

RFID & Privacy in the Information Age
Opening Address
J. Clark Kelso
Chief Information Officer
State of California
December 1, 2005
Sacramento, California

Good morning, my friends. I'm pleased and honored to have been asked to open this forum on RFID & Privacy in the Information Age with a few remarks from my perspective as the State's Chief Information Officer. I hope that my comments will set a useful foundation for the rest of today's discussion.

It is useful I think to begin by acknowledging just how novel the policy and legal issues are that confront us today, and just how young the law is with respect to informational privacy.

As a commercially viable, cost-effective technology, RFID is a technology that is itself in its youth – beyond its infancy to be sure, and well established, but still far from full maturity. Because of its capacity accurately to identify, locate, track and share information, and because of the increased capacity of databases and computers to match and synthesize vast amounts of information in real or near real time, RFID is rapidly finding adopters and adherents, both in government and in the private sector. A few examples:

- The Department of Defense has widely deployed RFID technologies to track military vehicles and supplies.
- The United States Department of Agriculture is exploring the use of RFID in tracking and managing the nation's livestock, with concerns about how quickly and effectively the government could respond to rapidly contagious diseases that may imperil the commercial viability of those resources.
- Some public libraries are using RFID to replace barcodes and have discovered that RFID technologies substantially improve both service to the public and their own management of their libraries.
- Many hospitals now employ RFID technologies to guard against infant abductions and to reduce the incidence of accidental infant mismatching.

Other applications in the hospital environment that improve accuracy of treatment, as well as reduce costs of treatment, are being explored.

- RFID is being deployed in some amusement parks as a way of locating and finding friends and family within the park.
- And, of course, we have the example of Wal-Mart that has adopted RFID – and is insisting that its suppliers adopt RFID – to improve Wal-Mart’s inventory control and management.

One of the interesting things about this list is how diverse it is. From the military, to hospitals, to libraries to retailers – RFID has found important uses. And it has found these wide variety of uses because RFID is one of those transformational technologies that fundamentally changes the way organizations manage their resources and information. With RFID, we are not talking about a few marginal improvements in an asset management system. It’s not just a better database. It’s a whole new way of gathering information; it’s a whole new way about identifying and tracking organizational resources.

That is why I say that RFID technology is still in its youth. We have only just begun to learn how this technology can be used to improve services and reduce costs. But because of its flexibility and because it can deal at the most granular level with individual units, assets and people, RFID’s potential for growth and expansion seems quite enormous.

The law of privacy is also still quite young. Go back as recently as forty years and you would find that the law of privacy barely existed. There were a few dimly-recognized state law causes of action to protect some limited aspects of privacy, but the law was really quite disjointed and incomplete. It was only in the late 1960s and early 1970s that law and principles of information privacy began to emerge.

In the United States, the law of privacy has developed largely as a patchwork of specific enactments governing limited subject matter areas. Congress did not adopt at the federal level an over-arching set of privacy principles, although those principles have certainly found expression in Fair Information Practices promulgated first by the Department of Health, Education and Welfare in the 1970s and much more recently by the Federal Trade Commission.

This ultimately left gaps in the law that have been filled, often by additional

patchwork enactments, at the state and local levels of government. California expressly protects privacy in the privacy clause of the California Constitution, and we were one of the early states to adopt statutes dealing with informational privacy. I think it fair to say that California retains a leadership position in protecting privacy interests. There is a substantial amount of law already on our books, and we have had, and continue to have, members of the Legislature, including Senator Joe Simitian, who have committed substantial time and resources to examining privacy issues.

It is only relatively recently that Congress has involved itself directly in the regulation of privacy in broad business areas, such as the Graham-Leach-Bliley which dealt with financial services, the Health Insurance Portability and Accountability Act which deals with health information, and the Children's Online Privacy Protection Act.

On the international side of things, probably the most significant and useful developments have been the great work done by the Organization for Economic Cooperation and Development (OECD) in crafting and promulgating Fair Information Practices which were ultimately codified in OECD guidelines in 1980, and, much more recently, the European Union's Data Protection Directive which became effective in 1998.

All of these legal developments – virtually the entire law of information privacy – have taken place within our lifetimes. And that makes the law of information privacy still in a developmental stage, at least from a legal perspective. That is why, when we see new information technologies appear on the scene which have brand new abilities to collect information and brand new ways of using that information, we have a feeling that the technology may be running ahead of our capacity to use that technology consistently with our notions of information privacy.

Several years ago, the United States Department of Justice conducted a substantial survey of public attitudes about the government's collection and use of criminal history and other personal information. Overall, the survey results suggested a majority of Americans are comfortable with government use of personal information so long as that use is directly tied to real public benefits and public safety, and there are safeguards against misuse. The survey also indicated that privacy is an issue Americans care a great deal about.

But what I found most interesting in the survey results was the identification of three large segments of public attitudes about information privacy. First, the survey administrators identified – in their words – “Privacy Fundamentalists” who generally will reject any information gathering and favor strong legislation to protect privacy. At the other extreme, the survey identified those who were “Privacy Unconcerned,” those who will readily disclose private information for benefits and are likely to believe that public order and public safety are much more important than privacy. Between those two extremes are “Privacy Pragmatists,” who want to know a lot of details about what information must be disclosed, to whom, for what purposes, and to what end or benefit. The Privacy Pragmatists engage in a cost-benefit analysis and then make a final judgment about a particular collection and use of information.

The percentage of respondents in each of these three categories changed depending upon what type of information was involved. Not surprisingly, when the questions dealt with health information, the percentage of Fundamentalists increased. But when questions dealt with criminal justice uses or with consumer uses, the percentages of Unconcerned and Pragmatists rose.

This suggests to me that the public’s approach to information privacy in the United States is actually quite sophisticated and sensitive to the actual contexts in which privacy issues arise and to the proposed uses of any information that is gathered.

It also suggests to me that any discussion of privacy needs to be well grounded both in the actual details of the contexts and the information to be gathered and used, and in the specific privacy interests and protections that the law recognizes. In other words, this is not a subject that can be dealt with appropriately in broad strokes from 150,000 feet. Our analysis must be much more granular.

And that leads me back to the OECD’s Fair Information Practices guidelines. Even though we have not adopted the broad regulatory approach suggested by the OECD’s Fair Information Practices, I think that virtually any discussion of informational privacy issues in specific contexts – such as privacy in the context of RFID technologies – will be better informed by following the analytic framework established by those principles.

There are eight privacy design principles in OECD’s Fair Information Practices guidelines:

- Purpose specification principle -- The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Collection limitation principle -- There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data quality principle -- Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- Use limitation principle -- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or b) by the authority of law.
- Security safeguards principle -- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- Openness principle -- There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- Individual participation principle -- An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

- Accountability principle -- A data controller should be accountable for complying with measures which give effect to the principles stated above.

I believe that if we approach our discussion of RFID and privacy with an eye on the details – don't look on RFID as a single, monolithic technology to be regulated, but actually approach this topic from the perspective of specific business or regulatory contexts in which RFID may have a role to play – and with an eye on the full spectrum of Fair Information Practices and how they apply to these contexts, then I think we will ultimately find the most appropriate regulatory approach.

We may discover at the end of this journey that existing regulations adequately protect privacy within each or most of the contexts in which RFID may have application. Or we may discover that we have gaps in those existing laws to be filled. And we may discover some entirely new contexts in which RFID may be deployed where there is a need for a more comprehensive legislation or regulation. We won't know the answers to these questions unless we take the journey.

I want to thank the organizers of this conference for bringing us together in what I suspect is going to be the first of many interesting and important policy discussions on the topic of RFID and privacy.