Trust, corruption, and surveillance in the electronic workplace

John Weckert

Centre for Applied Philosophy and Public Ethics, Charles Sturt University

Abstract: Trust is an important requirement in an efficient workplace. However, there are new possibilities for corruption in the electronic workplace, and also new opportunities for the monitoring and surveillance of employees. These possibilities and opportunities can work against the creation and maintenance of a workplace with a trusting environment. This paper explores some of the relevant issues in this tension.

Key words: trust, monitoring, surveillance, corruption, workplace

1. INTRODUCTION

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, filling out of documents and keeping of records, which is all largely unproductive work. Societies function better the more trust that there is, and without any trust could not function at all [11]. Colman and others talk of trust as social capital in this context:

Like other forms of capital, social capital is productive, making possible the achievement of certain ends that would not be attainable in its absence. ... For example, a group whose members manifest trustworthiness and place extensive trust in one another will be able to accomplish much more than a comparable group lacking that trustworthiness and trust [3, pp. 302, 304].

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35609-9_29](https://doi.org/10.1007/978-0-387-35609-9_29)

Fukuyama goes as far as to say that the cost of police, prisons, lawyers and so on are a tax on breakdown of trust [4, p. 11]. This is not to say that the value of trust is merely economic efficiency. Trust is clearly of central importance in personal relationships, and in general it would be said that it is just more pleasant to be in a trusting environment than in a non-trusting one. The point here is that it does have this efficiency aspect as well.

This trust is no less important in the workplace than in society in general. A workplace in which people can be, and are, trusted, has much more potential to be efficient and productive than one in which tasks are accomplished only through constant supervision.

In recent years the workplace has changed. Most are now heavily computerised, networked, and probably connected to the Internet. This has created many new opportunities for criminal and corrupt activities, as will be shown in the next section, and has enabled much more efficient monitoring and surveillance of employees.

Given the importance of trust on the one hand, and the changed conditions in the workplace on the other, there appears to be a tension that is more acute than previously. While there is a need to create and maintain a climate for trust, there is also a need to minimise opportunities for workplace crime and corruption. While this tension is of course not new, it has increased with the new opportunities for these activities together with the ease of checking on what employees are doing.

This paper is primarily analytic, and does not report any new empirical results, but the next section does draw heavily on an empirical study in which the author participated. That section discusses the new opportunities for workplace corruption, and the one following that presents an account of trust. In order to see whether or not the apparent tension is real, it is necessary both to know whether the opportunities for corruption have increased and to know what trust is. Attention then turns specifically to trust in the workplace.

2. NEW OPPORTUNITIES FOR CORRUPTION

Governments in Australia, along with their counterparts in other countries, are becoming more reliant on computer networks for their operations, including the storage and transfer of information, communication, and purchasing. In order to assess the potential for corruption in this electronic environment (called eCorruption here), the Independent Commission Against Corruption (ICAC) in the state of New South Wales (NSW) commissioned a report on vulnerabilities for eCorruption in the NSW public sector. This section is based on that report

[6]. While it reports on only public sector workplaces, there is no reason to think that anything is much different in the private sector.

In the move to computerisation and automation, entire organisations, and certainly the content and processes of individual jobs, have been reorganised. ... Tried and true methods of risk control (for example, double entry bookkeeping) have been supplanted. Many positions have been 'dumbed down' – that is, the skills and understanding needed to perform tasks have been reduced due to 'smart' software programs and 'intelligent' machines. Processes which once had several steps and therefore several check points are now completed instantaneously. Creation of large databases with networked access means that many more people in organisations have access to information which was previously difficult or time-consuming to find.

More specifically, a number of areas were identified that vulnerable to eCorruption. Some of these are:

- Databases – with large databases, and particularly with large scale data warehousing, a developing trend, a great deal of information can be discovered, altered or destroyed by anyone who gains access. And in the case where the databases are accessible through large networks, many more people can access them;
- Authentication – passwords are most commonly used for authentication, but they are notoriously unreliable. Apart from inherent problems associated with the relative ease of 'cracking' passwords, it was found that many people are extremely careless with their passwords, sharing them with others, and writing them in obvious places, even on the computer itself. This makes it relatively easy for someone to undertake some activity for which they have no authorisation and perhaps which is criminal;
- Outsourcing – some, but not all, of those interviewed considered that there were extra security risks associated with outsourcing, because it was more difficult to know who had access to information and to verify the legitimacy of that access. Others however argued that with strict contracts in place, the risks were no greater;
- Electronic payments – because of the relative ease with which payments can be made to illegitimate accounts, fraud is not uncommon;
- Premature technology – new technology introduced too quickly and systems developed quickly in order to have an on-line presence with minimum delay can result in inadequately tested software that has security flaws.

It was also noted in the report that in general, managers apart from IT managers, were perceived as being more concerned with functionality of

systems than with security. This of course increases the potential for eCorruption.

If the findings of the report are accurate, the potential for eCorruption in public sector workplaces is considerable – probably greater than the potential for corruption in previous workplaces. The risks can be minimised by increasing security, but it is here that the tension arises that was noted earlier. To what extent can security be increased without creating an environment unfavourable for trust? In order to see more clearly how this question might be answered, it is necessary to look more closely at the notion of trust itself.

3. TRUST

Many discussions of the value of trust, whether in the workplace, e-commerce, or society in general, assume that the concept is well understood. In fact, this is not so, and quite radically different accounts have been given. And what account is accepted is important for the argument of this paper. At one extreme are cognitive accounts. Here, trust is primarily a matter of beliefs and expectations about the trustworthiness of others. At the other extreme are non-cognitive accounts, where the emphasis is on attitudes and the like [1]. The more plausible position seems to be one that has elements of both the cognitive and the non-cognitive, and such an account will be presented shortly. But first it will be useful to eliminate the cognitive approach, given its initial attractiveness.

A purely cognitive account of trust turns out not to be plausible. Consider the account of Coleman, which is clearly cognitive:

... the elements confronting the potential trustor are nothing more or less than the considerations a rational actor applies in deciding whether to place a bet. ... The potential trustor must decide between not placing trust, in which case there is no change in his utility, and placing trust, in which case the expected utility relative to his current status is the potential gain times the chance of gain minus the potential loss times the chance of loss. A rational actor will place trust if the first product is greater than the second ...[3. p. 99].

Here extensive employee monitoring and surveillance actually enhances trust rather than causing problems for it. The more monitoring the greater the trust! This follows because beliefs and expectations about the employees' behaviour will justifiably be stronger. Monitoring maximises 'the potential gain times the chance of gain' and minimises 'the potential loss times the

chance of loss.' So monitoring is obviously the rational thing to do if the desire is to increase trust.

Cognitive accounts like this, however, will not withstand close scrutiny. While there is a cognitive element in trust, that cannot be all that it is. A child's trust in its parents surely cannot be explained in terms of belief alone. Young children are not capable of the right sorts of beliefs. And trust between friends is also not based on a careful weighing up of risks and benefits. There is also a paradox inherent in cognitive accounts of trust of the Coleman type [10]. Suppose that an employer, A, does not monitor B, her employee, on the assumption that if B is not doing her job properly, she will learn about it soon enough. This requires a reasonable level of trust on A's part. Suppose now that she does acquire monitoring equipment that gives her the capability to keep track of B's activities. Obviously the more that this equipment is used, the greater will be her certainty that B is carrying out her work properly. On cognitive account, her trust in B should be stronger the more that she monitors B's activities. But this is not so. The more that B is monitored, the less space there is for trusting her. The paradox inherent in a Coleman type cognitive account of trust is that the conditions which should make trust stronger, the monitoring, diminish it, and make it redundant. The more monitoring that there is, the less need there is for trust. In a situation of total monitoring, say a maximum security prison, trust disappears, or almost.

This problem can be highlighted too, by considering the situation from a slightly different angle. Suppose that the workplace had a completely secure computer network. What would such a network be like? It would be completely reliable, that is, there would be no breakdowns. All firewalls would be completely safe, so no intruders could ever get through. Encryption would be undecipherable without the appropriate keys, those keys would be safe, and authentication techniques would be foolproof. Would trust matter? It would, because while intruders would be kept out, there would be no guarantee that legitimate users were behaving properly. They could be practicing deceit, stealing information and so on. Suppose that there was a perfect system of monitoring. All activity is logged, and all inappropriate behaviour punished. Everything that all insiders do is monitored, so there is no chance that they can do anything undetected. Is trust required now? Some is. While it may not be necessary to trust the general users, the employees, simply because they are not in a position to misbehave, those undertaking the monitoring and surveillance must still be trusted to do the right thing. Perhaps they are monitored too, but that just moves the trust to another level, and so on *ad infinitum*. This regress can perhaps be avoided by automating the monitoring. When anything untoward is noticed, the perpetrator will automatically be punished in some way, and their deeds made public. In

such a system perhaps trust would not be necessary within the system, but it would still be necessary to trust the developers and maintainers of the monitoring system. Is it implemented in a manner that is fair, or does it favour certain people? But even if such a system were fair, would anyone really want to work in a workplace with this kind of environment? Probably not. It seems to be a very high price to pay to avoid the need to trust other human beings. The system would have modelled a very efficient police state. So either we head toward a police state system, or we try develop and maintain trust and trustworthy behaviour in the workplace.

Trust then, cannot be purely cognitive, that is, it cannot be simply a matter of beliefs and expectations, or weighing up risks and benefits. The account of trust proposed in this paper is similar to that of Jones [7]. If person A trusts person B, then A has an attitude of trust toward B, or A takes a stance of trust toward B: A *sees* B's behaviour *as* being trustworthy. In order not to beg any questions, it can be said that 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. For the sake of brevity however, we will talk of A's seeing B as someone trustworthy.

Trust now resembles a Kuhnian paradigm [8]. While not wanting to push this analogy too far, this approach does highlight some of the important features of trust, in particular the intertwining of the attitudinal and the cognitive, and the robustness of trust. Trust also contains an element of commitment which is often overlooked, although many writers talk about the risk and uncertainty aspects. While these and other features are not incompatible with accounts couched in terms of attitude of stance, the seeing as approach does make them more obvious.

According to Roberts, emotions can be described in terms of seeing as, and it is his sense of seeing as which is central here. When we see something as, we construe it in a certain way. Speaking of Wittgenstein's duck-rabbit example, he writes:

Just as seeing the duck-rabbit as a duck is not merely knowing that it can be seen as a duck, nor merely judging that it can be so seen, but is construing it as such,... Construing seems to involve dwelling on or attending to, or at a minimum holding onto, some aspect, ...It seems to mean bringing some perceived paradigm, ... *to bear* [13, p. 187].

If A sees B as trustworthy, he construes him as trustworthy, which is not just believing or expecting him to be trustworthy. There is little doubt that I can see someone in that way without having any explicit beliefs at all about the matter. In fact, we do not normally think about trust too much, or someone's trustworthiness, except when we have been disappointed, or let

down. This is similar to Kuhn's view that normal science is conducted within an unquestioned paradigm.

One feature of trust which this model does challenge but which seems to be commonly held, is that while trust is difficult to build it is rather fragile and easy to demolish. Trust can certainly be difficult to build, but it is not so obviously fragile. This view of the fragility of trust seems to be based on something like a Popperian falsificationist view of science, which says that while a theory cannot be verified, it is falsified by one incompatible observation. The situation in science is not as simple as that, but with respect to trust, the idea that being let down once diminishes it seems to get support from Descartes' claim in the *Meditations*, that it is wise not to place too much trust in something that has deceived us. It is probably true that if I know that A has deceived me in a situation in which I trusted him, my trust will be weakened or perhaps lost. But most cases are not like this. When expectations are not met, when it appears that I have been let down, it is not always the case, and probably is not usually, that deceit is involved. Suppose that I trust A to do X but that he fails to do it. It is not likely that I will immediately cease trusting him on the basis of that one, or even a few, lapses of this kind, unless, of course, I do suspect deceit. There could be any number of reasons why A did not do X. It might have been because of a misunderstanding between us and he did not know that I expected him to do it. Unknown to me, he might have had good reasons for not doing X, but reasons such that if I did know of them I would approve of his not doing it. One does *not* immediately see someone's behaviour as being untrustworthy. Just as in science where, if there is incompatibility between an observation and a theory, there is more than one way to explain the incoherence, so there is also in the case of trust. One need not reject a theory, or the trust, outright. Lakatos' "protective belt" [9] and Quine's *maxim of minimum mutilation* [12] are relevant here. Our important beliefs and attitudes are affected least, or mutilated least, if we find some explanation which does not involve rejecting trust.

This account does cohere with the way things actually are. One does not lose one's trust in someone or even in a government merely on the basis of one or two lapses, any more than one begins to trust in a situation where there is mistrust, just because of one or two apparently trustworthy actions.

There will always be some risk and uncertainty associated with trust. If A trusts B then A takes some risk with respect to B, and in a sense, the greater the trust, the greater the risk. I risk a lot more in a loving relationship than I do in a casual friendship. The commitment is greater so there is much more at stake. The *seeing as* account of trust accommodates this, as can be seen in the following discussion of reasonable trust.

If “A trusts B” is cashed in terms of “A sees B as trustworthy,” then the reasonableness of trust must be spelt out in terms of the reasonableness of the *seeing as*. A’s seeing B as trustworthy is reasonable to the extent that A’s seeing B in this way gives a coherent account of B’s behaviour. On this view, a few cases of possibly untrustworthy behaviour will not count against the reasonableness of the overall trust. They can be counted as just anomalies to be explained away. A will try to ‘minimally mutilate’ his view of B. If there are too many anomalies, of course, such a stance becomes no longer viable. This is similar to Kuhn’s view of paradigm change in science. Where the threshold is will vary, depending on the strength of the trust. Where the trust is very strong, say the trust in a parent, the trust “paradigm” will be very resistant to challenge. Too much is at stake. Where the trust is less, there will be a correspondingly weaker resistance to change.

On this account, where trust is lost, there will be something like a “gestalt switch.” After the switch, A will see B as untrustworthy, and possibly trustworthy actions will be interpreted as anomalies, and explained away.

Finally, something needs to be said about the application of this model. So far it has been applied to trust relationships between individuals only, but this requires qualification. Often we trust a person in some respect but not in others. Person A might trust B to bank A’s money, but not to stay sober at a party. Trust is frequently relative to contexts, but that is compatible with the *seeing as* model. A sees B as trustworthy in context C, but not necessarily in context D. This model of trust can also accommodate trust of institutions. For example, A sees the government as trustworthy, or A sees business X as trustworthy. Again, these could be relativised to particular contexts.

4. THE WORKPLACE

The focus of this paper was on the apparent tension in the workplace between trust on the one hand, and corrupt behaviour on the other. In the second section it was seen that there are increased possibilities for corruption, and in the following one an account of trust was developed that has implications for workplace practices. Clearly if there is excessive and intrusive monitoring and surveillance, there will be little or no room for trust. As seen previously, trust involves risk, and if there is no risk there can be no trust. Additionally, if employees are never in a position where they can behave corruptly, they cannot be seen as moral and reliable people who normally do the right thing. They do not have any real choice in the matter. In other words, they cannot be *seen as* trustworthy.

An obvious rejoinder here of course is that this lack of space for trust does not matter. Organisations, whether they be public sector departments or

private businesses, need to perform their functions efficiently, and minimise or eliminate poor work practices, and corrupt and criminal activities. Given the increased opportunities for eCorruption noted earlier, increased computer security, including monitoring and surveillance, may be a necessity. If this leaves no room for trust of employees, it is a price worth paying.

But the price can be quite high. As was seen earlier, Fukuyama, talking about trust in society in general, says that costs incurred by police, lawyers and so on are “a direct tax imposed by the breakdown of trust in society.” He continues

People who do not trust one another will end up cooperating only under a system of formal rules and regulations ... This legal apparatus, serving as a substitute for trust, entails what economists call “transaction costs.” Widespread distrust in a society, in other words, imposes a kind of tax on all forms of economic activity, a tax that high-trust societies do not have to pay [4, pp. 11, 27-27].

The situation in the workplace is not so different. The ICAC report, as was seen earlier, mentioned that public sector managers see functionality as more important than security, particularly “where budgets and deadlines are tight” [6, p. 9]. It is obvious that workplace costs are lower in situations where employees can be and are trusted.

While it might be assumed that electronic monitoring improves productivity and quality, a recent study by Stanton and Julian casts some doubt on this [14]. Their research suggests that monitored employees will do what they are told and nothing more. If they believe that quantity is being monitored they will concentrate on that at the expense of quality, and if think that it is quality that is being monitored, they will neglect quantity. They claim, in a report of their work, that their study shows how important trust is in the workplace, and that

The greater the use of employers’ monitoring and surveillance techniques, the greater the climate of mistrust within the organisation [5, p. 18].

All that any of this shows, of course, is that there is a high price to pay for a lack of trust. But it does not follow from this that employee monitoring and surveillance are never justified. They might still be justifiable if the risk of criminal or corrupt behaviour (or even terrorism) is too great. In such situations is trust in general necessarily diminished? And is computer security always in opposition to trust, in the sense that the more security the less space for trust?

Is trust necessarily diminished by workplace monitoring and surveillance? While this is not necessarily so, there is obviously a risk. On the *seeing as* account of trust, trust can withstand isolated instances of real or apparent untrustworthy behaviour. A trusting employer will not immediately

lose trust in employees in the face of isolated instances of apparent untoward behaviour. Conversely, employees will not necessarily immediately lose trust in their employer if they are monitored. Given that trust is robust, in a generally trusting workplace environment, trust can withstand some monitoring and surveillance and some untoward behaviour, but not too much. Once some threshold is reached, trust is lost, and then it is difficult to regain. This unfortunately gives no hints as to how much monitoring and surveillance will be accepted, but it does indicate an area that requires more empirical research.

The second question is whether computer security is necessarily a threat to trust. Different types of technologies can be distinguished. The purpose of authentication technologies is to ensure that people are who they say that they are. In the off-line world there are various and well established ways in which it is possible to authenticate someone. Commonly this is done merely by sight, or more formally by written signature. Many of the common authentication cues are not available on-line, and the relevant technologies are merely attempts to bring the on-line world more into line with the off-line in this respect [2]. Knowing who someone is, or at least having an idea of the sort of person someone is, is an important element of trust. While there is regularly trust of strangers, and there must be to have a trusting society, it is much more difficult to trust a shadowy figure who is unseen. Without reliable authentication, the on-line world is largely inhabited by these shadowy figures, so authentication technologies are necessary for trust on-line. Certainly it would be better if authentication were not required, and that people were always who they said they were, but alas, that is not the case! The point here thought, is that authentication does not eliminate the space for trust. Once someone is authenticated, that person must still be trusted.

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

Monitoring and surveillance technologies however, are potentially trust inhibiting, and this includes technologies for creating and checking audit trails. These can be, and often are legitimate security tools, but their use can help cause a breakdown in trust, as was noted earlier. 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 employees are doing.

5. CONCLUSION

For a workplace to reach its full potential, trust is important. On the other hand, the new computerised and networked workplace offers both additional opportunities for corrupt behaviour on the part of employees, and improved monitoring and surveillance capabilities for employers. The argument of this paper has been that trust, properly understood, is not necessarily diminished by judicious monitoring and surveillance, but that the danger exists that this will happen. 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 monitoring and surveillance workplace trust can withstand.

REFERENCES:

1. Becker, L. C. "Trust as noncognitive security about motives", *Ethics*, vol. 107, 1996, 43 - 61.
2. Clarke, Roger "Authentication: a sufficiently rich model to enable e-business", at <http://www.anu.edu.au/people/Roger.Clarke/EC/Trust.html>, 2001.
3. Colman, J. S. *Foundations of Social Theory*. Harvard University Press, Cambridge, Mass. 1990.
4. Fukuyama, Frances. *Trust: The Social Virtues and the Creation of Prosperity*. Penguin Books, London, 1995.
5. Graham-Rowe, Duncan. "No one likes a back-seat boss", *New Scientist*, 8 December, 2001, p. 18.
6. Independent Commission Against Corruption. *eCorruption: eCrime Vulnerabilities in the NSW Public Sector*, Summary Report, 2001.
7. Jones, K. "Trust as an affective attitude", *Ethics*, vol 107, pp. 4 – 25, 1996.
8. Kuhn, T. S. *The Structure of Scientific Revolutions*. second edition, University of Chicago Press, Chicago, 1970.
9. Lakatos, I. "Falsification and the methodology of scientific research programmes", in *Criticism and the Growth of Knowledge*. I. Lakatos, and A. Musgrave, Eds. Cambridge University Press, Cambridge, 1970, pp. 91 – 196.
10. Nissenbaum, Helen. "Can trust be secured online? A theoretical perspective", *Etica e Politica*, No. 2, December 1999, at <http://www.princeton.edu/~helen/>
11. Putnam, Robert D. *Making Democracy Work: Civic Traditions in Modern Italy*. Princeton University Press, Princeton, 1994.
12. Quine, W. V. *Philosophy of Logic*, Prentice-Hall, Englewood Cliffs, NJ. 1970.
13. Roberts, R. C. "What an emotion is: a sketch", *The Philosophical Review*, vol. XCVII, April 1988, 183 - 209.
14. Stanton, Jeffrey M. and Julian, Amanda L. "The impact of electronic monitoring on quality and quantity or performance", *Computers in Human Behavior*, 18 January, 2002, pp. 85-101.