March 2007

Control, trust, privacy, and security: evaluating location-based services

L. Perusco
University of Wollongong

Katina Michael
University of Wollongong, katina@uow.edu.au

Control, trust, privacy, and security: evaluating location-based services

Abstract

Location-based services (LBS) are those applications that utilize the position of an end-user, animal, or thing based on a given device (handheld, wearable, or implanted), for a particular purpose. This article uses scenario planning to identify the possible risks related to location-based services in the context of security and privacy. The original contribution of this article is that the dilemma has been related specifically to LBS, under the privacy-security dichotomy. Here, each side of the dichotomy is divided into three key components that combine to greatly magnify risk. Removing one or more components for each set decreases the privacy or security risk. Where more elements are present in conjunction, the risk is increased.

Disciplines

Physical Sciences and Mathematics

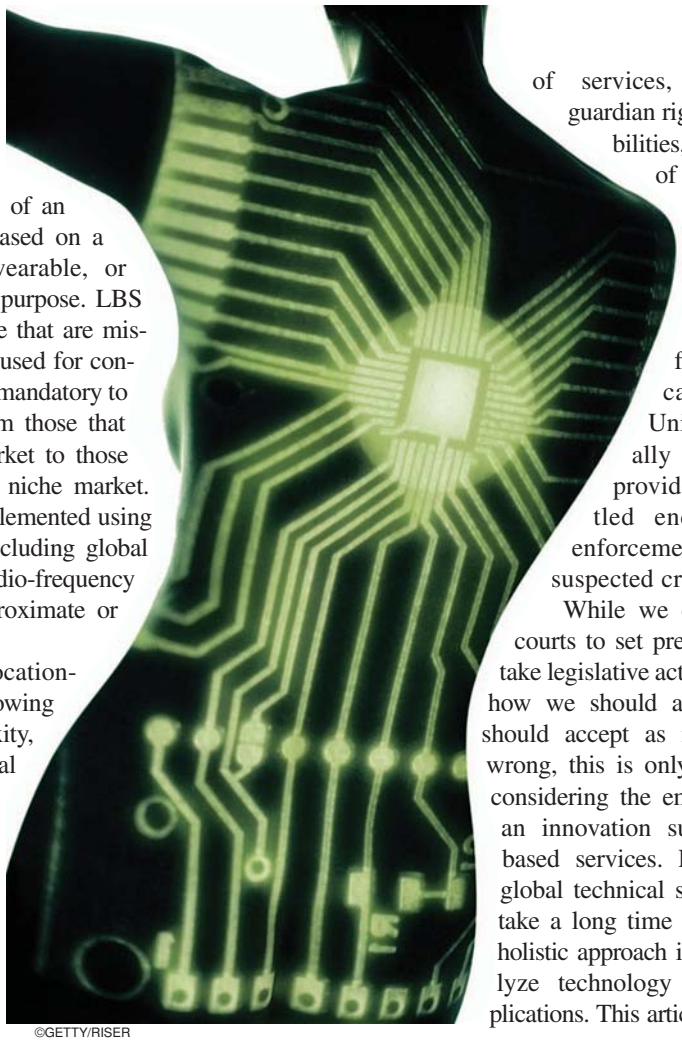
Publication Details

This article was originally published as: Perusco, L & Michael, K, Control, trust, privacy, and security: evaluating location-based services, IEEE Technology and Society Magazine, 2007, 26(1), 4-16. Copyright 2007 IEEE.

Control, Trust, Privacy, and Security:

Evaluating Location-Based Services

LAURA PERUSCO AND KATINA MICHAEL



©GETTY/RISER

Location-based services (LBS) are those applications that utilize the position of an end-user, animal, or thing based on a given device (handheld, wearable, or implanted), for a particular purpose. LBS applications range from those that are mission-critical to those that are used for convenience, from those that are mandatory to those that are voluntary, from those that are targeted at the mass market to those that cater to the needs of a niche market. Location services can be implemented using a variety of access media including global positioning systems and radio-frequency identification, rendering approximate or precise position details.

The introduction of location-based services, which are growing in sophistication and complexity, has brought with it a great deal of uncertainty. Unaddressed topics include: accountability for the accuracy and availability of location information, prioritization and location frequency reporting, the user's freedom to opt-in and opt-out of services, caregiver and guardian rights and responsibilities, the transparency of transactions, and the duration of location information storage. Some of these issues are the focus of court cases across the United States, usually between service providers and disgruntled end-users or law enforcement agencies and suspected criminals.

While we can wait for the courts to set precedents and then take legislative action to learn about how we should act and what we should accept as morally right or wrong, this is only a small part in considering the emerging ethics of an innovation such as location-based services. Laws, similar to global technical standards, usually take a long time to enact. A more holistic approach is required to analyze technology and social implications. This article uses scenarios,

in the form of short stories to summarize and draw out the likely issues that could arise from widespread adoption of LBS. It is a plausible future scenario, grounded in the realism of today's technological capabilities.

Role of Scenarios in the Study of Ethics

Articles on ethics in engineering and computing, for the greater part, have been about defining, identifying and describing types of ethics, and emphasizing the importance of ethics in the curriculum and the workplace. A small number of ethics-related studies more directly concerned with invention and innovation consider the possible trajectories of emerging technologies and their corresponding social implications [1], [2]. Within the engineering field, these studies commonly take on the guise of either short stories or case-based instruction [3], [4]. This article uses scenario planning to identify the possible risks related to location-based services in the context of security and privacy. While "day-in-the-life scenarios" have been popular in both human-computer interaction and software engineering studies, they have not been prevalent in the ethics literature [5].

The most well-known usage of stories related to ethical implications of technology have been constructed by Richard G. Epstein [6]. His 37 stories in the *Artificial Intelligence Stories Web* are organized thematically based on how the human experience is affected by the technology [7]. Of fiction, Epstein writes that it is "a great device to help one envision the future and to imagine new concepts and even applications" [8]. His *Silicon Valley Sentinel-Observer's Series* ran as a part of *Computers and Society* [9]. John M. Artz has written about the importance of stories advancing our knowledge when exploring areas where we do not fully understand a phenomenon [10]. Artz calls stories and our imagination "headlights" that allow us to consider what might lie beyond: "[c]onsider imagination as the creative capacity to think of possibilities. Imagination lets us see the world, not as it is, but as it could be. And seeing the world as it could be allows us to make choices about how it should be." In 1988, Artz indicated the shortage in short stories in the field, and this paper addresses the shortage by focusing on LBS.

> **When is a person sufficiently impaired to warrant monitoring?**

The definition of a scenario used in this paper is "[a]n internally consistent view of what the future might turn out to be" [11]. Scenarios can be used to combine various separate forecasts that pertain to a single topic [12], 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. According to Godet a scenario "must simultaneously be pertinent, coherent, plausible, important and transparent" [13].

The Track, Analyze, Image, Decide, Act (TAIDA) scenario planning framework is used here with respect to LBS to i) identify aspects of the current situation that may have an impact on the future under consideration; ii) deliberate on the possible future consequences of the aspects identified in *tracking*; iii) approach possible changes intuitively to create a plausible future, "to create not only an intellectual understanding but also an emotional meaning," iv) determine what should be done about a given scenario in response to issues raised, and v) offer recommendations that will address these issues [14]. Analysis of the future scenario presented will be conducted using deconstruction to draw out the social implications. 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" [15].

The Roman philosopher Seneca said: "[t]here is no favorable wind for the man who knows not where he is going" [13]. There is certainly merit in exploring the potential effects of LBS before they occur. As Michael and Michael highlight: "[m]ost 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" [16]. "[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" [17].

The scenario "Control Unwired" continues five short stories and is set in Australia. The critical analysis that follows is also presented within a predominantly Australian context.

Control Unwired

Vulnerability - *The Young Lady*

The street appeared to be deserted. Kate wasn't surprised – this part of town always quieted down at night, especially on weekday evenings like this one. There wasn't much around except office buildings and coffee shops that served to provide a steady stream of caffeine to the office workers.

Kate fished her smart phone out of the pocket of her grey suit jacket [18], [19]. Pressing a few buttons, she navigated through the on-screen menu to the *Services* option, then to *Call a Taxi* [20]. The device beeped at her,

If a person's resistance is bypassed or circumvented, their adaptive capacities can be overloaded, inducing feelings of desperation and helplessness.

flashing the message: *No signal available* [21].

Kate swore, shoving the PDA back into her bag. The surrounding buildings must have been blocking the GPS signal [22]. She knew she needed to get to a more open area.

What a pain, she thought. They overload me with cases, expect me to stay late, and then the gadget they give me to get home doesn't work.

Although Kate was irritated more than anything else, there was a niggling sort of apprehension in the pit of her stomach. She felt alone – very alone, and not at all comfortable being by herself, at eleven in the evening, in a deserted place.

Shaking off the uneasiness, she berated herself. *Get a grip, Kate. You're not a child.*

As Kate strode off, a dark shadow detached from a nearby alleyway. It followed, silently, at a distance, keeping out of the dim pools cast by the streetlights.

Unfortunately, Kate didn't know which direction she should go to find a clear space for her phone to get a fix on her location.

If I keep heading the same way, she thought, *I'm bound to find somewhere sooner or later.*

The surrounding structures were slightly lower here, the taller office blocks just down the road. As Kate walked, the shadow some way behind flickered in the wind, as though it were wearing a long coat. It followed stealthily, steadily decreasing the distance between itself and Kate.

Suddenly, Kate's phone bleeped for attention. Kate pulled it out of her bag again and read the message on the screen: *Signal acquired.*

"Finally," she breathed. Quick fingers navigated back to the *Call a Taxi* command. The phone gave a comforting reassurance that a taxi was on its way, with an estimated arrival time of less than a minute [23].

The shadow hung back, unsure, watching.

Within thirty seconds of making the call, a taxi veered out of nowhere and pulled to an abrupt stop alongside Kate. She opened the door and slid into the back seat.

As the taxi pulled away, the shadow shifted slightly and melted back into the darkness.

Liberty - *The Husband and His Wife*

The next day, the sun filtered into an east-facing bathroom window, where a man stood studying himself in the mirror.

Slight lines crinkled the skin near his eyes and mouth. His hair was still quite thick and healthy, but flecked with the salt-and-pepper grey of an aging man. Although Colin was well past his sixtieth birthday, he could have easily passed for a man in his fifties.

Suddenly, the telephone rang. Colin paused for a moment, listening – the ring only sounded in the bathroom [24]. The kitchen, bedroom, and lounge room were all silent.

"Even the damn phone knows where I am," he muttered, shaking his head. He touched the hard lump of the RFID tag that was stitched into the hem of his shirt [25], [26]. "Helen, not again!"

Colin stabbed at an unobtrusive button on the bathroom wall, [27] and his reflection instantly gave way [28] to the face of an attractive woman with bobbed blonde hair [29] – Helen, his wife, calling from the airport in Hong Kong.

"Oh sweetheart, you look tired." Helen sounded concerned.

Colin shrugged. "I don't feel tired. I think I just need to get some fresh air."

"Open the window, then. It might make you feel better."

Colin thought that what would make him feel better was a nice long walk without his wife checking up on him every five minutes.

"You haven't been to the cupboard yet to take your morning medicines," Helen said.

"Why don't you stop pussyfooting around and just inject me with one of those continuous drug delivery things?" [30], Colin frowned.

Helen smiled. "Great idea," she teased. "We could put a tracking chip in it too. Two birds, one stone" [31].

"At least then I wouldn't have to wear this stupid bracelet [32]. They're made for kids [33], Helen." Colin knew his wife was joking, but the truth was that he often did feel like a recalcitrant child these days.

"Well," Helen replied, "If you didn't insist on being so pig-headed, you wouldn't have to wear it. I was terrified when you collapsed. I'm not going to let it happen again. This way I know you're not gallivanting about without someone to look after you."

"Ever considered that I can take care of myself? I'm not a child."

"No, you're not. And you're not a young man either," Helen admonished. "You need to accept that with your condition, it's just not safe to be going off by yourself. What if something happened to you? Who would know? How would we find you?"

"I feel like a prisoner in my own home, Helen. I can't even take the thing off without you knowing about it. You know they use these for prisoners?"

"Parolees, dear. And they're anklets." She leaned in closer to the screen. "Someone needs to take care

of you, Colin. If you won't, I'll have to do it myself."

Colin sighed. "You just don't understand what it's like to be getting… older. Not being able to do everything you used to. Being betrayed by your own body. It's bad enough without you babying me along like some kind of octogenarian invalid."

"Well, I guess that's the downside to marrying a woman almost twenty years younger than yourself," Helen grinned.

"The only downside." Colin smiled back at her, but his heart wasn't really in it. They had been through this argument countless times before.

He changed the subject. "Heard from our dear daughter lately? Or Scott?"

"Kate called me last night. She's doing well."

"How's her new job?" Colin asked.

"Well, she says she enjoys it, but she's working very long hours," Helen replied.

"And I bet you're worried about her being alone in the city at night for five minutes," Colin said.

Helen gave a self-conscious smile. "It's not a very nice part of town. I'll feel much better about her working late when the firm moves closer to the inner city."

"And Scott?"

"Haven't heard from him. He's back in Sydney now, though. I wish he'd call."

"Maybe if you weren't always pestering him to marry his girl from Melbourne, he'd call more," Colin grinned.

Helen glanced up, away from the screen.

"Sweetheart, I have to go – they've just given the final boarding call for my flight. Enjoy the rest of your day. I'll see you when I get home tonight." She blew a rather distracted kiss at the screen, then it went blank.

Colin's shoulders sagged. Alone again.

He shuffled into the kitchen to make breakfast. Helen had left him skim milk and pre-packaged porridge oats.

"Wow," he muttered. "Cosmic Blueberry or Bananarama? Such decisions."

Just as Colin was finishing off the last few spoonfuls, the watch on his wrist emitted a low beep. He glanced at the screen: *Low battery – critical.*

Colin smiled. The device had been flashing low battery messages intermittently since yesterday evening. It had less than three days' standby time, and being on a business trip, Helen wasn't around to make sure it got recharged [34].

The screen on the little device winked out.

Munching on his porridge, Colin reached over to the cutlery drawer and took out the kitchen scissors. Very carefully, he snipped out a neat little rectangle from the hem of his shirt. The RFID tag came with it.

He swallowed down the rest of his breakfast and tossed the tag onto the counter.

Colin was going for a walk.

No alert went out to Helen. No neighbors came hurrying to see what he was doing. He reveled in the possibility of heading out without someone watching his every move [35].

Colin wandered off, his own man, if only for a morning.

Association - *The Friends and Colleagues*

"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. 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. 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," he continued with his mouth full [36].

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" [37]. He smiled. "It's crazy that New South Wales is already trialing these tracking implants, while Victoria's only recently got a widespread implementation of the anklets [38]. They've been around commercially for years. Mum's got Dad wearing a tracking watch now, for peace of mind after the whole angina scare.

"But the implants are much better," Scott continued. "Who wants a chunky anklet or bracelet that makes you look like a 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 [39]. It's about overcrowding, too – jails everywhere have had an overcrowding problem for years [40].

"I also think electronic monitoring and parole are much better in terms of

rehabilitation," Scott went on. "People can change [41]. Often they've committed a fairly minor crime, then they go to prison, get mixed up with worse crowds [42]-[44]. 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 [40].

"On parole, they can still go to work and earn money, be productive members of society, get their lives back [44], [45]. But they're watched, very closely – the tracking systems alert us if anything looks off. It's imprisonment without prisons."

Janet smiled. "That's very *Alice in Wonderland*. When the Cheshire Cat disappears – how does it go? 'I've often seen a cat without a grin, but a grin without a cat is the most curious thing I ever saw in all my life!'"

Scott laughed. "I suppose you could compare it to that." He noted Janet's skeptical look. "It's not like we're sending people out of jails willy-nilly. There is a pretty thorough system in place to determine who gets paroled and who doesn't."

"So how does that work?" asked Janet.

"Well, a while ago it was mainly based on crime-related and demographic variables. We're talking stuff like what sort of offense they're doing time for, the types of past convictions on their record, age, risk of re-offending" [46].

She 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" [47].

"So prisons are the new asylums?" Janet frowned.

"Not quite but I see your point," Scott admitted.

> **Can it be considered reasonable to impinge upon the freedom of someone who is merely suspected of committing a crime?**

"What about terrorists?" Janet argued. "How can you guarantee that there won't be another incident like the Brisbane rail bombings"[48]?

"Like I said, anyone considered really dangerous is still kept in a regular prison," Scott said. "All the major landmarks and places people congregate in Sydney are tagged anyway [49]. There's no way a convicted terrorist would get within a hundred meters of anything worth attacking."

Janet raised her eyebrows, unconvinced. She thought of the newspaper reports about security breaches of public places that had been linked to professional cybervandals. As far as she was concerned, no new technology was the silver bullet.

Scott continued, "And you know that governmental powers now allow 'persons of interest' to be implanted as well."

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 they should just track everyone, to be on the safe side?"

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.

Policing - *The Officer and the Parolee*

Scott paused on the landing in front of Doug's apartment and steeled himself. Doug was his last visit of the day. Scott was a fairly likeable guy and had a rapport with most of his cases, but Doug, convicted of aggravated sexual assault, was different [50].

Scott knocked on the door.

A few seconds passed, then it opened a fraction and a stubbled face peered out. Doug wore a stained long-sleeved shirt and ratty jeans.

"Scott," he sneered. "So nice of you to drop by."

"Let's just do this, Doug."

Scott followed Doug into the living room. He pulled out a small device and waved it up and down the man's left arm. It beeped and Scott checked the screen.

"Your chip seems fine," he said. "Just a routine check – we like to do one every now and then to make sure everything's okay. Congratulations on your new job, by the way. How do you like house painting?"

"My true bloody calling," Doug leered.

"Er… great. Keep it up then. With good behavior like this you'll be done in no time."

Scott felt relieved that he would no longer have to sift through Doug's daily tracking logs.

Doug just smiled.

Duplicity - *The Victim*

Doug waited more than two hours after Scott left before removing his shirt. He peeled off the electrical tape covering an ugly, ragged scar on his upper arm [51]. The scar wasn't from the chip's implantation. It was created by the deep cut Doug's heavily pierced cyberpunk friend had made to remove it [52].

The tiny chip – smaller than a grain of rice – was stuck to the back of the tape. Gingerly, Doug set it on the table in front of the TV and smiled.

His chip was having a night in.

He was going out.

Doug pulled his shirt back on and shrugged into a long coat.

He knew there would be a young woman in a grey suit leaving her office soon. She worked at the law firm that was hot stuff in the news. *Stupid really*, he thought, *that she's not afraid to wander the streets in that part of town at night, alone. A Smart girl like that should know better*.

The stairwell was quiet. He slipped out into the darkness, a shadow among the other shadows.

He wanted to pay that attractive little lawyer a visit before she caught her taxi home.

Critical Analysis

Legal and Ethical Issues

According to Ermann and Shauf, our "ethical standards and social institutions have not yet adapted… to the moral dilemmas that result from computer technology" [53]. This has a great deal to do with the way Helen uses the LBS technologies available to her. In *Liberty*, Helen obviously cares about her husband and wants what is best for his health. She is willing to "help" Colin look after himself by monitoring him and restricting the activities she allows him to participate in, especially when he is alone. It is not too difficult to imagine this happening in the real world if LBS becomes commonplace. It is also conceivable that, for some people, this power could be held by a hospital or health insurance company. However, Helen fails to balance her concern for her husband's physical welfare with his need to be an autonomous being. Although LBS technologies are readily available, perhaps she has not completely thought through her decision to use these technologies to monitor Colin, even if it is ostensibly for his own good. It could even be seen as selfish.

Consideration of legal issues is also important – it does not appear that there is any specific Australian legislation that covers the unique possibilities of LBS tracking. One situation that is likely to appear with more frequency is people using LBS technologies to monitor loved ones "for their own good." Several issues are raised here. When is a person sufficiently impaired to warrant such monitoring? Should their consent be necessary? What if they are considered to be *too* impaired to make a rational decision about monitoring? this sort of situation, LBS tracking can be a joint process that "is continually informed by the goal of fostering… autonomy" [54].

Another significant legal and ethical issue is that of monitoring people such as those suspected of being involved in terrorist activities. As hinted at in *Association*, this is not mere fancy – the Australian Government, for example, has passed new anti-terrorism laws that, among other things, would give police and security agencies the power to fit terror suspects with tracking devices for up to 12 months [55].

The current climate is indicative of individuals' willingness to relinquish their privacy (or at least someone else's) for the sake of impenetrable security.

Autonomy is an important part of a person's identity. Resistance to a situation is often unconsciously employed to "preserve psychically vital states of autonomy, identity, and self-cohesion from potentially destabilizing impingements" [54]. If a person's resistance is bypassed or circumvented, their adaptive capacities can be overloaded, inducing feelings of desperation and helplessness. The natural reaction to this is to exert an immediate counterforce in an attempt to re-establish the old balance, or even to establish a new balance with which the individual can feel comfortable [54].

These ideas about autonomy, identity and resistance are demonstrated in *Liberty* through Colin. He experiences feelings of helplessness and vulnerability because of his loss of autonomy through constant LBS monitoring. His unsupervised walk can be seen as an attempt to redress the balance of power between himself and Helen. With these issues in mind, perhaps the kindest and least disruptive way to implement a monitoring program for an aging individual is to develop a partnership with that person. In

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 to 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 offense. 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 offense" [40]. With no crime involved, the punishment of electronic monitoring or home detention must be out of proportion.

With measures such as those in Australia's counter-terrorism laws, there is obviously a very great need for caution, accountability, and review in the exercise

of such powers. Gareth Evans, the former Australian Labor foreign minister, commented on the laws by saying:

> **The threat of terrorist attacks has led the Australian Government to propose giving itself extraordinary powers that never could have been justified previously.**

> "It is crucial when you are putting in place measures that are as extreme in terms of our libertarian traditions as these that there be over and over again justification offered for them and explanations given of the nature and scale of the risk and the necessity… it is a precondition for a decent society to have that kind of scrutiny" [56].

The July 2005 London subway bombings are the justification offered repeatedly by Australian Prime Minister John Howard for the new laws, reinforced by Australian Secret Intelligence Organization (ASIO) director-general Paul O'Sullivan. However, this "justification" ignores the reality that "the London bombers were 'clean skins' who had escaped police notice altogether" [57]. Tagging suspicious people cannot keep society completely safe.

We do not make a judgment on whether pre-emptive control legislation is proper or not. We suggest, however, that the laws recently enacted by the Australian Federal Government (and agreed to by the Australian States) could be indicative of a broader trend.

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" [58]. Could the same argument be used in the future to justify monitoring everyone in the country? If pre-emptive control is a part of government security, then widespread LBS monitoring could be the most effective form of implementation.

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

Social Issues

Control emerges as a significant theme in the scenario *Control Unwired*. Even in LBS applications that are for care or convenience purposes, aspects of control are exhibited. The title reflects the dilemma about who has control and who does not. For example, in *Vulnerability*, Kate experiences a loss of control over her situation when her GPS-enabled smart phone does not work the way she wants it to work, but a sense of control is restored when it is functioning properly again. Helen has control over Colin in *Liberty*, and in turn Colin has little control over his own life. In both *Association* and *Policing* we see how Scott uses LBS every day as a control mechanism for parolees. Finally, in *Duplicity*, the question arises whether faith in this sort of control is fully justified.

Trust is a vitally important part of human existence. It develops as early as the first year of life and continues to shape our interactions with others until the day we die [59]. In relationships, a lack of trust means that there is also no bonding, no giving, and no risk-taking [60]. In fact, Marano states:

> "[w]ithout trust, there can be no meaningful connection to another human being. And without connection to one another, we literally fall apart. We get physically sick. We get depressed. And our minds… run away with themselves" [59].

An issue that arises in *Liberty* is that of trust, recalling Perolle's notion of surveillance being practiced in low-trust situations and the idea that the very act of monitoring destroys trust [61]. We can see this happening in the Colin/Helen relationship. Helen does not trust Colin enough to let him make his own decisions. Colin does not trust Helen enough to tell her he is going out by himself, without any kind of monitoring technology. He resents her intrusion into his day-to-day life, but tolerates it because he loves his wife and wants to avoid upsetting her. Their relationship could be expected to become increasingly dysfunctional if there is a breakdown of trust. It is near impossible to predict the complex effects of LBS when used to track humans in this way, especially as each person has a different background, culture, and upbringing. However, if Perolle [61] and Weckert [62] are agreed with, these types of technological solutions may well contribute to the erosion of trust in human relationships – what would this entail for society at large? Freedom and trust go hand-in-hand. These are celebrated concepts that have been universally connected to civil liberties by most political societies.

Technological Issues

There is a widely held belief that it is how people use a technology, not the technology itself, that can be characterized 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" [63]. However, there are other researchers who argue 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 [63]. The LBS applications in the scenario all appear to show aspects of control. This would suggest that the technology itself is not neutral – that LBS are designed to exercise control.

Control Unwired seems to echo Dickson's argument that technology is not neutral because of its political nature: "dominating technology reflects the wishes of the ruling class to control their fellow men" [63]. We can certainly see elements of this idea in the scenario. All of the LBS functions depicted are about control, whether it be control over one's own situation (*Vulnerability*), caring control of a loved one (*Liberty*), or forced control over parolees (*Association, Policing*, and *Duplicity*). These situations imply that LBS is not neutral, and that the technology is designed to enhance control in various forms.

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" [64]. The idea is that technological forces contribute to social change more than political, economic, or environmental factors. The authors 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 artifacts of technology are chosen by a social selection environment, [like] the success of living organisms is determined by a biological selection environment" [65]. 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 [66].

Technological potential is not necessarily social destiny [67]. 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 (rightly or not) that it is necessary in the current climate.

The scenario also demonstrates that technology and society evolve at least partially in tandem. In *Association*, 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. Throughout *Control Unwired* we can see LBS becoming an integral part of daily life. If this does happen, consideration must be given to what will happen if the technology fails – which it inevitably will. No technology is completely perfect. There are always shortcomings and limitations.

Examples of deficiencies in LBS technologies can be found scattered throughout the scenario. In *Vulnerability*, Kate appears to be over-reliant on LBS (why does she not simply call a taxi from her office before leaving?) and when the technology fails, it creates a potentially dangerous situation. Even more dangerous circumstances occur in *Duplicity*. Doug, a convicted sex offender, is able to break his curfew without anyone knowing. Perhaps measures could be implemented to stop such breaches from going undetected, but that would not stop them from happening altogether. One U.S. study found that about 75 percent of electronically monitored "walk offs" were re-apprehended within 24 hours [45]. That means a quarter went free for more than a day – plenty of time to commit other offences. And, although the offender may be caught and punished, it is difficult to remedy the damage done to an individual who is robbed or assaulted.

And no technology is completely fail-safe. Even electricity, a mainstay of daily life, can suddenly fail, with socially and economically devastating effects. Most of Auckland, New Zealand, went without power for five weeks during a massive blackout in 1998 [68]. A 1977 electricity outage in New York led to widespread looting, arson and urban collapse [69]. If we become as reliant on LBS as we have become on other technologies like electricity, motor vehicles, and computers, we must be prepared for the consequences when (not if) the technology fails.

Risk to the Individual versus Risk to Society

Any technology can be expected to have both positive and negative effects on individuals and on the wider community. Emmanuel Mesthane of Harvard's former Technology and Society Program wrote: "[n]ew technology creates new opportunities for men and societies and it also generates new problems for them. It has both positive and negative effects and it usually has the two at the same time and in virtue of each other" [70]. From Table I, it is obvious that there is an inherent trade-off between the interests of the individual and the interests of society as a whole: the privacy of the individual is in conflict with the safety of the broader community. As G.T. Marx reflects, "[h]ow is the desire for security balanced with the desire to be free from intrusions" [71]? This work is certainly not the first to allude to this issue. For example, Kun has said that "perhaps one of the greatest challenges of this decade will be how we deal with this theme of privacy vs. national security" [72].

Table I
Positives and Negatives of LBS for Different User Types

User Type	Positives	Negatives
Voluntary user. The most likely type, probably using commercial LBS applications such as in-vehicle routing and navigation.	• Choice. User can opt out of LBS by shutting down, deactivating the device or leaving it in a stationary position. • Safety. Accurate location information may provide timely help in the event of an emergency. • Convenience. E.g. increased ease of routine transactions such as at toll-ways. • Security of the individual. E.g. building access, navigational capabilities.	• Security risk. Even though use is voluntary, the user has a lack of control over who accesses location information. • Privacy risk. Things such as location information and automated transactions can be traced back to the user. • False sense of security. Someone watching from afar cannot necessarily help in an emergency situation such as in the prevention of a kidnapping or attack.
Mandatory user. Possible in the form of government applications (e.g. home imprisonment) and domestic applications (e.g. tracking minors).	• Safety. Personal security may be increased- if someone can see where the user is at all times. • Accountability. Location can be monitored constantly, so the user may be held responsible for their activities. If a crime is committed, they may be implicated or cleared based on location information. • Security of society. The user's knowledge that someone can see their every move may prevent them from taking part in a criminal activity.	• Invasion of privacy. Location can be viewed at any time, with or without user consent. • Security risk. Location information is constantly available, so data leaks are potentially very serious. • Decreased autonomy. Independence is important to mental and emotional wellbeing. • May give user a false sense of security. Someone watching from afar cannot necessarily prevent harm to another. • May give society a false sense of security. Monitoring does not mean that a crime cannot be committed.
Non-user. Unlikely to be a large group if LBS become widespread. Many in this category would have personal reasons for not adopting LBS, or could not afford to use the technology.	• Privacy. Personal location information remains relatively protected. • Autonomy. High level of independence and control over their own activities. • Simplicity. There is no need to deal with the possibility of the technology failing.	• Safety risk. Help may be delayed in the event of an emergency, although programs like E911 now mean that emergency services can pinpoint a caller's location with an accuracy of between 50 and 300 meters [24]. • Security risk. The person's activities may pose a danger to society, community misses out on the security benefits of LBS. • Risk of prejudice. A person may be suspected of wrongdoing without evidence, simply by reason of opting-out of LBS.

The original contribution of this article is that the dilemma has been related specifically to LBS, under the privacy-security dichotomy [73]. Here, each side of the dichotomy is divided into three key components that combine to greatly magnify risk. Removing one or more components for each set decreases the privacy or security risk. Where more elements are present in conjunction, the risk is increased.

Significant privacy risk occurs when the following factors are present (Fig. 1):

- Omniscience – LBS tracking is mandatory, so authorities have near-perfect knowledge of people's whereabouts and activities.
- Exposure – security of LBS systems is imperfect, leaving them open to unauthorized access.
- Corruption – motive exists to abuse location-related data. This includes unauthorized or improper changes, thus compromising content integrity.

It is not difficult to see why the danger in this privacy-risk scenario is so great. A nation with "all-knowing" authorities means that a large amount of highly sensitive information is stored about all citizens in the country. Security of electronic systems is never foolproof. And, where there is something to be gained, corrupt behavior is usually in the vicinity. The combination of all three factors creates a very serious threat to privacy.

Significant security risk occurs with the following conditions (Fig. 2):

- Limitedness – authorities have limited knowledge of people's activities.
- Vulnerability – security of individuals and infrastructure is imperfect.
- Fraudulence – motive exists to commit crimes.

This security-risk dimension is a life situation that people have to contend with in the present day: limitedness, vulnerability, and fraudulence. Law enforcement authorities cannot be everywhere at once, nor can they have instant knowledge of unlawful activity. Security of infrastructure and people can never be absolute. In addition, there are always individuals willing to commit crimes for one reason or another. These factors merge to form a situation in which crimes can be committed against people and property relatively easily, with at least some chance of the perpetrator remaining unidentified.

As mentioned above, the security-risk half of the dichotomy typifies our current environment. However, the majority of society manages to live contentedly, despite a certain level of vulnerability and the modern-day threat of terrorism. The security-risk seems magnified when examined in the context of the LBS privacy-security dichotomy. LBS have the potential to greatly enhance both national and personal security, but not without creating a different kind of threat to the privacy of the individual. The principal question is: how much privacy are we willing to trade in order to increase security? Is the privacy-risk scenario depicted above a preferable alternative to the security-risk society lives with now? Or would society lose more than it gains? And how are we to evaluate potential ethical scenarios in the context of utilitarianism, Kantianism, or social contract theory?

Major Implications

The issues of control, trust, privacy and security are interrelated (Table II). As discussed above, increased control can impair or even destroy trust; i.e., there is no need to be concerned with trusting someone when they can be monitored from afar. In contrast, increased trust would normally mean increased privacy. An individual who has confidence in

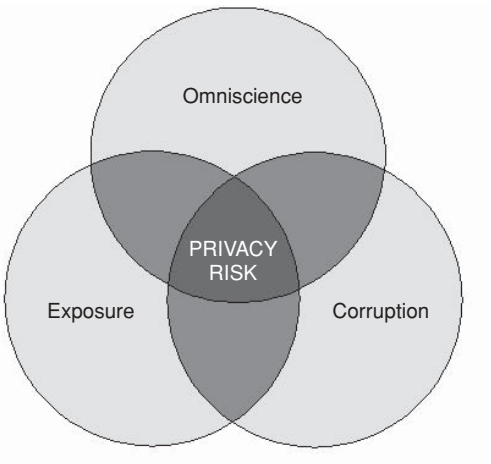


Fig. 1. Privacy risk.

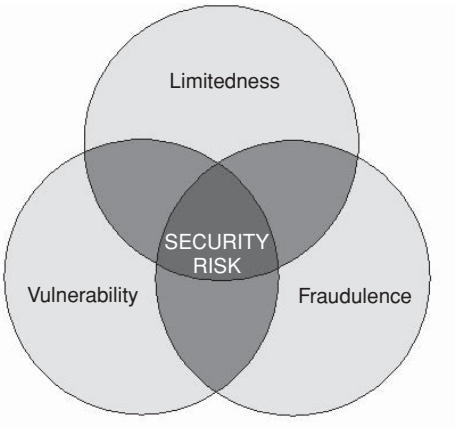


Fig. 2. Security risk.

Table II
Unanswered Questions in LBS

Privacy	Control
• Who has access to location information? • Can an individual wearing a tracking device deactivate it? • Do the benefits that accrue from LBS in a given context outweigh the impacts of seriously invading an individual's privacy? • Is this individual's privacy worth more than the safety and security of society?	• Who is controlling whom, and for what reasons? • Does the person to be monitored need to consent? • Is an individual too impaired to consent to their own monitoring? If so, who should be able to make the decision for them? • If an individual does not consent to monitoring, are there special circumstances (e.g. an indictable crime), that warrants control without consent? • How can it be ensured that inaccuracies in reported location do not adversely affect the individual being monitored?
Security	**Trust**
• What restrictions are placed on organizations (and their employees) that handle location information? • How well protected are the LBS electronic systems and subsequent support systems? • What measures are in place to manage mandatory LBS users? • What backup measures are in place in case the system fails?	• Does the LBS context already involve a low level of trust? • If the LBS context involves a moderate to high level of trust, why are LBS being considered anyway? • Will the use of LBS in this situation be trust-building or trust-destroying?

another person to avoid intentionally doing anything to adversely affect them, probably does not feel the need to scrutinize that person's activities.

Privacy requires security as well as trust. A person's privacy can be seriously violated by a security breach of an LBS system, with their location information being accessed by unauthorized parties. The other effect of system security, however, is that it enhances control. A secure system means that tracking devices cannot be removed without authorization, therefore, control is increased. Of course, control and privacy are mutually exclusive. Constant monitoring destroys privacy, and privacy being paramount rules out the possibility of LBS tracking. These relationships are summarized in Fig. 3.

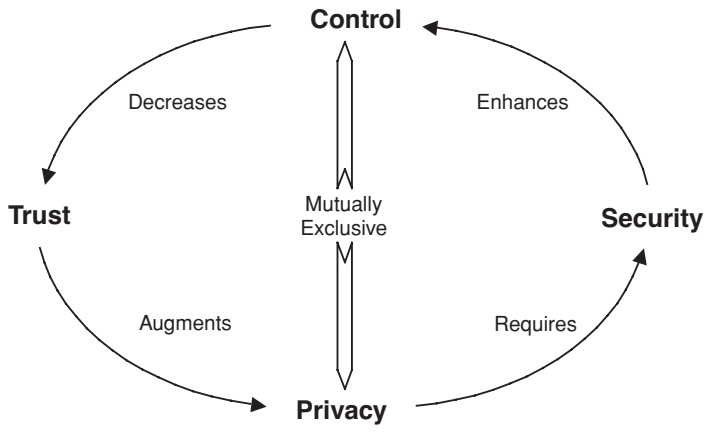


Fig. 3. Relationships between major issues in LBS.

The most significant implication of the work presented here is this: the potential for LBS to create social change raises the need for debate about our current path and consideration of future probabilities. Will the widespread application of LBS significantly improve our lives? Or will it have negative irreversible social effects?

Technological progress is not synonymous with social progress. Social progress involves working towards socially desirable objectives in an effort to create a desirable future world [65]. Instead of these lofty ideals, technological progress is based on what is technically possible. However, there is a difference between what can be done and what *should* be done – the relentless pursuit of technological advancement for its own sake is arguably a pointless exercise. Do we really need more electronic gadgets in our daily lives? As Kling states:

> "I am struck by the way in which the news media casu-

ally promote images of a technologically rich future while ignoring the way in which these technologies can add cost, complexity, and new dependencies to daily life" [74].

In the *Association* section of the scenario, Janet's comment about *Alice's Adventures in Wonderland* can be seen as more than just a superficial remark. In the book, Alice has the following conversation with the Cat:

> "Would you tell me, please, which way I ought to go from here?"
> "That depends a good deal on where you want to get to," said the Cat.
> "I don't much care where—" said Alice.
> "Then it doesn't matter which way you go," said the Cat [75].

Martin Gardner says that John Kemeny, author of *A Philosopher Looks at Science*, compares Alice's question and the Cat's answer to the "eternal cleavage between science and ethics" [75]. The same could be said of LBS technologies and possible future applications. New technologies provide exciting opportunities, but human decision-making based on social and ethical considerations is also needed in determining the best path to follow. Technology merely provides us with a convenient way to reach the destination. Without a sense of direction, where might we find ourselves? And where is the logic behind a "directionless" destination? There is clearly a serious need for thought and discussion about how we want LBS to be used in the wider context of its potential application.

Besides developing a sense of purpose for the use of LBS, we need to examine very carefully the possibility of the technology having unintended side effects such as the breakdown of trust and abuse of its application. Certainly, the potential effect of unplanned consequences should not be underestimated. According to Jessen:

> "The side effects of technological innovation are more influential than the direct effects, and they have the rippling effect of a pebble hitting water; they spread out in ever enlarging concentric circles throughout a society to transform its behavior, its outlook, and its moral ethic" [76].

Of course not all secondary effects can be foreseen. However, this does not mean that deliberating on the possible consequences is without some genuine worth. Surely some form of preparation to deal with adverse outcomes, or at least to notice them before they become irreversible, is better than none at all.

The scenario *Control Unwired* has demonstrated the potential of LBS to create social change. It has also shown that the use of LBS may have unintended but long-term adverse effects. For this reason the major recommendations are cross-disciplinary debate and technology assessment using detailed scenario planning. We need to critically engage with LBS, its potential applications, and possible side-effects instead of just blindly hurtling along with the momentum of technology-push.

Author Information

The authors are with the University of Wollongong, School of Information Systems and Technology, Wollongong, Australia; email:katina@uow.edu.au.

Acknowledgment

The authors would like to acknowledge the significant contribution of Dr. M.G. Michael, Honorary Fellow at the School of Information Systems and Technology at the University of Wollongong and a member of the IP Location-Based Services Research Program.

References

[1] J.E. Jacobs, "Social implications of computers: ethical and equity issues," *ACM Outlook*, pp. 100-114, 1988.
[2] C. Huff, "Practical guidance for teaching the social impact statement," *ACM CQL*, pp. 86-89, 1996.
[3] "Cases on Engineering Ethics Practice," *Onlineethics.org*; http://www.onlineethics.org/eng/cases.html, accessed Oct. 2006.
[4] A. Ghafarian, "Integrating ethical issues into the undergraduate computer science curriculum", *ACM CCSC - JCSC*, vol. 18, no. 2, pp. 180-188, 2002.
[5] J.A. Rohn et al., "Usability in practice: Alternatives to formative evaluations — Evolution and revolution," *CHI 2002*, pp. 891-897, 2002.
[6] R.G. Epstein, *The Case of the Killer Robot*. New York, NY: Wiley, 1997.
[7] R.G. Epstein, "Stories and plays about the ethical and social implications of artificial intelligence," *Intelligence*, pp. 17-19, Fall 2000.
[8] R.G. Epstein, "Latest developments in the killer robot computer ethics scenario," *ACM SIGCSE*, pp. 111-115, 1995.
[9] R.G. Epstein, "In-depth! *The Silicon Valley Sentinel-Observer's* public affairs NetTV program presents: Toxic knowledge," in *Proc. Ethics and Social Impact Component on Shaping Policy in the Information Age*, 1998, pp. 86-91.
[10] J.M. Artz, "The role of stories in computer ethics," *Computers and Society*, pp. 11-13, 1998.
[11] M. Lindgren and H. Bandhold, *Scenario Planning: The link between future and strategy*. New York, NY: Palgrave-Macmillan, 2003, p. 21.
[12] J.P. Martino, "A review of selected recent advances in technological forecasting," *Technological Forecasting and Social Change*, vol. 70, no. 8, pp. 719, 722, 2003.
[13] M. Godet, "The art of scenarios and strategic planning: Tools and pitfalls", *Technological Forecasting and Social Change*, vol. 65, no. 1, pp. 3, 7, 11, 2000.
[14] M. Lindgren and H. Bandhold, *Scenario Planning: The link between future and strategy*. New York, NY: Palgrave Macmillan, 2003, pp. 38-39, 47, 168.
[15] P. Hogan, *On Interpretation: Meaning and Inference in Law, Psychoanalysis, and Literature*. Athens, GA: Univ. of Georgia, 1996, p. 9.
[16] K. Michael and M.G. Michael, "Microchipping people: The rise of the Electrophorus", *Quadrant*, vol. 49, no. 3, pp. 22-33, 2005.
[17] S. Žižek, "Cyberspace, or the unbearable closure of being" in *Endless Night: Cinema and Psychoanalysis, Parallel Histories*, J. Bergstrom, Ed. Berkeley, CA: Univ. of California Press, 1999, pp. 92, 101-102.
[18] G. Aquino, "Dialled in: GPS cell phones," *PC World,* Mar. 2004; http://www.pcworld.com/article/id,115273-page,1/article.html, accessed Jan. 2007.
[19] "CF Card GPS for PDA's," *FileSaveAs*, http://www.filesaveas.com/gpscfcard.html, accessed Sept. 2005.
[20] "Agis develops real time location service for savvy mobile phone users," press release, Agis, Singapore, Apr. 25, 2005; http://www.asiagis.com.sg/agis/pdf/Navfone_Press.pdf, accessed Sept. 2005.

[21] Trimble, *How GPS Works*, http://www.trimble.com/gps/whygps-anim00.shtml, accessed Sept. 2005.
[22] S. Dooley and P. Gough, "Software integration lowers the cost of A-GPS," *Wireless-Web*, 2005; http://wireless.iop.org/articles/feature/6/8/7/1, accessed Sept. 2005.
[23] N. Pikabea, "GPS for taxis," *Innovations Report,* May 2004; http://innovations report.de/html/berichte/kommunikation_medien/bericht29210.html, accessed Jan. 2007.
[24] B. Gates *et al., The Road Ahead*. New York, NY: Viking, 1995, pp. 218-219.
[25] Accenture, *Silent Commerce Chips Away at Star City Casino Wardrobe Worries*, http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_successes/StarCityCasino.htm.
[26] *TAGSYS RFID Products*, TAGSYS, Cambridge, MA; http://www. tagsysrfid.com/ eng/rfid/tagsys_produit/rfid_tag-4-1-1.html, accessed Sept. 2005.
[27] K.J. Lin, T. Yu, and C.Y. Shih, "The design of a personal and intelligent pervasive-commerce system architecture," in *Proc. Second IEEE Int. Workshop on Mobile Commerce and Services*, Munich, Germany, 2005, p. 163.
[28] Monster Cable, *The award-winning Flat Screen InvisiSound Mirror Frame makes home theater audio and video disappear*, Monster Press Room, Brisbane, CA, Jan. 2005; http://www.monstercable.com/press/press_result.asp?pr=2005_01_Frame.asp, accessed Sept. 2005.
[29] G. McArthur, "Videoconferencing over IP – The switch is on," *Business Communications Rev.*, Sept. 2004; http://www.bcr.com/bcrmag/2004/09/p62.php, accessed Sept. 2005.
[30] M. Madou, *BioMEMS/BioNEMS: Research in the laboratories of Marc Madou*, INRF Research Summary, Irvine, CA, 2003; http://www.inrf.uci.edu/research/marcmadou.pdf, accessed Sept. 2005.
[31] H. Brøseth and H.C. Pedersen, "Hunting effort and game vulnerability studies on a small scale: A new technique combining radiotelemetry, GPS and GIS," *J. Applied Ecology*, vol. 37, iss. 1, p. 182, 2000.
[32] C.S. *Miner et al.*, "Digital jewelry: Wearable technology for everyday life", *CHI '01 Extended Abstracts on Human Factors in Computing Systems*, p. 45, Mar. 2001.
[33] *Wherify's GPS Wherifone*, Wherify Wireless, Redwood Shores, CA; http://www.wherify-wireless.com/univLoc.asp, accessed Sept. 2005.
[34] Environmental Studies, *GPS Marine Tracking Systems / Vessel Tracking*, http://www.environmental-studies.de/GPS/GPS-tracking-systems/Marine-Tracking/marine-tracking.html, accessed Sept. 2005.
[35] J. Dodd, "Parents & technology: The Wherify GPS personal locator offers help but fails to protect," *General Computing*, vol. 15, iss. 2, p. 35, 2004.
[36] Department of Education, Science and Training, Probation Officer/Parole Officer – NSW/ACT, *Job Guide*, 2005; http://jobguide.thegoodguides.com.au/statespecific.cfm?jobid=615&state_id=NSW, accessed Sept. 2005.
[37] American Probation and Parole Association, *Electronic Monitoring*, 1996; http://www.appa-net.org/about%20appa/electron.htm, accessed Sept. 2005.
[38] Applied Digital Solutions, *Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device*, 2003, http://adsx.com/news/2003/051303.html, accessed Sept. 2005.
[39] NSWLRC, *NSWLRC Report: Sentencing*, http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_ip27chp1, accessed Oct. 2006.
[40] D. Brown, D. Farrier, S. Egger, and L. McNamara, *Criminal Laws,* 3rd ed. Leichhardt: NSW: Federation, 2001.
[41] American Probation and Parole Association, *Discretionary Parole*, 2002; http://www.appa-net.org/about%20appa/discretionary_parole.htm, accessed Jan. 2007.
[42] D. Sugg, L. Moore, and P. Howard, "Electronic monitoring and offending behavior: reconviction results for the second year of trials of curfew orders," Research, Development, and Statistics Directorate, U.K. Government, London, U.K., 2001, http://www.probation.homeoffice.gov.uk/files/pdf/r141[1].pdf, accessed Sept. 2005.
[43] Department of Corrections – New Zealand, *Electronic Monitoring*, 2004, http://www.corrections.govt.nz/public/aboutus/factsheets/reducingreoffending/electronic-monitoring.html, accessed Sept. 2005.
[44] Law Reform Commission NSW, "Chapter 7: Parole," in *Sentencing*, Discussion pap. 33, New South Wales, Australia, 1996; http://www.lawlink.nsw.gov.au/lrc.nsf/pages/DP33CHP7, accessed Sept. 2005.
[45] National Law Enforcement and Corrections Technology Center, 'Keeping Track of Electronic Monitoring', *National Law Enforcement and Corrections Technology Center Bulletin*, National Institute of Justice, Rockville, MD, 1999; http://www.justnet.org/pdffiles/Elec-Monit.pdf, accessed Sept. 2005.
[46] New South Wales Council for Civil Liberties, *Parole, Sex Offenders and Rehabilitation Programs*, New South Wales, Australia, 2003; http://www.nswccl.org.au/docs/pdf/Parole_Sex Offenders_Note.pdf, accessed Sept. 2005.
[47] S.J. Lee and J.F. Edens, "Exploring predictors of institutional misbehavior among male Korean inmates," *Criminal Justice and Behavior*, vol. 32, no. 4, pp. 412-414, 2005.
[48] AAP, "Terror tape targets Melbourne," *The Australian*, Sept. 12, 2005.
[49] K. Michael and A. Masters, "The advancement of positioning technologies in defense intelligence" in *Applications of Information Systems to Homeland Security and Defense*, D. Essam and H.A. Abbass, Eds. London, U.K.: IDG Press, 2005, pp. 193, 201.
[50] A.M. Piehl, B. Useem, and J.J. DiIulio, "Right-sizing justice: A cost-benefit analysis of imprisonment in three states," *Civic Report 8*, 1999, http://www.manhattan-institute.org/html/cr_8.htm, accessed Sept. 2005.
[51] J. Scheeres, "Tracking Junior with a microchip," *Wired News*, 2003; http://www.wired.com/news/technology/0,1282,60771,00.html, accessed Sept. 2005.
[52] M. Millanvoye, "Teflon under my skin," *UNESCO*, 2001; http://www.unesco.org/courier/2001_07/uk/doss41.htm, accessed Nov. 2001.
[53] M.D. Ermann and M.S. Shauf, Eds., *Computers, Ethics and Society*. New York, NY: Oxford Univ. Press, 2002, p. vi.
[54] E. Adler and J.L. Bachant, "Intrapsychic and interactive dimensions of resistance: A contemporary perspective," *Psychoanalytic Psychology*, vol. 15, no. 4, pp. 451, 454, 1998.
[55] N. Gilmore, "PM defends anti-terrorism laws," *Lateline*, 2005; http://www.abc.net.au/lateline/content/2005/s1456384.htm, accessed Jan. 2007.
[56] AAP, "Terror laws shouldn't go overboard: Evans," *The Sydney Morning Herald*,2005;http://www.smh.com/au/news/national/terror-laws-shouldnt-go-overboard-evans/2005/09/27/1127586836368.html?from=moreStories.
[57] M. Wilkinson, "Powers pave way for secret new world," *The Sydney Morning Herald*, pp. 1, 6, Sept. 28, 2005.
[58] J. Kerr, "House arrest for terror suspects," *The Sydney Morning Herald*, p. 1, Sept. 28, 2005.
[59] H.E. Marano, "Trust someone, again," *Psychology Today*, vol. 31, iss. 4, p. 7, 1998.
[60] T. Mizrahi, "How can you learn to trust again?," *Psychology Today*, vol. 35, iss. 2, p. 12, 2002.
[61] J.A. Perolle, "Computer-supported cooperative work" in *Computers, Surveillance and Privacy*, D. Lyon and E. Zureik, Eds., Minneapolis, MN: Univ. of Minnesota Press, 1996, pp. 47, 59.
[62] J. Weckert, "Trust and monitoring in the workplace," in *Proc. IEEE International Symposium on Technology and Society*, 2000, p. 245.
[63] J. Lipscombe and B. Williams, *Are Science and Technology Neutral*? Manchester, U.K.: Univ. of Manchester, 1979, p. 19.
[64] L. Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MA: M.I.T. Press, 1977, p. 76.
[65] E. Braun, *Futile Progress: Technology's Empty Promise*. London, U.K.: Earthscan, 1995, p. 21.
[66] T.P. Hughes, "Technological momentum" in *Does Technology Drive History*?, M.R. Smith and L. Marx, Eds. Cambridge, MA: M.I.T. Press, 1994, p. 101.
[67] D. Lyon, *Surveillance Society: Monitoring Everyday Life Berkshire*, U.K.: Open Univ. Press, 2001, pp. 23-24.
[68] CNN, "Power outage hits Auckland hours after crisis declared over," *CNN World News*, 1998. http://www.cnn.com/WORLD/9803/27/auckland.outage/, accessed Oct. 2005.
[69] K. Westcott, "New York's "good and bad" blackouts," *BBC News*, 2003; http://news.bbc.co.uk/1/hi/world/americas/3154757.stm, accessed Oct. 2005.
[70] P. Bereano, "Technology is a tool of the powerful," in *Computers, Ethics and Society*, M.D. Ermann and M.S. Shauf Eds. New York, NY: Oxford Univ. Press, 2003, p. 85.
[71] G.T. Marx, *Undercover: Police Surveillance in America*. Berkeley, U.K.: Univ. of California Press, 1988.
[72] L.G. Kun, "Homeland security: the possible, probable, and perils of information technology," *IEEE Engineering in Medicine and Biology*, vol. 21, no. 5, pp. 28-33, 2002.
[73] L. Perusco, K. Michael, and M.G. Michael, "Location-based services and the privacy-security dichotomy," in *Proc. Third Int.Conf. on Mobile Computing and Ubiquitous Networking*, 2006.
[74] R. Kling, "The seductive equation of technological progress with social progress" in *Computerization and Controversy: Value Conflicts and Social Choices*, R. Kling, Ed. Boston, MA: Academic, 1996, pp. 22-23.
[75] L. Carroll and M. Gardner, Ed., *The Annotated Alice*. New York, NY: Penguin, 1970, p. 88.
[76] P. Jessen, cited in *Technology Assessment: Creative Futures*, M.A. Boroush, K. Chen, and A. Christskis, Eds. Ann Arbor, MI: Univ. of Michigan Press, 1980, pp. 245-246.