Monitoring Technologies and Digital Governance

Peter Danielson
University of British Columbia, Canada

INTRODUCTION

Digital government is a technological adventure. It applies new technologies—in particular, computer-mediated communication—to the ongoing development of democratic forms of government. While the primary focus in digital government literature is on computer-mediated politics and formal governance, these technologies have wider effects. Generally, new information technologies enable new forms of control (see Beniger, 1986, for an excellent history and the general connections between information, control, and governance). The technological changes that make digital government an option alter the possibilities of governance at all levels. Driven by the declining price of computer hardware (so-called Moore's law) sensors (e.g., cameras, RFID tags), computers and networking make it possible to find out about and to control many hithertofore uncontrolled aspects of our lives. This article considers the effect of new monitoring technologies in the broad sense introduced by McDonald (2001) as inclusive of the range of control mechanisms—personal, informal, social, market, legal, and political—that we deploy.

In general, we expect technological innovation to create ethical problems. Innovations move communities from technological and social situations for which their norms are well adapted to new situations in which the fit tends to be worse (Binmore, 2004). Even seemingly small changes in technology, especially communications and monitoring technology, produce significant stress on norms. (Consider how cell phones and then cell phone cameras challenge norms governing privacy in public spaces.) Therefore, we should expect moves toward digital government to face ethical problems. This article considers problems due to a suite of monitoring and surveillance technologies that promises significant benefits but raises issues in terms of the values of control, privacy, and accountability.

BACKGROUND

We need to remember how new the ensemble of monitoring technologies is. Gelernter's (1991) seminal proposal to build a mirrorworld allowing citizens to examine many aspects of their local government and healthcare system in real time seemed wildly utopian when published in the early 1990s. Now, the Internet has become so integrated into everyday life in rich countries that schoolchildren are surprised that some books are not available online.

This article suggests that we should consider a wide range of examples in order to form our evaluation of monitoring technologies. Our approach contrasts with what is favored in the sociological and popular literature critical of technology, much of which focuses on two metaphors: Orwell's (1949) Big Brother and Foucault's (1977) account of Bentham's (1969) panopticon prison design (Lyon, 1994; Mann, Nolan, & Wellman, 2003; Rheingold, 2003). Both metaphors suggest that more monitoring technology means stronger governance in the sense of tighter control. However, as we shall see, it is not clear that introducing surveillance in some contexts (we will consider the case of the clinical consulting room) has these unidirectional effects. Rather than trying to coin less misleading metaphors, it seems better to engage in an informal technological survey, forecast, and risk assessment. We will consider selected cases of new monitoring technology, sketching how each changes the players, options, strategies, social norms, and outcomes in social situations and using what we call an informal strategic approach (Danielson, 2005). Indeed, merely surveying some of the myriad new monitoring technologies currently available should be educational, as most of them have a low public profile.

To draw on a particularly significant example, the number of video cameras used for surveillance has increased enormously. Much of the public space in London is under government video surveillance, and the estimated 200,000 cameras in Shanghai are planned to double by 2010 (Epstein, 2004). The Chinese example makes two additional points. First, as the world's leading non-democratic state, China raises the question of the role of democracy in digital government. We face a terminological choice. On the one hand, digital government could be given a neutral interpretation related only to efficient governance of whatever kind. On this reading, effective (but non-democratic) digital government would include China's use of video or network surveillance to monitor

and suppress political dissent (Walton, 2004). This article will follow the alternative convention, under which digital government assumes democratic goals. (The clearer term for this value-driven approach is *digital democracy*.) Similarly, we shall use the term *governance* with a normative bias, looking for ways to improve self-control and legitimate governance, for example, and not manipulation or tyranny.

Second, Epstein (2004) reminds us that by turning to surveillance cameras, China deploys modern technology to perform a job that, under Mao Zedong, was largely society's responsibility. This brings us to a recurring theme: technology may not simply introduce or increase governance, but it may shift the balance between various controlling mechanisms and parties.

While surveillance is timely, relevant, and obviously controversial, we will not begin our account with surveillance for several reasons. First, surveillance technologies are unique in their strategic functions. Often, they gain much of their power by revealing themselves to their subjects; think of all those signs announcing hidden cameras. (This is the shared truth in the Big Brother and panopticon metaphors.) Truly invisible surveillance cannot deter people as readily as more obvious surveillance. Therefore, surveillance understates one of the main problems with new monitoring technologies in a democracy—their generally unnoticed role. This leads to the second, more general reason to put off discussing surveillance: it is very complex. In this article, we use *monitoring* to include surveillance (see Danielson and McQuade [2005] for a more nuanced account).

We select our examples with three goals: (1) to cover a wide range of emerging technologies; (2) to use technologies embedded in varied social relationships, institutions, and cultures; and (3) to start with the simpler case of physical things, move to non-human animals, and end with persons. In effect, we will try to apply a simple Kantian model that ranks ethical significance as least for things and as most for persons. As we shall see, technological change will not respect this ethical scheme.

NEW MONITORING TECHNOLOGIES

Things

The technologies under consideration change ordinary objects like books, commodities in stores, cell phones, and cars in a characteristic way: they become easier to monitor. They cease to be isolated and become linked to a communications system, where they can be stored in a private database (at minimum) and perhaps even addressed and interrogated. These are forms of dataveillance, whereby things become linked to records in large databases. For example, UPC scanning allows shops to use customers to help to maintain inventory. Loyalty cards go further, linking products via their purchasers into purchasing histories that retailers use for planning or for selling to third parties.

This technology changes individuals' strategic situations; we should be asking who is scanning our purchases and transit tickets, which is a question most of us previously needed to ask only about our credit cards, identity papers, or driver's licenses. Unless people understand which personal information is being read or exchanged, their participation in transactions is unlikely to be fair. Perhaps introducing some new terms that are common in writing in this field will alert us to think of more things that are now part of an infosphere with an infocloud surrounding them. Or, in time, we may generalize from our experience with card and UPC scanners in shops and other venues. The Internet, which began as a research platform, continues to play that role. Several ongoing experiments help us to envision what we might expect from a developed infosphere that includes many of the objects we use every day. An example is the Microsoft Research Advanced User Resource Annotation (AURA) system, whose motto is "Annotate the Planet!" and which allows people to link products to arbitrary Web pages via their product identifiers.

Books and Barcodes

Books are a good place to start. They are familiar, full of information, and traditionally quite local and inert. That is to say, one can walk past the shelves in a library knowing that there is a great deal of information in the books but needing to take each one down and actually read it in order to find out it. Even then, one won't readily find out if one has already read it (and when), who else has read it, where it was reviewed, and how the reviewers rated it. Second, each book is created with a unique identity (the ISBN) that it wears on its barcode. This is the link between the traditional book and books enhanced with an infosphere. Readily available open-source software allows one to surf the infosphere of books by scanning their barcodes.

Barcoding can support various follow-up technologies. Some stores currently supply terminals that allow customers to check prices via barcodes. Local wireless networking would allow an allergy meter to alert a consumer with Internet-based information to avoid any of an open-ended list of allergens or any other features that they (or their agents) programmed into it. Projecting into the near future, one can imagine a multi-factor value analysis output: no serious allergy alert, mediocre nutrition, good environment, excellent price, personal use history, and so forth.