

Embargo Tuesday 29 October 2002
Spy vs Spy: the science of surveillance and security
Session 7: 3.30pm Living (in)security – panel discussion



Position: Trust, Surveillance and Security
Dr John Weckert
Charles Sturt University

The Science Forums

The third dimension

The most common social issues raised in discussions of surveillance and security relate to personal privacy and personal freedoms.

While these are undoubtedly important, a third issue, less commonly mentioned, also deserves examination in this context, and that is trust. This will be the focus here.

Trust

The relationship between trust on the one hand, and surveillance and security on the other, is quite complex.

We will look briefly at three things:

- why trust is so important,
- the nature of the complexity, and finally
- what implications the complexity of this relationship has for surveillance and security.

Where there's trust...

There is little doubt that trust is important. A group, whether an organisation or a society, can achieve much more with it than without it. Things are more efficient where there is trust. Where there is lack of trust there must be surveillance and security.

Some talk of trust as social capital in this context. Others, Fukuyama for example, argue that costs incurred by police, lawyers and so on are "a direct tax imposed by the breakdown of trust in society." In addition to the organisational and societal benefits of trust, it plays a vital role in the important relationships of friendship and love.

Risk assessment?

The relationship is complex because of what trust is and what it is not.

Trust is often seen as being closely related to risk assessment. *A trusts B to do X* means something like *A has good reasons to believe that B will do X*. On this account, the relationship between trust and surveillance and security is quite simple. The more surveillance and security that there is, the better will be A's grounds for believing that B will do X, so the greater the trust.

But this cannot be right. Trust always involves risk, making oneself vulnerable to the actions of another, so where there is no risk or vulnerability there can be no trust.

It is better to see trust in this way: if person A trusts person B, then A has an attitude of trust toward B, or A takes a stance of trust toward B, or A sees B as someone who will, typically, do as he or she says, who is reliable, who will act with the interests of A in mind, and so on.

On this account surveillance and security have the potential, not to strengthen trust, but to destroy it, or at least, to leave no space for it.

The situation is not so simple of course. Sometimes surveillance and security are important for maintaining trust, and sometimes we may think that they are more important than trust.

Consider these cases. An employer continually keeps his or her employees under surveillance. They clearly do not trust them. There is no room for trust, and employees generally do not like not being trusted. Next, think of airline security. Here it enhances our trust in the safety of the aircraft. Finally, the security in a high security prison leaves no room for trust, but here issues of the safety of the community override issues of trust.

Embargo Tuesday 29 October 2002

Implications

What are the implications for the complexity of this relationship?

First, we shouldn't automatically think that surveillance and security always increase trust. Sometimes they do, but careful thought is required regarding their use. Once trust is lost it is difficult to regain.

Technologies that can be called blocking technologies such as locked front doors and firewalls, pose little threat for trust. While they do indeed indicate that we live in a world in which not all can be trusted, they help to create an environment in which "insiders" can interact in relative safety, and they therefore encourage trusting.

Surveillance technologies however, are potentially trust inhibiting. These can be, and often are legitimate security tools, but their use can help cause a breakdown in trust. Such technologies need to be used with extreme care. A useful rule of thumb might be to use them in response to a known or suspected problem, rather than merely to see what people are doing. But even this needs qualification. Randomly monitoring employees in the workplace should be avoided, but there may be strong justification for so doing in an airport or bank.

For a society to operate efficiently, trust is important. Trust, properly understood, is not necessarily diminished by judicious surveillance and security, but there is a danger that it will be. And once trust is lost, it is very difficult to regain. It is important that further research is conducted to help our understanding of how much surveillance and security trust can withstand.

Profile

Dr John Weckert is Associate Professor of Information Technology in the School of Information Studies, and Principal Research Fellow in the Centre for Applied Philosophy and Public Ethics (CAPPE), an Australian Research Council funded Special Research Centre, at Charles Sturt University.

He is manager of the CAPPE Computer Ethics Programme, and the Australian Computer Society (ACS) representative on the Technical Committee on Computers and Society of the International Federation for Information Processing (IFIP).

The Science Forums

UTS Faculty of Science

Project Manager: Mary Mulcahy 0439 448 861

Consultant: Jenny Eather 0417 207156

mary.mulcahy@uts.edu.au, jenny.eather@uts.edu.au

phone 61 + 2 + 9514 2249, fax 61 + 2 + 9514 9968