A Social Ecological Model of ICT Cooption: Surveillance Creep in the Information Age

Darryl Coulthard
Deakin University, darryl.coulthard@deakin.edu.au

Susan Keller
Deakin University

A social ecological model of ICT cooption: Surveillance creep in the information age.

Darryl Coulthard
Susan Keller
Deakin University

Email: darryl.coulthard@deakin.edu.au

Abstract

A model for ICT cooption is introduced using the example of 'surveillance creep' which is the phenomenon of increasing dataveillance as the result of the introduction of seemingly benign, useful and convenient technological artefacts. The model identifies and discusses five main components of ICT artefact development and deployment: design, properties, affordances, appropriation and agent interests and locates them in a complex interrelated social ecology. The model provides a way to empirically examine how and why technology favours particular social or organisational outcomes.

Keywords

Surveillance, social ecology, design, appropriation, affordances

INTRODUCTION

Digitisation of information provides undreamt of production and access to information. It would seem a world where everyone is a winner where consumers are empowered by access to information and choice, popular sentiments about government policy can be quickly ascertained from blog sites and opinion surveys, businesses can produce and market more efficiently and effectively. As a consumer, there is the promise of convenience and empowerment. Such a personal technology as the iPhone promises the consumer to seamlessly and effortlessly use these technologies to obtain information about products, monitor their health, listen to music and orient themselves geographically and of course to purchase products (Andrejevic, 2007; Geddes, 2009). For the government and corporation, the information collected by these technologies can be used to improve services and offer a more 'customised' response. Not only is increased efficiency and effectiveness of the production process and supply chain promised but also an unprecedented understanding of consumer and political behaviour (Mount, 2010).

Indeed, in the age of information a concern for information flow, its collection, storage, mining and use seems anachronistic. Information has become a commodity and it has a use value that can only be realised by its flow (Lyotard, 1984). Information does indeed seem to 'demand' the integration and transmission of information. However, such information collection and integration does not come without a price. There is the misuse of the information and personal details that may arise should the integrated information be lost or stolen. Geddes (2009) for example, explains that the level of personal detail remaining in a mobile telephone, even after most information has been deleted by the user, is substantial and could easily be used for identity theft, stalking and credit card fraud. The spectre of 1984 with the government knowing more and caring more about its citizens than might be necessary and desirable is well known. However, there is also the emerging threat that private businesses and corporations may also know much more than we would like them to know.

The rise of 'dataveillance'(Clarke, 1988) 'surveillance society', (David Lyon, 1994) and the 'superpanopticon' (Poster, 1990) have been well described by authors such as (Andrejevic, 2007; Campbell & Carlson, 2002; Gary T. Marx, 2002; Webster & Robins, 1993). It would seem that, contrary to popular views of ICT as empowering, there is a very real danger of increased control by the state, by businesses and by employers. This is both surprising and alarming and raises important political issues for civil society.

For the Information Systems discipline it raises the issue as to how and why the introduction of information technology is leading to greater 'dataveillance'. A key theoretical problem in Information Systems concerns how new technology interacts with people, businesses and organisations to have particular social and organisational outcomes. Some outcomes will be desired, some may lead to changes in the distribution of power, and others may be in some way undesirable or rejected. Most will have unanticipated outcomes. One of the central tasks we believe of Information Systems is to examine how from the set of possible outcomes, particular outcomes are realised.

The challenge we have set ourselves is to develop a conceptual model that identifies the key elements of the process of this technology *cooption*. Technology cooption, stresses the co-construction of the technology use and appropriation by the designer, owner of the designed artefact, and the user. The more orthodox terms of technology diffusion, acceptance or adoption implies a certain given-ness of the technology; something that is taken up or left. An artefact is designed and produced and the user adopts or fails to adopt the artefact. What we wish to include, is that how an artefact is adopted may be unintended by the designer or owner of the design, and future design may incorporate or constrain ways of using the artefact. Finally, cooption also points to the notion that by use and appropriation of an artefact, the context of use changes, enabling more, less or different use opportunities but also transforming our lives and changing our selves. In sum, co-option stresses the interplay between the various agents imagining, developing, using and restricting the technology, the interaction of the potentialities of the technologies with the agents themselves and the resulting social/organisational outcomes.

The purpose of this paper is to introduce a simple model of technology cooption and to illustrate the model by describing how the properties of new information technology and interactivity, and the agents involved in particular, lead to 'surveillance creep' and increased management and measurement by the state, corporation and employer over the citizen, consumer and employee. The model is what sociologists describe as a theory of the middle range (Merton, 1968). As shall be described, it is underpinned and receives much of its dynamic from our understanding of the broader social currents and attempts to explain how these broader trends interact with agents engaged in the making and using of technology and the affordance those technologies offer.

SURVEILLANCE CREEP AND TECHNOLOGY COOPTION

Our initial question was that given the promise of empowerment for the citizen, consumer and worker of information technology, why does it appear, according to a near consensus of commentators, to be doing the exact opposite (Andrejevic, 2007; Campbell & Carlson, 2002; Clarke, 1988; David Lyon, 1994; Gary T. Marx, 2002; Poster, 1990; Webster & Robins, 1993)? Why is there surveillance creep? Why, in the infamous words of Scott McNealy of Sun Microsystems is there 'no such thing as privacy on the Internet' and that we should 'just get over it'. Is it an inevitability emerging from the new technologies? Do the new, interactive technologies have an inherent bias towards dataveillance and surveillance creep (Innis, 1951)?

There appear to be four clusters of research streams and responses regarding surveillance creep. The first is that of cataloguing surveillance creep and its associated technologies and what is happening. The pioneering work of Clarke (1988), who coined the term 'dataveillance' to refer to this phenomenon, is important in this regard. This work has shown us what has happened and the potentialities of the technologies for what could happen (for eg., Akin, 2009; DeVries, 2003; Kizza & Ssanyu, 2005; G. T. Marx, 1985; Slettemeås, 2009; Wen & Gershuny, 2005; Whitaker, 1998).

A second strand has attempted to identify the social drivers of surveillance creep. One of the most influential has been what might be considered a 'family' of social theories that are centrally concerned with the problem of government. These theories cover firstly, the emerging state, secondly the welfare of citizens and latterly the governance of consumers (Andrejevic, 2007; Bauman, 2008; Beniger, 1986; Giddens, 1987; Higgs, 1997). According to Lyon (2001, pp. 109-125). The first can be described as a "Big Brother" perspective and concerns state formation and the imperative of military competition between states and with subjecting citizens to central government control (e.g. Giddens, 1987). The second is a "Soft Sister" approach which employs and considers the kind of surveillance necessary to make the welfare state possible (eg. Beniger, 1986 pp 407-425; Cohen, 1985). Related to this approach and often Marx-inspired, are studies that regard surveillance technology as a weapon in the class struggle, one intended to subject the consumer (Beniger, 1986 pp. 344-389; Gandy, 1993 pp 95-122; Parenti, 2003 pp 131-150) and the employee (e.g. Marx, 1990) to the will of those in possession of capital goods (Bennett & Raab, 2003 p. 24; Lyon, 2001 pp 112-113).

These families of social theories and approaches help to explain *why* surveillance creep is occurring. They also introduce the concepts of conflict of power between state and citizen, corporation and consumer, which is often lacking in IS research.

A third strand has been ethical and legal to determine whether there is a legal or ethical defence against surveillance creep. This is usually discussed in terms of privacy. Lindsay (2005) in his extensive review of this, suggests not. Lindsay among others (eg., Cohen, 2000) suggest that privacy is a flawed and often inchoate concept where the concerns of the individual can often be readily dismissed by appeals to the commonweal (e.g. security and economic benefits). There is in a sense, nothing to stop surveillance creep.

Finally, there is the 'temptation theory' of technology that contends that surveillance enabling technology is so powerful, inexpensive and unobtrusive now that the temptation to use it is simply too great particularly in the face of weak ethical or legal opposition and societal fears about terrorism (see for example, Akin, 2009; O'Harrow, 2006; Rosen, 2004; Winner, 1980 pp 290-300).

With the partial exception of temptation theories, none of these theories and approaches to our knowledge have attempted to identify how the technology itself is coopted. They tend to explain what has happened and why but not the processes by which the technologies themselves are taken up, the various ends they are put to and how this produces surveillance creep. At best we get an overall view of how the consumer is duped into unequal bargains or how the citizen is unaware of the reaches of surveillance (eg. Fernback, 2007). This area, we believe is not only under theorised but that it is a key task of Information Systems to study the relationship of technology to the agents involved and how the adoption or cooption of the technology occurs. In terms of temptation theories, it needs to identify what it is that makes the technology simply too 'tempting' not to exploit.

Our work is to focus on how surveillance creep occurs, or in this introductory paper of our social ecological model, how technology in our everyday life proves 'tempting' and is coopted for multifarious and potentially conflicting purposes by the agents involved and how such cooption of technology leads to surveillance creep.

A SOCIAL ECOLOGICAL MODEL FOR TECHNOLOGY COOPTION

Kranzberg's first law of technology states that: "Technology is neither good nor bad; nor is it neutral"(Kranzberg, 1986). By this, Kranzberg means that technology interacts with the social ecology in ways that are difficult to foresee or control. By social ecology (Kranzberg, 1986) or information ecology (Davenport & Prusak, 1997; Nardi & O'Day, 1999) we mean a 'system of people, practices, values and technologies in a particular local environment' (Nardi & O'Day, 1999). The term 'ecology' is appealing as a metaphor because it emphasises a process of dynamic complex interactions, conflicts and struggles that lead to particular ecological outcomes. It looks at *how* things come about. As an ecology it also provides a nexus between the physical properties of technology and their human design and use.

The same technology can be 'good' or 'bad' depending on the context and indeed whether a short-term or long-term perspective is taken. Technology is designed, and as such, it is a reflection of a society's values and power relationships. Embodied in the design are decisions about who will use the technology, how they will use it and to what purpose. However, technology may be used and customised by people in ways not envisaged by the designers (Mackay & Gillespie, 1992). This raises the question of what it is about a particular technology that enables such unplanned and unintended uses. A useful approach for thinking about this issue is the concept of affordances. In simple terms, an affordance is an action possibility that involves the interaction between an actor's capabilities and the real, objective or physical properties of an environment (Scarantinoyz, 2003) or in this context the physical properties of technology.

We contend that there are five key elements that effect the cooption of a technology and which produce a particular social or behavioural outcome such as surveillance creep. This forms a design and use cycle, which is provided in Figure 1.

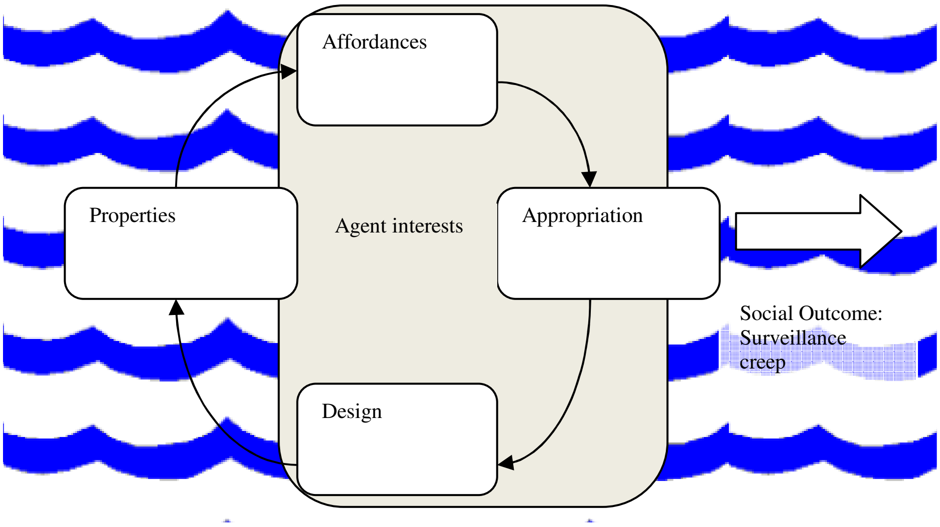

Figure 1: Social ecological model for technology cooption

The circular arrows and the elements (design, properties, affordances, appropriation, agent interests) describe the design and use cycle. It is circular to highlight the ongoing process of design and use. A particular IT artefact is designed with particular physical properties. These properties provide affordances that are taken up by agents. These affordances, which may or may not have been explicitly designed, are then appropriated by various agents to address their interests. This is how the technology is used, how it is adopted and adapted by the user. This in turn leads to new design that might design out undesired features or enhance desired ones. A similar approach to considering how technology is coopted is the work of (Carroll, 2004). While Carroll (2004) focuses on appropriation as part of the design process, our interest is how appropriation occurs, especially the interests of the agents that impact this process.

In the centre of the circle are the interests of the agents – the users, designers, and owners of the technologies. Such agents may include software designers, businesses, governments, citizens, employees and consumers. As shall be described further below the interests of these agents will differ and at times conflict according to what they see as an affordance, what they appropriate and use, and what they see as desirable designs.

The model is informed from three disciplinary sources that place human practice and engagement as its ontological building blocks. This includes design theory where the design of technological artefacts is characterised as a socio-cultural endeavour (see for example Rosenman & Gero, 1998), ecological psychology and the work of affordances where the human agent is not a passive recipient of technology but comes with certain abilities, predilections and viewpoints (pre-existing perspective?) on any given technology (see for example Gaver, 1996; Norman, 1988) and finally the practice theories of sociology which introduce the notions of appropriation that underpin and circumscribe the available practices and perspectives' of the agents and their technologies (Giddens, 1984; Schatzki, 1996). This is what we refer to as the social ecology, which is represented in the model by the wavy lines. The circular form of the model is derived from the iterative nature of design and use or appropriation as mediated by agent interest.

From this social ecology of interests, design, properties, affordances and appropriations, social outcomes are produced as a result of the playing out of the possibilities in design and properties between the different interests of the agents. We also suggest that it is an essentially contested process and one that is generally an unequal one. It is contested because agents use technologies according to their own interests, and it is unequal as the owners of the design of the technology are in a far better position to realise their interests.

The model allows the researcher to drill down into each of the elements for greater examination while having some understanding of where the element fits into the larger social ecological context. It also shows how each element impacts other elements and contributes to social outcomes. We believe that how technological artefacts interact with human agency to be a central question of Information Systems. The model also places issues of interest, power and conflict as being central. How technology is coopted is potentially a contested phenomenon.

In the next section, we illustrate how our model sheds light on ICT surveillance creep.

THE SOCIAL ECOLOGY MODEL AND ICT SURVEILLANCE CREEP

Design

While design means different things to different people, Winograd (1996) argues that through the various definitions of design there runs a common thread 'linking the intent and activities of a designer to the results that are produced when a designed object is experienced in practice'. Artefacts thus reflect the intentionality of the designer which consciously or unconsciously reflects society's values (Nissenbaum, 2001). And since much technology is designed by corporations to pursue their interests, designs will favour these aims rather than broader social concerns such as privacy. For example, when Netscape invented cookies in 1994, no effort was made to address privacy issues; the browser did not provide cookie management tools nor were cookies even mentioned in the documentation (Shah & Kesan, 2009). It was only the public uproar after the Financial Times (Jackson, 1996) ran a story about the cookies that Netscape began a redesign that gave users the option to turn cookies off.

Shah and Kesan (2009) conclude that as a society we should not expect that firms will uphold values for the greater good if these values are in conflict with the profit motive. While this point is arguable, what is certain is that technology is designed and can thus be engineered in ways to intentionally destroy privacy, for example to capture consumer information or to produce audit trails (Froomkin, 2000). Conversely, privacy enhancing technologies could be designed. For instance, designers could engineer technologies that withheld or did not gather identifying information (Froomkin, 2000). Technologies are designed to open up certain possibilities and close down others and this outcome may be intentional or unintentional. Lack of privacy and surveillance may be wittingly or unwittingly built into the design. Perhaps most commonly technology is designed blindly without serious thought towards privacy implications or other social implications but may nevertheless provide privacy eroding affordances.

Properties of ICT

A designed artefact by its nature exhibits various properties. In this context, we define a property as a real or objective attribute of the technology. Properties are characteristics of the technology, and while a technology may have many properties, the ones of interest are those that support the goals of the agents involved. It is this interaction between the properties of the technology and the goals of the agent that give rise to affordances.

Technologies may be built on other technologies with resulting properties. For example, cookies provide a means for a website to store text on a user's computer and typically contain a unique identifier, and expiration date, and the domain name the cookie is valid for. When the user requests a site, this unique identifier is also sent to the website. Websites can then use this unique identifier to retrieve information about the user including pages visited, ads that the user has clicked on, and page preferences. Cookies are built on a combination of Internet and browser technology, web servers, storage devices and usually database management systems. While individually, each of these technologies has many properties, the ones of interest are those that work together to provide cookie technology. Some of the relevant properties include:

- The capacity of web servers or databases to generate unique identifiers and other information and send them back to the browser over the Internet.
- Browsers' capacity to receive the unique identifiers and other information and save this data as a file on the user's machine.
- Browsers' capacity to locate, on the user's hard-drive, previously stored cookie files for a particular website.
- Capacity of browsers and Internet technologies to send the cookie information back to the originating website with page requests
- The capacity of databases to save and retrieve large amounts of information associated with a unique identifier.
- Capacity of the browser to support banner ads, which allows third party organisations to also store cookies on the user's machine.

It is an agent's interaction with these properties of cookie technology that gives rise to various dataveillance affordances, in other words an affordance is an emergent action possibility, it is something that the technology can be brought to do that is within the boundary of consciousness or arc of intentionality of the agent (Dreyfus, 1996).

Affordances

The word affordance was coined by ecological psychologist James Gibson (1977) and refers to the action possibilities an environment can offer an actor. The affordance concept was popularised by Norman (1988) in his book 'The Design of Everyday Things'.

Dreyfus (1996) drawing on Gibson (1977) and Merleau-Ponty (1962) provides a useful approach to understanding affordances. Dreyfus argues there are three aspects to an affordance or what makes a thing an action possibility. Firstly, the physical properties of the object must meet or address at the very least minimum human physical capabilities. Secondly action possibilities emerge as a result of the general skills that a human being may possess. Finally, affordances arise because of the stock of cultural skills within a community. Dreyfus uses the example of the chair. A chair affords sitting for Westerners because, one, it is a physical shape that permits the action and humans get tired standing, secondly sitting can be learned, and finally it forms a cultural practice in Western society.

The concept of affordance provides the nexus between the physical property and use. In the context of social interaction, affordances have been used to describe the material properties of the environment that affect how people interact (Gaver, 1996; Kreijns & Kirschner, 2001). This is not to say that social behaviour cannot be accounted for in terms of 'social conventions' and 'communities of practice', but the ecological psychology approach examines how social activities are embedded in and influenced by the physical environment (Gaver, 1996).

Our interest here is how the properties of an ICT system influence and interact with social activities leading to non neutral or ‘biased’ outcomes (Innis, 1951; Kranzberg, 1986). For example, we can examine how privacy or the lack of privacy is embedded in and influenced by the properties of the technology.

For example, the cookies properties outlined previously can provide several emergent dataveillance affordances including:

- The ability to profile an individual’s preferences and activities on a website without the consent or even the knowledge of the individual. If the individual also fills out registration forms or completes online purchases these profiles can also be linked to personally indentifying information.
- The ability to collect information across more than one website. Although cookies are usually site specific, the property of the browser that allows third-party components of web-pages to store their own cookies provides a means for cross-site profiling. This occurs because many businesses use agencies like DoubleClick to serve banner ads on their site. Since these type of agencies serve ads across many different sites they are able to track an individuals’ use across multiple sites and build up very detailed profiles. While the privacy risks to individuals of this practice are well understood (Shah & Kesan, 2009), it is unsurprising that in both Internet Explorer and Firefox allowing 3rd party cookies is the default setting.

Which affordances are perceived of the properties of a designed artefact depends to a large degree on a particular actor’s needs and goals. For the individual, Yahoo’s mashup tool, Yahoo Pipes, can afford the creation of a webpage that assembles, in one place, information of interest from a variety of sources. For Yahoo, the mashup tool can afford a means of understanding the interests of a large number of individuals; information that has value for marketers. This leads many to observe, free internet services are paid for using micropayments of our personal data (Andrejevic, 2007; Campbell & Carlson, 2002; Conti, 2006; Fernback, 2007).

Appropriation

Technologies are encoded with forms of use, some intended by the designer and some not (Mackay & Gillespie, 1992). The intended forms of use may be reinforced by advertising but the properties of the artefact may allow it to be used in unintended ways. For example, cassette recorders were designed to play pre-recorded tapes but the recording property provided an affordance that meant the device was widely used for recording from records (Mackay & Gillespie, 1992).

In using mobile phones, teenagers often avoid connection costs by the practice of pranking (calling and hanging up before the receiver answers). Using the property that allows the caller’s number to be displayed, the mobile phone affords teens a modern-day smoke signal. The same caller-id property may provide a call-screening affordance for other phone users.

The process by which users adapt the technology to meet their needs is called appropriation (Carroll, 2004), and we argue that it is the affordances of a technology, its ‘intentional arc’ that allow it to be appropriated by particular actors for particular purposes (Dreyfus, 1996). Some technological appropriations may be taken up and included in future designs of the technology while other appropriations will be closed out. Indeed, Bar et al.(2007) argue that the appropriation process is primarily a political battle for power over the configuration of the technology and hence who can use it and how it can be used.

Agent interests

Much of the business and IS literature, if not most, views product development cycles like our model as a consensual model where everyone is a ‘winner’ and the customer the winner above all. The implicit assumption or belief is that the business designs and appropriates a system for the benefit of the consumer. There is not only a belief that in the long run the customer is sovereign and those businesses that meet the needs and wants of the consumer will ultimately triumph but also that every step along the way, the strategies and tactics businesses employ, serve the interests of the customer.

It is however, quite plain that the consumer is not necessarily ‘king’ but is often just as much an adversary as are other businesses in strategic and tactical battles for business supremacy or survival. After all businesses survive and run on profit and the consumer is merely a means to that end. As Porter (2001) pointed out, the use of ICT for efficiency and effectiveness, production and distribution, is a business imperative not a strategy. Strategy, among other things, involves a combination of getting the customer to buy more of your product and purchasing it in a manner that is advantageous to the business. Porter (2001) adds, that long-term advantage is doing this in a way that is difficult for other businesses to copy.

Put this way, there is conflict between the interests of the consumer and the business. In turn this sets up a conflict of interest between how new technologies are appropriated and designed. It is at this point that features can be designed in or out, particular affordances are appropriated that may not necessarily be in the interest of the consumer/citizen. At the centre of this model is power: the power of each agent – designers, owners, managers, users, employees, employers and citizens and consumers over the design of the artefact and the properties and how the artefact is used and to what ends. Power is not distributed equally and therefore the interests of the most powerful, well-organised agents tend to dominate. Power also operates at the level of the social ecology of the model – what is thinkable and what is permissible, it forms and structures the envelope of possibility of the social ecology itself (Foucault, 1976; 2002)

According to the surveillance literature most technological applications point to a Mephistopelean deal between the corporation and the consumer (for example, Andrejevic, 2007; Campbell & Carlson, 2002; Fernback, 2007). The corporation promises convenience and customisation and obtains the consumers' data, their shopping soul. The corporation in terms of the knowledge and understanding they receive concerning consumer behaviour and response is far greater than the convenience promise. In the words of Andrejevic (2007): "We are invited to actively participate in staging the scene of our own passive submission – and to view such participation as a form of power sharing" (p. 15).

This forms the crux of the conflict between the interests of the consumer and the corporation. The ICT promises empowerment but actually delivers surveillance and management of consumer behaviour. It is a short step from here to consider the design of the systems to produce such surveillance that the ICT affords. Significantly most of the control of such design is in the hands of the corporation. Looked at from the consumers' point of view the empowerment promised in choice and interactivity is immense. To illustrate this conflict, consider the following examples. It is easy enough to imagine that the iPhone could be used to scan items to determine their carbon footprint, nutrition details and the labour practices of the business: what might be called the global impact of the consumer item. The phone could have an application that undertakes the necessary trade-offs including price to decide on which item to purchase. That would be empowering. Possibly even more empowering would be an iBot that remotely interrogated retailer databases and undertook comparisons of the cost and global impact of the delivered item to the home. However such a system, while technically feasible would raise enormous resistance among food retailers and manufacturers.

The objections to such a system would include the fear that such a system would reduce demand if people knew the true cost or 'global impact' of the items. The use of the iPhone might lessen impulse or unplanned purchases and the iBot certainly would destroy such impulses completely: the chocolate bars placed temptingly beside the milk would not seduce the iBot algorithm. Quite simply the databases required for such a system are unlikely to be forthcoming as there is little organised demand for such systems.

It is much more likely that systems incorporating these elements would be designed and appropriated by retailers for their strategic and tactical ends. Such a system could be used to interrogate a database on limited grounds, e.g. calorie intake of a food item. This interrogation would be collected and compared to aggregate purchase data. Varying information, product placement, special deal and promotions could be compared on purchase. The interrogation would also provide an opportunity for cross promotions and up-selling. Such a system would be very empowering to the retailer. Of the two systems it is far more likely that this latter system would be designed and implemented, if it hasn't quite already.

THE OUTCOME OF TECHNOLOGY COOPTION: SURVEILLANCE CREEP

We argue that the net effect of this social ecology process and the struggle or conflict between the various agents is surveillance creep as shown by the arrow in Figure 1. The net effect could be consumer (or citizen or worker) empowerment. For some applications and technologies the social ecology process may lead to consumer empowerment rather than surveillance creep. The development of open source software and the peer-to-peer file sharing networks are two examples that led to greater user empowerment. The most important point however is that the outcome is a product of the struggles of the agents over the appropriation of the affordances and the design of the technology.

Surveillance creep is at least in part an outcome of these quotidian local and specific struggles. It involves business and employees of businesses organizing and appropriating the technology to reach the strategic and tactical ends of the business and the motivations of managers and employees to those ends: satisfaction with a job well done, prospects for promotion, loyalty to the business, the technical interests in the work and staving off potential business failure and job loss. In comparison, the consumer is far less organized and at this point we propose that the overwhelming and general evidence for surveillance creep lies in the lack of power and organizing capacity of the consumer vis-à-vis the corporation that allow businesses to collect, store and manage data in the pursuit of specific corporate goals.

Surveillance creep does appear natural, as an unplanned outcome. It generally is. If it were not so, such creep would rightly be seen as an 'unnatural' political exercise. Only when each of the elements that constitute technology cooption is examined can we see how social processes and imperatives interact with the temptations of possibility to lead to surveillance.

It needs to be emphasized that surveillance creep is a net or overarching outcome of these local struggles over appropriation and design and the empowerment or advancement of whom. Different technologies provide affordances that are 'biased' towards our simplified 'empowerment – surveillance' framework. The semi-porous or near boundarilessness nature of the internet provides a haven and organising capability for non-socially approved activities such as pornography, hackers and alternative politics. The internet as the wild west should not be under-estimated (eg., Rheingold, 2000). On the other hand, replacing an analogue key with a swipe card enables an employer to monitor office usage. Digitisation affords monitoring in cultures which view such monitoring as a means to improve performance and employee discipline. Grounded in such a context and the relative strengths of employees and employers, the 'temptation' for monitoring proves 'natural'. The ability to monitor may be a 'bias' of the technology and supports (Innis, 1951) groundbreaking work on the bias of technology.

The model as depicted has not, however described effects exogenous to the local struggle other than those mediated by the agents. Our view is that this does not exhaust the influence of such exogenous factors. Agents draw upon the prevailing stock of knowledge, 'Weltanschauung' to inform their choices, motivations and what works.

CONCLUSION

The model provides an analytical tool for understanding how the introduction of information technology can lead to social outcomes such as surveillance creep or, potentially consumer empowerment. While the model and discussion presented has been limited to surveillance and the interests and positions of corporations and consumers, the model can be further developed to incorporate government/citizen and employer/employee positions and to generalize from surveillance to the bureaucratic management (Lefebvre, 1971) and governmentality of the information age (Miller & Rose, 2008). We believe that with development and refinement it can provide a general model for technology cooption.

The strength of the model is firstly that it views information design and appropriation as being essentially contested: the researcher must understand the differing motivations, interests and knowledge and also differing capabilities of acting on and for their interests. Secondly, by its focus on properties and affordances it provides the opportunities to examine how particular technologies are 'inherently biased'. This and the elements of appropriation, design and interests provide the answer to Kranzberg's puzzling aphorism that information technology is not neutral. Most importantly, however, the model provides a middle range theory for empirical analysis by identifying the key elements and their proposed links.

REFERENCES

Akin, L. L. (2009, 06/22/09). Activity monitors: aka: cell phone and computer eavesdroppers. *The Forensic Examiner,* 46-49.

Andrejevic, M. (2007). *iSpy : surveillance and power in the interactive era*. Lawrence, Kan.: University Press of Kansas.

Bar, F., Pisani, F., & Weber, M. (2007). *Mobile technology appropriation in a distant mirror: baroque infiltration, creolization and cannibalism*. Paper presented at Seminario sobre Desarrollo Económico, Desarrollo Social y Comunicaciones Móviles en América Latina. Convened by Fundación Telefónica in Buenos Aires, April 20-21, 2007. from http://arnic.info/Papers/Bar_Pisani_Weber_appropriation-April07.pdf.

Bauman, Z. (2008). *Does ethics have a chance in a world of consumers?* Cambridge, Mass.: Harvard University Press.

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge, MA: Harvard University Press.

Bennett, C. J., & Raab, C. D. (2003). *The governance of privacy: Policy instruments in global perspective*. Aldershot, UK: Ashgate.

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586-606.

Carroll, J. (2004). *Completing Design in Use: Closing the Appropriation Cycle*. Paper presented at the European Conference on Information Systems (ECIS).

Clarke, R. A. (1988). Information Technology and Dataveillance. *Communications of the ACM, 31*(5), 498-512.

Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object *Stanford Law Review, 52(5)*, 1373-1438.

Cohen, S. (1985). *Visions of social control : crime, punishment, and classification*. Cambridge Oxford, UK ; New York, NY, USA: Polity Press : Blackwell.

Conti, G. (2006). *Googling considered harmful*. Paper presented at the Proceedings of the New Security Paradigms Workshop

Davenport, T. H., & Prusak, L. (1997). *Information ecology : mastering the information and knowledge environment*. New York: Oxford University Press.

DeVries, W. T. (2003). Annual review of law and technology: III. Cyber law: A. Privacy: Protecting privacy in the digital age. . *Berkeley Technology Law Journal, 18*(283-311).

Dreyfus, H. L. (1996). The Current Relevance of Merleau-Ponty's Phenomenology of Embodiment. *The Electronic Journal of Analytic Philosophy.*(4).

Fernback, J. (2007). Selling ourselves? *Critical Discourse Studies, 4*(3), 311-330.

Foucault, M. (1976). Two lectures. *Power/knowledge: Selected Interviews and Other Writings, 1972-1977*. M. Foucault and C. Gordon. Brighton, Sussex, Harvester Press**:** xi, 270.

Foucault, M. (2002). The subject and power. *Power: Essential Works of Foucault 1954-1984*. in J. Fabian, (ed) London, Penguin.

Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review, 52*, 1461-1543.

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information.* Boulder, CO: : Westview Press.

Gaver, W. W. (1996). Affordances for interaction: the social is material for design. *Interactions, 8*(2), 111-129.

Geddes, L. (2009). Rat in your cellphone. *New Scientist, 204,* 34-37.

Gibson, J. J. (1977). The Theory of Affordances. In R. E Shaw and J. Brasford (Eds.), *Perceiving, acting, andknowing: Toward an ecological psychology* (pp. 67-82): Hillsdale, NJ: Lawrence Erlbaum Associates,

Giddens, A. (1984). *The Constitution of Society: Outline of the theory of structuration.* Cambridge: Polity Press.

Giddens, A. (1987). *The nation state and violence*. Berkeley: University of California Press.

Higgs, E. (1997). The determinants of technological innovation and dissemination: The case of machine computation and data processing in the general register office, London, 1837-1920. . *Jahrbuch fur Europaische Verwaltungsgeschichte,, 9*(161-178).

Innis, H. A. (1951). *The bias of communication*. [Toronto]: University of Toronto Press.

Jackson, T. (1996, 12 February). This Bug in Your PC is a Smart Cookie. *Financial Times,* p. 15.

Kizza, J. K., & Ssanyu, J. (2005). Workplace Surveillance In J. Weckert (Ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (pp. 1-18). Hershey, PA: Idea Group.

Kranzberg, M. (1986). Technology and History: "Kranzberg's Laws". *Technology and Culture, 27*(3), 544-560.

Kreijns, K., & Kirschner, P. A. (2001, October 10-13). *The Social Affordances of Computer-Supported Collaborative Learning Environments.* Paper presented at the 31st ASEE/IEEE Frontiers in Education Conference, Reno, NV.

Lefebvre, H. (1971). *Everyday life in the modern world.* London,: Allen Lane.

Lindsay, D. (2005). An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. *Melbourne University Law Review, 29*(1), 131-178.

Lyon, D. (1994). *The electronic eye : the rise of surveillance society*. Cambridge [England]: Polity Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life.* Buckingham: Open University Press.

Lyotard, J.-F. (1984). *The postmodern condition : a report on knowledge*. Manchester: Manchester University Press.

Mackay, H., & Gillespie, G. (1992). Extending the Social Shaping of Technology Approach: Ideology and Appropriation. *Social Studies of Science, 22*(4), 685-716.

Marx, G. T. (1985). I'll be watching you: Reflections on the new surveillance. *Dissent, 32*, 26-34.

Marx, G. T. (2002). What's new about the "New Surveillance"? Classifying for change and continuity. *Surveillance and Society, 1*(1), 9-29.

Merleau-Ponty, M. (1962). *Phenomenology of perception*. New York,: Humanities Press.

Merton, R. K. (1968). *Social theory and social structure* (1968 enl. ed.). New York: Free Press.

Miller, P., & Rose, N. (2008). *Governing the present: Administering economic, personal and social life*. Cambridge: Polity.

Mount, F. (2010). Living with monsters. *London Review of Books, 32*(8), 24-26.

Nardi, B. A., & O'Day, V. (1999). *Information ecologies : using technology with heart*. Cambridge, Mass.: MIT Press.

Nissenbaum, H. (2001, March). How Computer Systems Embody Values. *Computer 34,* 118-119.

Norman, D. A. (1988). *The Design of Everyday Things*: Doubleday.

Norman, D. A. (1988). *The design of everyday things / Donald A. Norman* New Yoir: Doubleday.

O'Harrow, R. (2006). *No place to hide: The terrifying truth about the people who are watching our every move*. London: Penguin Books.

Parenti, C. (2003). *The soft cage: Surveillance in America from slavery to the war on terror*. New York: Basic Books.

Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review*(March), 63-78.

Poster, M. (1990). *The mode of information : poststructuralism and social context*. Cambridge: Polity Press in association with Basil Blackwell.

Rheingold, H. (2000). *The virtual community : homesteading on the electronic frontier* Cambridge, MA: MIT Press.

Rosen, J. (2004). *The naked crowd : reclaiming security and freedom in an anxious age*. New York: Random House.

Rosenman, M. A., & Gero, J. S. (1998). Purpose and function in design: from the socio-cultural to the techno-physical. *Design Studies*(19), 161-186.

Scarantinoyz, A. (2003). Affordances Explained. *Philosophy of Science, 70*, 949–961.

Schatzki, T. R. (1996). *Social Practices: A Wittgensteinian Approach to Human Activity and the Social.* Cambridge: Cambridge University Press.

Shah, R. C., & Kesan, J. P. (2009). Recipes for cookies: how institutions shape communication technologies. *New Media & Society, 11*(3), 315-336.

Slettemeås, D. (2009). RFID—the "Next Step" in Consumer–Product Relations or Orwellian Nightmare? Challenges for Research and Policy. *Journal of Consumer Policy, 32*(2), 219-244.

Webster, F., & Robins, K. (1993). I'll be watching you: Comment on Sewell and Wilkinson. *Sociology, 27*(2), 243-252.

Wen, H. J., & Gershuny, P. (2005). Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges. *Human Systems Management, 24*, 165-173.

Whitaker, R. (1998). *The End of Privacy: How Total Surveillance Is Becoming a Reality*: New Press.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(121-136).

Winograd, T. (Ed.). (1996). *Bringing design to software*. New York: ACM Press.

ACKNOWLEDGEMENTS

We would like to acknowledge the anonymous reviewer who provided many helpful and insightful comments.

COPYRIGHT