1-1-2006

Using scenario planning in the evaluation of information security applications

Laura Perusco
University of Wollongong

Using scenario planning in the evaluation of information security applications

Abstract

This paper provides a broad overview of the scenario approach as it relates to the evaluation of location based services (LBS) technologies and their appl ication. A scenario is a plausible vision of the future, based around a particular technology or application and developed via a scenario planning methodology. The main worth of the scenario planning approach is that it allows an application to be evaluated in terms of potential social impacts as well as technical merit and commercial viability. A sample scenario is presented within the paper to illustrate how the scenario planning methodology can be used. This scenario is analysed via deconstruction to draw out major issues presented regarding the use of LBS. The major contribution of this paper is a demonstration of the merits of scenarios in evaluating new technologies.

Keywords

Using, scenario, planning, evaluation, information, security, applications

Disciplines

Physical Sciences and Mathematics

Publication Details

Perusco, L. (2006). Using scenario planning in the evaluation of information security applications. In K. Michael & M. G. Michael (Eds.), The First Workshop on the Social Implications of National Security: The Social Implications of Information Security Measures on Citizens and Business (pp. 105-117). Wollongong: University of Wollongong.

18/3/2005].
RFID Journal. 2005c, *RFID Journal – The World's RFID Authority* [Online]. Available URL: http://www.rfidjournal.com [Accessed 18/3/2005].
RFID News. 2005, *Radio-Frequency Identification Devices* [Online]. Available URL: http://www.rfidnews.com/ [Accessed 18/3/2005].
RFID Times. 2005. *RFID Times* [Online]. Available URL: http://rfidtimes.blogspot.com/ [Accessed 18/3/2005].
Rizoli. 2003, 'Where's the beef? Vt.'s Holstein Association tracks cattle with RFIDs in pilot program' [Online], *Mass High Tech*, Vol. 21, Iss. 9, p. 1. Available URL: http://proquest.umi.com.ezproxy. uow.edu.au:2048/pqdweb?index=0&did=303726401&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1113548978&clientId=20901 [Accessed 16/4/2005].
Semex. 2005, 'Morning, Noon and Night', *The Balance*, July, pp. 8-9.
Sensormatic. 1998, *Advantages of using RFID* [Online]. Available URL: www.sensormatic.com/smarteas. advantages.htm [Accessed 6/3/1999].
Sirit. n.d., *RFID* [Online]. Available URL: www.idsys.co.uk/english/intro_4.htm [Accessed 3/10/1997].
Texas Instruments. 2004, *Livestock ID* [Online]. Available URL: http://www.ti.com/tiris/docs/applications/ animal/livestock.shtml [Accessed 16/4/2005].
Victoria Department of Primary Industries – Agriculture and Food. 2005, *Your Guide to Victoria's Cattle Identification Legislation* [Online]. Available URL: http://www.dpi.vic.gov.au/dpi/nrenfa.nsf/9e58 661e880ba9e44a256c640023eb2e/ca73fdb4fb0e9046ca256fd400159214/$FILE/_h9p64ikp0a4j42826clh20chg60qg_.pdf [Accessed 22/10/2005].
Want, R. 2004, 'The Magic of RFID' [Online], *Queue*, October. Available URL: http://www.acmqueue. com/modules.php?name=Content&pa=showpage&pid=216 [Accessed 16/4/2005].
Williams, D. 2004, *RFID: Hot Technology with Wide-Ranging Applications* [Online]. Available URL: http://www.directionsmag.com/article.php?article_id=526&trv=1 [Accessed 19/3/2005].
Yoke-L. n.d., Yoke-L: The Bottom Line [Online]. Available URL: http://www.yokel.co.uk/bottom.htm [Accessed 16/4/2005].

7

Using scenario planning in the evaluation of information security applications

Laura Perusco
School of Information Technology and Computer Science, University of Wollongong

Abstract

This paper provides a broad overview of the scenario approach as it relates to the evaluation of location based services (LBS) technologies and their application. A scenario is a plausible vision of the future, based around a particular technology or application and developed via a scenario planning methodology. The main worth of the scenario planning approach is that it allows an application to be evaluated in terms of potential social impacts as well as technical merit and commercial viability. A sample scenario is presented within the paper to illustrate how the scenario planning methodology can be used. This scenario is analysed via deconstruction to draw out major issues presented regarding the use of LBS. The major contribution of this paper is a demonstration of the merits of scenarios in evaluating new technologies.

Keywords: scenarios, scenario planning, location-based services, evaluation methodology, social impacts

1 Introduction

This paper explains the use of scenarios and scenario planning methodologies as a tool in the evaluation and assessment of information security applications. It presents the specific example of a scenario that examines potential unintended effects of the widespread use of LBS.

In essence, a scenario is a narrative story. Though fictional, a good scenario is based on solid research and current technological capabilities. Developing a rich narrative around the potential uses of a technology creates a broad scope for exploring the social, ethical and legal implications of the technology. This paper looks at processes required to support the development and analysis of a cogent scenario, as well as the reasons for using scenarios when evaluating an information security system. A sample scenario is presented and analysed to illustrate the concepts described.

2 What is a scenario?

There is no single, authoritative definition of what a scenario is. The definition used in this paper is "[a]n internally consistent view of what the future might turn out to be" (Lindgren & Bandhold 2003, p. 21). A scenario is a narrative story that describes possible events in the future, however, to be plausible the events must be based on the past and emerge logically (Fazarkerley 2005, p. 79). Scenarios are designed to provide an overall picture of a possible future, and to describe this future in such a way that it is accessible to a layperson in the subject (Martino 2003, p. 722). Legal scenarios developed to demonstrate possible outcomes of a law (UTSCLC 2005, p. 3) are just one example of how scenarios are used by researchers. A major reason why a scenario approach is so useful to evaluating information security applications is that "new technologies cannot be analysed in isolation from their social context" (Weber 2002, p. 325).

Any credible scenario should aim to fulfil Godet's (2000, p. 11) requirements that a scenario be relevant, coherent and plausible all at the same time, as well as being transparent. In the sample scenario presented here, footnotes are used extensively to help meet the requirement of transparency.

As well as conforming to Godet's constraints for plausibility, the scenario must be interesting. Fazakerley (2005, p. 79) cites various authors (including van der Heijden, Fahey and Randall, and Lindgren and Bandhold) as saying that no matter what scenario planning methodology is used, the story "must be memorable, interesting and rich in information whilst being creative". In this context, the researcher must endeavour to generate an original story based around the information security application being evaluated, creating interest through plot and character development while maintaining a rigid adherence to the requirements of plausibility, coherency and transparency.

2.1 Why use scenarios?

The Roman philosopher Seneca said: "[t]here is no favourable wind for the man who knows not where he is going" (Godet 2000, p. 3). Information security applications are often closely linked to people's lives, as is the case with LBS, yet the potential social effects of such applications are often ignored or sidelined. LBS is a perfect example of an area where social and legal analysis has been severely lacking and certainly not proportionate to the rapid pace of technological development.

With this in mind, there is certainly merit in exploring the potential effects of new security technologies and applications before they occur. "[T]oday's process of transition allows us to perceive what we are losing and what we are gaining; this perception will become impossible the moment we fully embrace and feel fully at home in the new technologies" (Žižek 1999, pp.101-102). Scenarios enable this kind of social analysis.

It is also important for analysis of possible future implications to keep pace with technological development. As Michael and Michael (2005, p.22) highlight:

> Most alarming is the rate of change in technological capabilities without a commensurate and involved response from an informed community on what these changes actually "mean" in real and applied terms, not only for the present but also for the future.

This statement emphasises the need for "soft" analysis tools such as scenarios in conjunction with business cases and profit models. Anyone who is concerned about the possible implications of information security technologies should be able to access information about them. Potential issues involved with new commercially available technologies should be made available to a wide audience. Scenarios make complex issues readily accessible to citizens, making them comprehensible to the general public.

2.2 Limitations of scenario planning

The qualitative nature of scenario planning means that any scenario is unlikely to give a completely accurate prediction, but rather a plausible vision of how a particular information security application might affect society in the future. There are no concrete predictions or forecasts. However, at the same time, a quantitative methodology would not draw out the potential social and ethical issues from possible future uses of a technology.

In addition, the outcome of the scenario planning process is likely to be influenced by the scenario planning framework used. The one discussed here, TAIDA, is just one possible framework – there are others that may produce different results. Also, it is only viable to produce a limited number of scenarios, so countless others could conceivably exist.

Despite these limitations, scenarios can be exceedingly useful as a tool in the evaluation of information security applications. Perhaps the worth of scenario

planning is best expressed by Godet (2000, p. 3):

> Unfortunately, there are no statistics for the future, and often personal judgement is the only information available to deal with the unknown. It is, therefore, necessary to gather other people's opinions before forming one's own, and then to place bets in the form of subjective probabilities.

3 The process of scenario planning

Although scenarios are a useful tool, their development requires a specific scenario planning framework to be effective. Many such frameworks exist. The scenario in this paper was created using the first three steps of TAIDA (Lindgren & Bandhold 2003, p. 38) to guide and structure the process. TAIDA actually involves five steps, and though the last two (deciding and acting) were beyond the scope of this paper, they would certainly be useful in a practical evaluation.

According to Lindgren and Bandhold (2003), the first three steps of TAIDA are:

- *Tracking*: identifying aspects of the current situation and surroundings that may have an impact on the future under consideration (p. 47).
- *Analysing*: considering the possible future consequences of the aspects identified in the first stage (p. 39).
- *Imaging*: approaching possible changes intuitively to create a plausible future, "to create not only an intellectual understanding but also an emotional meaning" (p. 40).

Tracking has been performed by examining several existing precise LBS applications and reviewing literature pertaining to the possible future effects of LBS. The results of this process are largely presented within the actual scenario, with footnotes describing the bases for various aspects of the story. Analysing takes place in the background – the results of this step are not shown here other than as the grounding for the scenario. The results of the imaging step are presented as the scenario itself.

3.1 Scenarios as an evaluative tool

In light of the risk of attempting to evaluate information technology applications in isolation from social effects, scenarios become a very useful tool. The researcher can create a scenario depicting a plausible possible future where use of the application has become commonplace, using this vision to discuss potential societal impacts. A qualitative strategy such as this allows the complexities of the subject to be explored.

It is suggested here that scenario planning is one of three integrated approaches that may be used to explore the subject of possible social, ethical, legal and technological impacts of LBS. Although the data collection, scenario and analysis

complement should one another, each serves a different purpose and thus requires a different method.

The primary focus for research is a qualitative content analysis of relevant articles about the technical capabilities of LBS and their possible future effects, with a scenario being developed based on this information through scenario planning. This is followed by a discussion of the legal, ethical, social and technological implications arising from the scenario, drawn out by deconstruction. Figure 1 shows the different methodologies integrate to provide a solid analysis of potential future effects.

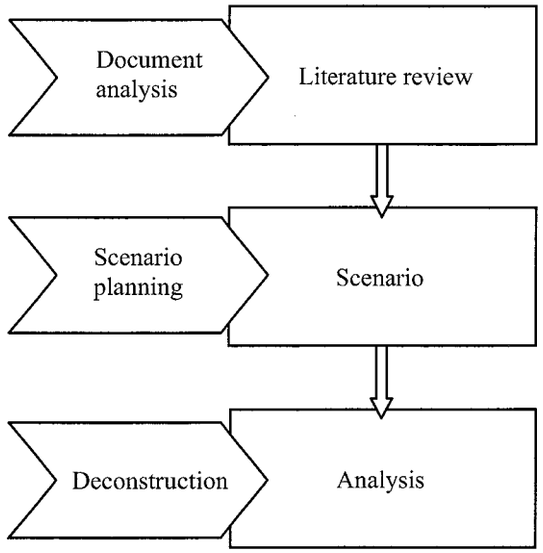

Figure 1: Relationship between methodologies used in developing and analysing a scenario

3.2 Analysing a scenario

It is proposed here that the most appropriate way to analyse a scenario is deconstruction. Deconstruction is an approach to literary analysis that aims "to create an interpretation of the setting or some feature of it to allow people ... to have a deeper understanding" (Feldman 1995, p. 1). The object is to draw out the meaning of the text through interpretation (Hogan 1996, p. 9).

Deconstruction as an analytical tool is usually used to expose the ideological limits of the author by looking at what is said, what is omitted, and how dichotomies are used to present a particular viewpoint (Feldman 1995, p. 51). However, in the case of scenario analysis, these techniques may be used to look at the underlying issues presented through the narrative. Implementation consists of examining events in the scenario and considering the issues that underpin those events as well as why these issues arise.

4 Prisoners without prisons: a sample scenario

'Hey Janet. Sorry I'm late.' Scott slid into the other seat at the table.

Janet sighed, pushing a latte and a sandwich towards him. She'd already finished her coffee. She gestured to her PDA. 'These gadgets do everything. They compare our schedules, pick a place convenient to both of us, make sure there's something vegetarian on the menu for me, and book a table.[1] Pity they can't get you here on time too.'

'I'm sure it's on the horizon,' Scott joked. 'So how's life in the Sydney office?'

'All right. The weather makes a nice change – I'm starting to get used to seeing sunshine in spring. How about your parolees?'

Scott laughed. 'There's a lot more of them. In Melbourne I had fifty or sixty cases at once. Now I've been allocated more than a hundred.' He bit into his sandwich. 'With less parole officers able to handle more cases, I guess I'm lucky to have a job,'[2] he continued with his mouth full.

Janet raised her eyebrows. 'With a lot of women intolerant of bad table manners, you're lucky to have a girlfriend. I assume the workloads are greater because they use those chips here?'

'The *caseload* is greater, the workload is the same – yeah, because of the chips.'[3] He smiled. 'It's crazy that NSW is already trialling these tracking implants,[4] while Victoria's only recently got a widespread implementation of the anklets. They've been around for years.

'The implants are much better,' Scott continued. 'Who wants a chunky anklet

1 This is similar to one of the scenarios that Lin, Yu and Shih use to illustrate the uses of pervasive commerce (p-commerce). One of their scenarios involves two people, John and Nancy, at different stores in a mall wanting to meet up for lunch. Their intelligent devices identify their locations and when they are likely to be ready, and present a list of nearby restaurants that could be reserved for lunch in 20 minutes [Lin, Lu and Shih 2005, p. 166]. This idea has been extended here to filtering restaurants by available menu selections.

2 There is strong competition for available parole officer positions with the Department of Corrective Services in NSW (Department of Education, Science and Training 2005).

3 Electronic monitoring may allow parole officers to take on more cases than was previously possible because some of their normal duties can be automated. However, it must be remembered that technology is merely a tool – electronic monitoring is not a substitute for parole officers (American Probation and Parole Association 1996).

4 The "tracking implants" referred to here are subdermal GPS-enabled personal locators – implantable GPS tracking devices. Although such technology is not currently available, it may not be far off. Applied Digital Solutions (the same company that developed the VeriChip) has announced a working prototype of this type of device. The prototype is quite large – about 5cm long and 1cm deep – but the company expects to be able to miniaturise the implant to the point where it is about the size of a grain of rice (Applied Digital Solutions 2003).

or bracelet that makes you look like collared freak? I'll bet it's really disconcerting having people stare at you suspiciously in the street, knowing that you're a criminal. It kind of defeats the purpose of parole – the idea is rehabilitation, reintegration under supervision. That's why the implants are so good – there's no stigma attached. No one can even tell you have one. And they're harder to remove, too.'

'I don't see what the big deal is,' Janet replied. 'Why not just keep people under lock and key?'

'Resources. It costs a lot to keep someone imprisoned, but the cost drops significantly if you imprison them in their own home instead.[5] It's about overcrowding, too – jails everywhere have had an overcrowding problem for years.[6]

'I also think electronic monitoring and parole are much better in terms of rehabilitation,' Scott went on. 'People can change.[7] Often they've committed a fairly minor crime,[8] then they go to prison, get mixed up with worse crowds. It can be pretty rough in there. There is certainly a danger that by imprisoning people with "harder" criminals, you run the risk of corrupting them further and exacerbating the problem.[9]

'On parole, they can still go to work and earn money, be productive members of society, get their lives back.[10] But they're watched, very closely – the tracking systems alert us if anything looks off. It's imprisonment without prisons.'

5 One NSW report stated that the daily cost of full-time imprisonment for one person was around $177 in maximum security, compared to $30 for home detention (NSWLRC 1996, p. 17). Using home detention rather than imprisonment equates to a saving per offender of $53,655 each year.

6 "Overcrowding is endemic to the Australian prison system ... Despite [a] significant number of new prisons built in the 1990s most Australian prison systems were operating above optimal capacity in 1998-99 and some like WA, SA and Qld were well above capacity" (Brown et al 2001, p. 1468).

7 "Parole is rooted in the fundamental belief that offenders can be motivated to make positive changes in their lives" (American Probation and Parole Association 2002).

8 A study of a two-year electronic monitoring trial program for parolees in the U.K. found that 89 percent of low-to-medium risk parolees completed their parole successfully. This was compared with 82 percent for medium-to-high risk parolees and 75 percent for high risk (Sugg, Moore and Howard 2001). When parole was first introduced to Australia in 1966, the element of risk inherent in such a system was recognised by the legislature. However, this was balanced against the same risks which are present when an offender is released into the community, unsupervised, at the end of his or her sentence. Parole seeks to limit community risk by promoting rehabilitation (Law Reform Commission NSW 1996).

9 Jails are often places where inmates learn more about crime than socially acceptable behaviour. Some prisoners are also vulnerable to brutalisation from other prisoners or even from prison officials. This can produce an embittered person who, upon release, goes on to commit far worse crimes than those for which they were originally incarcerated (Brown et al 2001, p. 1469).

10 Ostensibly, the main rationale for parole is the community benefit that stems from the rehabilitative effects of supervised, conditional early release. However, it seems apparent that at least part of the reason for parole is economic – the costs to the government and community of imprisonment are fairly obvious [Law Reform Commission NSW, above n 187]. One of the most significant advantages of parole and home imprisonment is that they allow the offender to work and pay taxes (and possibly even pay for their own monitoring costs), reducing the burden on the rest of society (National Law Enforcement and Corrections Technology Center 1999).

Janet gave him a sceptical look. 'So you're turfing people out of jails? How do you determine who gets paroled and who doesn't?'

'Well, a while ago it was mainly based on crime-related and demographic variables,' Scott replied. We're talking stuff like what sort of offence they're doing time for, the types of past convictions on their record, age, risk of reoffending.'[11]

Janet nodded.

'Now a bunch of other things are looked at too,' he continued, finishing off his sandwich. 'It's a lot more complex. Psychological factors play a big part. Even if someone displays fairly antisocial traits, they're still considered pretty low risk as long as they don't also show signs of mental illness.'[12]

'What about terrorists?' Janet argued. 'How can you guarantee that there won't be an incident in Australia like the London rail bombings?'

'Like I said, anyone considered really dangerous is still kept in a regular prison,' Scott said. 'And we'd be able to tell by location monitoring if a parolee was doing anything suspicious. There's no way a convicted terrorist would get anywhere near anything worth attacking.

'And you know that governmental powers now allow "persons of interest" to be implanted as well.[13] No one even remotely suspicious would be able to target a major landmark, business or tourist centre without alarm bells going off all over the place.'

Janet shook her head. 'I'm all for preventing terrorist attacks. But implanting people who haven't committed a crime? How far will they take it? What if the government decided that we should just track everyone, to be on the safe side?'

11 When considering whether or not to make a parole order, the NSW Parole Board is bound to consider a number of matters under s135(2) of the *Crimes (Administration of Sentences) Act 1999*. These issues include the offender's previous convictions, the offender's conduct in serving his or her sentence so far, and the likelihood that the offender will be able to adapt to normal community life. The Board must also consider reports prepared by or on behalf of the Crown in relation to the granting of parole (New South Wales Council for Civil Liberties 2003). It is assumed that such reports may take additional factors into account besides those listed in the *Crimes (Administration of Sentences) Act 1999*.

12 This idea comes from a paper about predictive models of inmate misbehaviour in institutions, but has been extrapolated to misbehaviour on parole (Lee and Edens 2005, pp. 412–414).

13 Australia's new anti-terrorism laws, among other things, allow people reasonably suspected of being involved in terrorism to be tracked and monitored for up to 12 months (Gilmore 2005). In a rather prophetic statement, Michael and Michael (2005, p. 25) state in their 'Microchipping People' article: "[i]f terrorism attacks continue to increase in frequency, there is a growing prospect of the use of chip implants for identification purposes and GPS for outdoor tracking and monitoring."

Scott shrugged. 'I guess we just need to find a nice balance between personal freedom and national security.'

He glanced at his watch and pushed his chair back. 'I need to get back to work,' he said apologetically.

5 Analysing the scenario

An analysis of the scenario above, *Prisoners Without Prisons*, reveals a number of important issues related to the use of LBS in enhancing national security. These include the ethical dilemma of using LBS to track suspected criminals, how LBS fit into society, and the momentum of LBS technologies. This section demonstrates how analysis of a scenario can be used to draw out such issues.

5.1 The ethics of pre-emptive control

Perhaps the most significant dilemma presented in *Prisoners Without Prisons* is the use of LBS technologies to monitor people such as those suspected of being involved in terrorist activities. As mentioned in the footnotes, this is not mere fancy – the Australian Government has enacted new anti-terrorism laws that, among other things, give police and security agencies the power to fit terror suspects with tracking devices for up to 12 months (Gilmore 2005).

This kind of power should give rise to concern. Can it be considered reasonable to impinge upon the freedom of someone who is merely suspected of committing a crime? For tracking implants especially, do governments have the right invade a personal space (i.e. a person's body) simply based on premise?

Criminals give up some of their normal rights by committing an offence. By going against society's laws, freedoms such as the right to liberty are forfeited. This is retributivism (i.e. "just deserts"). The central idea is proportionality: "punishment should be proportionate to the gravity of, and culpability involved in, the offence" (Brown et al 2001, p. 1376). With no crime involved, the punishment of electronic monitoring or home detention must be out of proportion.

This researcher does not make a judgement on whether pre-emptive control legislation is good or bad. It is suggested, however, that the laws recently proposed by the Federal Government (and agreed to by the States) could be indicative of a broader trend. Prime Minister John Howard said that "[i]n other circumstances I would never have sought these new powers. But we live in very dangerous and different and threatening circumstances ... I think all of these powers are needed" (Kerr 2005, p. 1). Could the same argument be used in the future to justify monitoring everyone in the country? Everyone's privacy being invaded in such a way would likely lower significantly the chance of crimes being committed, or

at least the chance of criminals remaining unpunished. If pre-emptive control is a part of government security, then widespread LBS monitoring could be the most effective form of implementation.

Without suggesting a far-fetched Orwellian scenario where draconian policies and laws mean that the entire population is tracked every moment of their lives, there is a possibility that the current climate is indicative of individuals' willingness to relinquish their privacy (or at least someone else's) for the sake of enhanced security.

5.2 The neutrality (or otherwise) of LBS technologies

There is a widely held belief that it is how people use a technology, not the technology itself, that can be characterised as either good or bad. People often see technology as neutral "in the sense that in itself it does not incorporate or imply any political or social values" (Lipscombe and Williams 1979, p. 19). The converse argument is that technology is not neutral because it requires the application of innovation and industry to some aspect of our lives that "needs" to be improved, and therefore must always have some social effect.

The uses of LBS presented in the scenario suggest that the technology itself is not neutral – that LBS are designed to exercise control. This may be control over one's own situation as presented at the beginning of the scenario, where Janet and Scott meet for lunch. Alternatively, it may be forced control over parolees and other criminals or suspected criminals. These situations imply that LBS is not neutral, and that the technology is designed to enhance control in various forms.

5.3 The technological momentum of LBS

Some believe that technology is the driving force that shapes the way we live. This theory is known as technological determinism, one of the basic tenets of which is that "changes in technology are the single most important source of change in society" (Winner 1977, p. 76). The idea is that technological forces contribute more to social change than even political, economic or environmental factors.

This researcher would not go so far as to subscribe to this strongest sense of technological determinism doctrine. The social setting in which the technology emerges is at least as important as the technology itself in determining how society is affected. As Braun says: "[t]he successful artefacts of technology are chosen by a social selection environment, [like] the success of living organisms is determined by a biological selection environment" (Braun 1995, p. 21). Technologies that fail to find a market never have a chance to change society, so society shapes technology at least as much as it is shaped by technology. In this light, Hughes's theory of technological momentum is a useful alternative to technological determinism: similar in that it is time-dependent and focuses on technology as a force of change, but sensitive to

the complexities of society and culture (Hughes 1994, 101).

Technological potential is not necessarily social destiny. However, in the case of LBS, it is plausible to expect it to create a shift in the way we live. We can already see this shift occurring in parents who monitor their children with LBS tracking devices, and in the easing of overcrowding in prisons through home imprisonment and parole programs using LBS monitoring.

As described previously, the threat of terrorist attacks has led the Australian Government to give itself extraordinary powers that never could have been justified previously. In this situation, LBS has enabled the electronic monitoring of suspicious persons, however, it is not the technology alone that acts as the impetus. Pre-emptive electronic tracking could not be put in place without LBS. Neither would it be tolerated without society believing that it is necessary in the current climate of unrest.

The scenario also demonstrates that technology and society evolve at least partially in tandem. Through the conversation between Scott and Janet, we learn that LBS tracking implants were not introduced simply because they were technically feasible. The reasons for their use were to reduce overcrowding in prisons and to mitigate the burden of criminals on the ordinary taxpayer. Social and economic factors, as well as technological ones, contributed to this measure being taken.

Although technology is not the sole factor in social change, and arguably not the most important, LBS are gaining momentum and are likely to contribute to a shift in the way we live. This can be seen both in the scenario and in real-life examples today.

6 Conclusion

This paper has presented an overview of scenarios as an evaluative tool. Although scenario planning has its limitations, it should certainly not be ignored entirely. It is important to consider social issues as well as technical problems when assessing an information security application. Scenario planning provides a framework for exploration. Although any particular scenario *per se* is unlikely to come true, it provides an example of what *could* happen if the technology is in widespread use, and gives ground for prevention or mitigation of potential undesirable effects. The scenario presented here illustrates how the technique can generate a plausible vision of how technologies may affect a particular situation. It must be kept in mind that a technology cannot be evaluated in isolation from its impact on society, and it has been demonstrated here that scenarios can be a very useful tool for analysis of such issues involved in a technology's application.

References

Applied Digital Solutions, *Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device* (2003) <http://adsx.com/news/2003/051303.html> [Accessed September 21, 2005].

American Probation and Parole Association, *Discretionary Parole* (2002) <http://www.appa-net.org/ about%20appa/discretionary_parole.htm> [Accessed September 25, 2005].

Braun, E., *Futile Progress: Technology's Empty Promise* (1995).

Brown, D., Farrier, D., Egger, S. and McNamara, L., *Criminal Laws* (3rd ed, 2001).

Department of Education, Science and Training, 'Probation Officer/Parole Officer – NSW/ACT', *Job Guide 2005* (2005) <http://jobguide.thegoodguides.com.au/statespecific.cfm?jobid=615&state_id= NSW> [Accessed September 24, 2005].

Fazakerley, V., *Critical Issues for the Future of the Australian Urban Water Supply Industry*, PhD thesis, Curtin University of Technology (2005).

Feldman, M.S., *Strategies for Interpreting Qualitative Data* (1995).

Gilmore, N., 'PM defends anti-terrorism laws', *Lateline* (September 8, 2005) <http://www.abc.net.au/ lateline/content/2005/s1456384.htm> [Accessed September 22, 2005].

Godet, M., 'The Art of Scenarios and Strategic Planning: Tools and Pitfalls', *Technological Forecasting and Social Change*, (Sep 2000) Vol. 65, Iss. 1, 3.

Hogan, P., *On Interpretation: Meaning and Inference in Law, Psychoanalysis, and Literature* (1996).

Hughes, T.P., 'Technological Momentum' in Smith, M.R. and Marx, L. (eds), *Does Technology Drive History?* (1994) 101.

Kerr, J., 'House arrest for terror suspects', *The Sydney Morning Herald* (September 28, 2005) 1.

Law Reform Commission NSW, 'Chapter 7: Parole' *Discussion Paper 33(1996) – Sentencing* (1996) <http://www.lawlink.nsw.gov.au/lrc.nsf/pages/DP33CHP7> [Accessed September 25, 2005].

Lee, S.J. and Edens, J.F., 'Exploring Predictors of Institutional Misbehavior among Male Korean Inmates', *Criminal Justice and Behaviour* (Aug. 2005) Vol. 32, No. 4, 412.

Lin, K.J., Yu, T. and Shih, C.Y., 'The Design of A Personal and Intelligent Pervasive-Commerce System Architecture', *Proceedings of the Second IEEE International Workshop on Mobile Commerce and Services* (2005).

Lindgren, M. and Bandhold, H., *Scenario Planning: The link between future and strategy* (2003).

Lipscombe, J. and Williams, B., *Are Science and Technology Neutral?* (1979).

Martino, J.P., 'A review of selected recent advances in technological forecasting', *Technological Forecasting and Social Change* (Oct 2003) Vol. 70, Iss. 8, 719.

Michael, K. and Michael, M.G., 'Microchipping People: The Rise of the Electrophorus', *Quadrant* (Mar 2005) Vol. 49, Iss. 3, 22.

National Law Enforcement and Corrections Technology Center, 'Keeping Track of Electronic Monitoring', *National Law Enforcement and Corrections Technology Center Bulletin* (Oct. 1999) <http://www.justnet.org/pdffiles/Elec-Monit.pdf> Accessed September 25, 2005].

New South Wales Council for Civil Liberties, *Parole, Sex Offenders and Rehabilitation Programs* (Feb. 2003) <http://www.nswccl.org.au/docs/pdf/Parole_SexOffenders_Note.pdf> [Accessed September 25, 2005].

NSWLRC, *NSWLRC Report 79: Sentencing* (1996).

Sugg, D., Moore, L. and Howard, P., 'Electronic monitoring and offending behaviour: reconviction results for the second year of trials of curfew orders' (2001) <http://www.probation.homeoffice.gov.uk/files/ pdf/r141[1].pdf> [Accessed September 24, 2005].

UTSCLC, *Be Informed: ASIO and Anti-Terrorism Laws* (February 2005) 3.

Weber, K.M., 'The Political Control of Large Socio-technical Systems: New Concepts and Empirical Applications from a Multidisciplinary Perspective' in Sørensen, K.H. and Williams, R. (eds) *Shaping Technology, Guiding Policy: Concepts, Spaces and Tools* (2002) 325.

Winner, L., *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (1977).

Žižek, S., 'Cyberspace, or the Unbearable Closure of Being' in Janet Bergstrom (ed), Endless Night: Cinema and Psychoanalysis, Parallel Histories (1999) 92.