequences.

Tom Beech, 20, from Wokingham, Berkshire, found out last August that he and his mates weren't the only ones visiting Facebook. "I'd had a really bad day and was feeling overworked and underpaid," he says. "My mistake was to complain about it on Facebook." He started a group called "I work at Argos and can't wait to leave because it's s**t." He was suspended, then sacked for gross misconduct.

Freedom of speech does not ensure job security, as blogger Emma Clarke, a freelance voice artist, found. Clarke is heard by millions of London Tube commuters each day, warning them to "mind the gap". She used her website to publish a series of spoof announcements, which included: "Here we are crammed again into a sweaty Tube carriage. If you are female, smile at the bloke next to you and make his day. He's probably not had sex for months." When her words hit the headlines last November, Transport for London made their own brief announcement: Clarke would not be working with them again.

And with one in five employers now using the Internet to check the "online footprint" of job applicants, Peter Cunningham, UK and Ireland director of Viadeo, an online network for business professionals, adds this warning: "If you've written a blog or posted information on a website revealing company information or criticising your boss, any new employer will think twice before taking you on."

In short, as Ben Doherty puts it, "Never write anything on a website that you are not prepared to shout across the room."

Do you think that Britons are the victims of too much surveillance? Email YouSaidIt@readersdigest.co.uk.

7 Rules **TO WORK BY**

Some simple tips for what to do—and not do—when using your work computer:

- Know your company's e-policy (computer-use policy) and comply with it.
- Assume you're being monitored and behave accordingly.
- Never criticise your company online.
- Don't use personal email accounts or post to a blog.
- Avoid sending any message that could embarrass you or others if made public.
- Don't think instant messaging is less permanent than email.
- When surfing the Web, never click on anything flagged NSFW (not safe for work).

HONEY, I STOLE SOMEONE ELSE'S KID

An elderly man sent to school to collect his four-year-old grandson came home with the wrong boy.

The unnamed 77-year-old picked up little Zacari Gillis from Long Branch primary school in Florida and cycled several miles home with him perched on his handlebars.

The mistake was finally detected by the man's wife when he walked through the front door with the bewildered infant.

Zacari was eventually returned unscathed to a frantic aunt waiting at the school gates and exchanged for the correct child.