This is the published version:

Hirst, Martin 2013, Someone’s looking at you: welcome to the surveillance economy, *The Conversation*.

Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30060028

Reproduced with the kind permission of the copyright owner.

Copyright: 2013, Conversation Media Group
Someone’s looking at you: welcome to the surveillance economy

Martin Hirst
Associate Professor Journalism & Media at Deakin University

Big data has ushered in the surveillance economy: is it the price of doing business in the digital economy?

Image sourced from www.shutterstock.com

26 July 2013, 2.24pm AEST

Author

DEAKIN UNIVERSITY JOBS

Lecturer in Construction Management

More Jobs Where experts find jobs

Everything that fugitive whistle-blower Edward Snowden has revealed about America’s global espionage network PRISM should make you alert and alarmed. His expose shows that we are clearly living in a well-established surveillance society. But it also reveals more than that: surveillance is at the heart of the global digital economy too.

One document revealed that in 2001 the Australian telco, Telstra, signed an agreement to allow US spy agencies access to data about its American customers. However, according to the agreement, Telstra is not permitted to let other governments access the same data.

In response, Telstra issued a brief statement only saying that the agreement reflected its contractual obligations at the time and the revelation has received only limited media coverage.

The surveillance society

Everything you do is subject to surveillance. As Robert O’Harrow Jr explains it, there is “no place to hide”. We are under constant watch, both physically and electronically. Surveillance is the new normal. It’s everywhere and this ubiquity makes us take it for granted.

Under the circumstances, the old adage: “if you’ve done nothing wrong, you have nothing to fear” from the surveillance state no longer holds true.
This argument is predicated on the belief that beyond the limited function of protecting the public interest (say, through the police), the state is not interested in what you do, whom you talk to, where you go, what you buy, or what you believe in.

We no longer live in that world. The number of government agencies taking an interest in information about us has grown like topsy. The national security state has extended the policing functions of government to all areas of life.

Government welfare agencies have been caught spying on recipients; single mothers and pensioners. In the UK, education authorities followed a family in an effort to catch them fraudulently enrolling children “out of area”. In Australia, a local council accessed personal data about residents’ phone use to track down unregistered pets.

If you still harbour lingering doubts that we live in a total surveillance society, now is the time to get real and take a look outside.

We are under almost constant video surveillance. Try walking through any reasonable-sized town or city without being caught on CCTV. It is impossible; you can’t even duck in and out of shops, or use under-road pedestrian walkways. There are thousands of state-monitored cameras looking at traffic, public transport and pedestrian flows; thousands of private cameras are also monitoring every transaction we make in banks, shops, pubs, hotel lobbies, restaurants and supermarkets.

This footage is also available to the authorities. All they have to do is ask. In some cases, they don’t even have to ask. When police in Boston began the hunt for the marathon bombers, they sequestered surveillance tapes from the 200 businesses on Boylston Street. Tens of hundreds of civilians who had taken happy snaps of the event on their phones also volunteered the images.

You might argue that was a good use of “citizen journalism”, but there was also a dark side. In the information vacuum created by the lack of a clear suspect in the bombing, social media “netizens” took matters into their own hands. Within hours, amateur sleuths began posting images of swarthy young men with backpacks, suggesting they could be the bombers.

This is dangerous, particularly in a society with a strong vigilante culture. It was pure dumb luck that none of the wrongly implicated young men was physically targeted by angry mobs seeking revenge.

There’s another reason to be concerned. We don’t just have to contend with ubiquitous physical surveillance via thousands of CCTV installations. In the world of “big data” there is no escape. Our electronic fingerprints are being gathered around the clock and they are being stored, sorted, filtered, filed and manipulated. We are all potential targets for state surveillance.

A salient example in this case is the hundreds of people who might know Edward Snowden or have come into contact with him in the past two to three years. Anyone who ever exchanged an email or text message with Snowden is now caught up in a dragnet containing billions of bytes of information.

People who “have nothing to fear” are now on the intelligence community’s radar; just in case one innocuous message reveals a secret that can help the FBI capture Snowden. They could be caught up in this for many years, particularly if Snowden is returned to the USA to stand trial.
How wide will that net be cast? It is hard to tell, but the capabilities involved here mean that anyone with even six degrees of separation from the target can be digitally strip-searched.

The latest release of information from the Snowden cache is perhaps the most worrying, for it reveals the extent to which the digital economy and the surveillance state are symbiotically connected.

The surveillance economy

From documents released by Snowden it seems clear that many major hi-tech companies have been covertly cooperating with the US National Security Agency (NSA) to throw open our emails and video conversations, alongside anything we choose to store in the "cloud". Google, Microsoft and other companies have not denied that they are cooperating with the FBI, the NSA and other spy agencies. Their argument, like Telstra's, is that it is the price of doing business.

According to a Microsoft statement, the company has to comply with lawful requests from the security apparatus. The problem is that there is no public disclosure when such requests are made. They are classified and not subject to any scrutiny.

It also appears that encryption tools might be compromised. There really is no place to hide, even if you really don’t want to be found.

Microsoft says it only acts on court-ordered requests and has not released encryption keys. But analysts say this is only half the truth and Microsoft itself admits it is not allowed to divulge the other ways in which it cooperates with law enforcement and security agencies.

Surveillance is “big data” and big data is big business. The surveillance economy puts information transactions at its core and when the bottom is dropping out of the market for real goods and services, capitalism will adapt. The latest systemic adaptation is to embrace new ways of surveilling customers and then turning the collected data into something that someone else is willing to buy.

The value of big data has been compared to the oil boom or “panning for gold” in terms of potential profitability. The numbers are staggering: 50 billion devices connected to the Internet by the end of this decade; so much available data to be mined that it doesn't yet have a number to describe it. So many connections are available to be tapped, correlated, combed, combined and sold that any attempt to visualise the connections would look like a spaghetti junction map of the universe with every planet, star and comet connected to every other object. The value of this market is currently estimated at over A$39 billion annually and growing at around 9% per year according to analysts IDC.
How big data sees the world - everything can be put through the ‘analytics’.

www.cisco.com/web/about/ac79/docs/sp/Information-Infomediaries.pdf

Click to enlarge

Big data analytics (a polite way of talking about surveillance) is now central to the global economy. As more commercial data is collected, nervous and security conscious governments will find more ways of mining it for political purposes too.