Watching You

Tim Lyddiatt

Governments desperate to win the wars against terror and crime are turning to technology to keep an eye on what's going on; when does their all seeing eye become too much for us to bear?

They're watching you. With their cameras and their computers, they are keeping an electronic eye on everything that you do: where you go, who you meet and what you say. Increasingly, those with the power to unleash such surveillance are doing so more and more and all around the world, governments, police and security forces are harnessing technology to keep an ever more powerful eye on everything that is going on. For governments, the temptation must be huge: suddenly in possession of tools to monitor practically everything, at all times, it must be hard to resist the urge and not do so. The possibilities are just too great, and the consequence of missing something often too dire to contemplate.

A US border agent watches video monitors of cameras placed along the US and Canada border at the American border crossing at Sweetgrass

The justification for spending the billions needed to introduce surveillance technology is always the same. It is to fight crime, to prevent terrorism, to ensure that the majority are unaffected by the actions of the few. In the UK, there are more CCTV cameras per capita than anywhere else on earth and were installed to help combat crimes ranging from parking offences and keeping bus lanes clear to the kinds of violence that often erupts in city centres. Their installation was also designed to instil a sense of security in the areas where they are placed – with someone watching, it is said, people are less likely to commit an offence. It is estimated that in an average day, the vast majority of UK citizens, those living in urban areas, are caught on camera hundreds of times a day. Even in the countryside, where there are fewer cameras, traffic is monitored with CCTV to catch those speeding through villages and cameras are installed as a preventative measure against vandalism or antisocial behaviour.

The other main justification for so many cameras being installed is that, even if they have not served as a preventative measure, they can help prosecutors in gaining convictions by providing evidence of crime. If a picture paints a thousand words, then a picture accompanied by a sound recording of the area being watched, and the ability to zoom in and pan around a subject, as is afforded by modern CCTV networks, surely paints many thousands more. At political demonstrations, police use still and video cameras in order to build databases of the people that regularly protest against anything from the war in Iraq to climate change and the new runway at Heathrow airport. Being caught on camera in the UK has become so common place that some are beginning to ask whether there is such a thing as privacy anymore.

Whilst the UK might be top of the CCTV ladder, it would be unwise to think that

CCTV is not being increasingly utilised by security forces the world over, or that CCTV is the only weapon in the UK – or any other country's – surveillance arsenal. In the aftermath of Iran's elections in June it was widely reported that government forces used advanced surveillance techniques to intercept mobile phone calls and text messages in an attempt to better disrupt the organisation of rallies and political protests. Perhaps as a result of this, and combined with the restrictions placed on local and international media in reporting the protests which prevented them from leaving their offices or hotels, the Iranian protests are said to have been organised and reported via social media.

Certainly, many western news organisations relied on messages sent via micro-blogging site, Twitter, and images posted to Flickr as their only means to tell the story. Just as in the terrorist attacks on Mumbai last year, these channels of information are viewed as both indispensible and with caution. Whilst they certainly provide the world with information that would otherwise be restricted by those that would seek to limit its flow, or is otherwise unobtainable – in Mumbai, people were sending tweets via their mobiles from inside the besieged hotels – the voracity and contextual significance of that information is harder to assess. Indeed, such is the immediacy of the medium that its use must be forever augmented against other sources in order to assess where in the emerging picture it fits at all.

Labourers walk under security cameras outside a shopping mall in Dubai

Internet communications are undoubtedly powerful tools. It is no coincident that it is only under a state of emergency – of war, or of coming under attack – that the president of the United States – should draft legislation ever be passed into law – could seize control of the Internet, preventing business and citizens from using it. Ethan Zuckerman, co-founder of the blogger advocacy group Global Voices Online, told the *MIT Review* at the time of the Iranian protests that "people inside Iran, blogging, Tweeting, and sharing photos are doing an amazing job of making this political movement visible to the world." Indeed, the conclusion that Anne-Marie Corley, author of the report in which Zuckerman is quoted, comes to is that, "social media is probably more important as a tool to share the protests with the rest of the world than it is as an organising tool on the ground."

As a result, it is unsurprising that governments should choose to use surveillance techniques online as well as keeping watch over the offline world. During the protests, the Iranian government chose to throttle Internet usage by slowing down connection speeds and limiting available bandwidth. They may have also used tools such as deep packet inspection in order to view the content of e-mails and other Internet communications. Indeed, there were reports of two women's rights campaigners who were confronted with transcripts of their Instant Messaging exchanges as justification for their arrest.

If Iran has beefed up its use of electronic surveillance then it is from China that it is learning its lessons. For years China has been the poster boy for online filtering, surveillance and censorship. The so called Great Firewall of China has a vivid and illustrious reputation for keeping messages found on the Internet in line with those of government. Indeed, the attraction of China's 1.3 billion people as a market to exploit has seen such technology sector giants as Microsoft, Yahoo and Google all earning themselves the dubious honour of having collaborated with the Chinese government and assisting them censor the Internet.

Internet users surf at a cyber cafe in Kuala Lumpur. Malaysia is considering setting up an Internet filter, similar to China's delayed "Green Dam" project, in a move the opposition said would stifle dissent and industry officials warned would hit investment.

The Chinese's most recent attempt to further strengthen the Great Firewall's integrity was the order made to install Green Dam Youth Escort software on every PC made in China and sold in the domestic market. According to the authorities, Green Dam was designed to protect young people from accessing pornography. *The Wall Street Journal* quoted a government official who described Green Dam as a means to, "construct a green, healthy and harmonious Internet environment, and prevent harmful information on the Internet from influencing and poisoning young people." At the same time, Internet privacy and free speech advocates are worried that Green Dam could easily be used to make it even more difficult for China's 300 million Internet users to obtain uncensored news and information. "This is a very bad thing," the chairman of the Hong Kong chapter of the Internet Society told the *New York Times*. "It's like downloading spyware onto your computer, but the government is the spy." As it transpired, Green Dam was not forced on to every PC manufactured in China for the domestic market; instead only computers used publically in schools, universities, libraries and Internet cafés – were legally required to install the software.

I was discussing all of this with a former network security expert at British Telecom. He let me finish, and then, quite matter-of-factly said: "Don't for a second think that it is only China and Iran that use electronic surveillance and monitor online communications." He told me that after 9/11, the British Home Office contacted his team – who were working on blocking access to child pornography online – "and asked us to block more than 5,000 websites they said were promoting terrorism." He declined their invitation to assist, citing the fact that the government cannot demand that content be taken down without a proper mandate, usually decided in court or in parliament. "If we had taken those sites down, it would have set a dangerous precedent of government interference in, and circumvention of, a legally defined system."

It would seem that the issue is not that of there being sufficient technology to monitor all electronic communication, but an ethical, legal one. This year, European law added all ISPs to all telecommunications companies in requiring them to log the date, time, duration and recipients of online communications. The content of such communications is not required to be recorded and kept under the terms of the legislation. Discussing similar legislation introduced in Bahrain recently, one senior telecoms insider told *Bahrain Telegraph:* "I have no issue complying with the legislation but the way it is constructed at the moment, both technically and in terms of legal phrasing, it allows government agencies to start monitoring my network without notifying me – and without leaving any trace of their having done so. To me that sets a worrying precedent."

A similar legal precedent has already been sidestepped in the US where warrantless wiretap investigations were carried out by members of the National Security Agency, often at the behest of then President George Bush. More recently, the same agency has been accused of intercepting and spying on millions of Americans' e-mails. Whilst some in the UK, US and across the world are concerned at such invasions of privacy, often they are defended in terms of 'protecting national security.' Indeed, after being accused of abusing his powers in the wiretapping controversy President Bush later claimed it was his "constitutional responsibility" to make the surveillance orders. In Britain too,

Image from CCTV video footage shows a suspected Pakistani militant aiming his weapon at a desk in Mumbai's Trident hotel

just as the justification for CCTV is to prevent crime or better execute the law by providing evidence, so the case for electronic surveillance is regularly made in terms of fighting the war on terror. It is within these terms, that many say that the rights of ordinary citizens are being eroded.

Earlier this year the Joseph Rowntree Reform Trust published the findings of two years of research made by the Foundation for Information Policy Research in to what it terms the 'Database State' of Great Britain. The report was commissioned after the dangers associated with compiling such extensive databases about ordinary people, and of not taking proper care of them, was vividly demonstrated. In October 2007 Her Majesty's Revenue and Customs lost two discs containing a copy of the entire child benefit database.

In the report's forward Joseph Rowntree Chair, David Shutt, explained that "the old line 'if you have nothing to hide, you have nothing to fear' was given a very public rebuttal. The millions of people affected by this data loss, who may have thought they had nothing to hide, were shown that they do have much to fear from the failures of the database state." The report's findings are damning.

"Of the 46 databases assessed only six are given the green light. That is, only six are found to have a proper legal basis for any privacy intrusions and are proportionate and necessary in a democratic society. Nearly twice as many are almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned, while the remaining 29 databases have significant problems and should be subject to an independent review."

Whilst it is undoubtedly true that electronic surveillance has prevented terrorist atrocities being perpetrated in the UK and elsewhere, it is also worth noting comments made by Detective Chief Inspector Mike Neville, head of Scotland Yard's Visual Images, Identifications and Detections Office about the role of CCTV in solving crime: "Cameras do not act as a deterrent as many criminals assume they are not working; only three per cent of London's street robberies had been solved using CCTV images."

The increased use of CCTV is almost certainly going to continue the world over, just as intelligence agencies will continue to find new ways to keep tabs on those that they suspect of criminal activity. I think that there is some truth in the old adage about 'having nothing to hide' but in this context – where such invasions of privacy having such limited results, when is the loss of privacy too big a price to have paid? In a world of electronic surveillance, how much is too much – and who decides when it is enough?