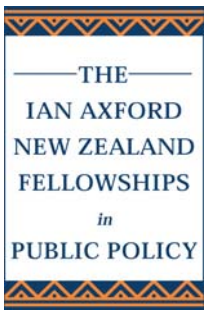

Safeguarding Consumer Privacy in a Technological Era: A Comparison of Privacy Protections in New Zealand and California

Prepared by

Saskia Kim

With funding from the sponsors of the
Ian Axford (New Zealand) Fellowships in Public Policy

July 2006

The Ian Axford (New Zealand) Fellowships in Public Policy programme is administered by

Fulbright New Zealand
PO Box 3465, Wellington, New Zealand
Telephone +64 4 472 2065, Facsimile +64 4 499 5364, Email info@fulbright.org.nz, www.fulbright.org.nz

ISBN 0-473-11336-8

THE IAN AXFORD (NEW ZEALAND) FELLOWSHIPS IN PUBLIC POLICY

The Ian Axford (New Zealand) Fellowships in Public Policy were named in honour of Sir Ian Axford, an eminent New Zealand astrophysicist and space scientist who is patron of the fellowship programme.

Since his education in New Zealand and England, Sir Ian has held Professorships at Cornell University and the University of California, and was Vice-Chancellor of Victoria University of Wellington for three years. For many years, Sir Ian was director of the Max Planck Institute for Aeronomy in Germany, where he was involved in the planning of several space missions, including those of the Voyager planetary explorers, the Giotto space probe and the Ulysses galaxy explorer.

Sir Ian is recognised as one of the great thinkers and communicators in the world of space science, and is a highly respected and influential administrator. A recipient of numerous science awards, he was knighted and named New Zealander of the Year in 1995.

The Ian Axford (New Zealand) Fellowships in Public Policy have three goals:

- To reinforce United States/New Zealand links by enabling fellows of high intellectual ability and leadership potential to gain experience and build contacts internationally.

- To increase fellows' ability to bring about changes and improvements in their fields of expertise by the cross-fertilisation of ideas and experience.

- To build a network of policy experts on both sides of the Pacific that will facilitate international policy exchange and collaboration beyond the fellowship experience.

Fellows are based at a host institution and carefully partnered with a leading specialist who will act as a mentor. In addition, fellows spend a substantial part of their time in contact with relevant organisations outside their host institutions, to gain practical experience in their fields.

The fellowships are awarded to professionals active in the business, public or non-profit sectors. A binational selection committee looks for fellows who show potential as leaders and opinion formers in their chosen fields. Fellows are selected also for their ability to put the experience and professional expertise gained from their fellowship into effective use.

We acknowledge and thank the following corporate and government sponsors that support the Ian Axford (New Zealand) Fellowships programme:

- Department of Building and Housing
- Department of Corrections
- Department of Internal Affairs
- Department of Labour
- Department of Prime Minister and Cabinet
- ERMA New Zealand
- Mighty River Power
- Ministry for Culture & Heritage
- Ministry for the Environment
- Ministry of Agriculture and Forestry
- Ministry of Economic Development
- Ministry of Education
- Ministry of Fisheries
- Ministry of Foreign Affairs and Trade
- Ministry of Health
- Ministry of Justice
- Ministry of Social Development
- New Zealand Customs
- State Services Commission
- Te Puni Kōkiri, Ministry of Māori Development
- The Treasury

ACKNOWLEDGEMENTS

I am deeply grateful and indebted to the many people who helped to make my experience as an Ian Axford (New Zealand) Fellow in Public Policy so rewarding and valuable.

First, I would like to thank the sponsoring government ministries and organizations for their support of the programme. I am particularly grateful to the Ian Axford Board and selection committee, Fulbright New Zealand and the Commonwealth Fund.

I want to especially thank Lauren Perry, my mentor at the Ministry of Justice and my academic mentor, Katrine Evans with the Privacy Commissioner's Office. Lauren welcomed me into the Public Law Group and consistently checked in with me to see how I was doing. She was a fantastic intellectual sounding board and provided the structure for the analytical framework of this report. I deeply appreciate her generosity and willingness to serve as my mentor. Katrine provided invaluable assistance, and her suggestions always improved my research and report. I am especially grateful to her for welcoming me into the office and always finding the time to share her knowledge with me. She also connected me to valuable professional contacts and invited me to attend relevant court hearings. Both Lauren and Katrine were unwavering in their encouragement and support and for that I am most grateful.

I want to also thank the members of the Public Law Group's Privacy team at the Ministry of Justice: Charlotte Connell, Sarah Kerkin, Kristina Temel and Michael Petherick. Each of them went out of their way to include me in policy discussions, respond to my questions and point me in the right direction. Special thanks go to the Public Law Group Managers and Public Law for hosting me and providing a wonderful working environment. I was very fortunate to be welcomed there by colleagues who were intelligent, extraordinarily friendly, kind and helpful.

Thanks to Marie Shroff, Privacy Commissioner, and all of the wonderful staff members in her office for hosting me and making me feel welcome. They deserve recognition for their generosity and kindness. Special thanks to Blair Stewart, Lindy Siegert, Jim Whitman and Wayne Wilson who greatly enriched my knowledge and thinking on the relevant privacy issues. Thanks also to the members of the investigations team, who were so willing to answer my questions and include me in discussions, and to the support staff for their helpful assistance.

Professor Paul Roth at the University of Otago helpfully provided comments and feedback on my many questions, and his *Privacy Law and Practice* was a wealth of information. Thank you to John Edwards and Tim McBride for sharing their time and knowledge with me, and also to Professor Graham Greenleaf at the University of New South Wales, Gary Hartley, Manager for Strategic Initiatives with GS1 New Zealand and David Russell, Chief Executive of the Consumers' Institute. Each helped me to develop my thinking on privacy issues, New Zealand's Privacy Act and radio frequency identification (RFID). Thanks also to Nicole Moreham, Faculty of Law at Victoria University of Wellington, for kindly and quickly answering my last minute questions. I am grateful to Bob Stephens at Victoria University of Wellington, School of Government for organizing seminars that allowed me to present my work. This proved enormously helpful to the development of this report.

Thanks to Judith Forman, Guy Stapleton and the rest of the staff at the Ministry of Justice's Knowledge and Information Services Centre. They provided invaluable help in locating research materials and other resources. Phillip Toye and Anne Yau with the Ministry of Economic Development were generous with their time in helping me understand New Zealand's proposed approach to the problem of spam.

I especially appreciate all of the support from Mele Wendt, Executive Director of Fulbright New Zealand, and Peggy Tramposch, Programme and Advising Team Leader. Both provided valuable assistance and were great resources. Thanks also to all the Fulbright New Zealand staff who helped to make our stay here so enjoyable.

I am also grateful to 2003 Ian Axford Fellow Daniel Pollak who first told me about the fellowship and helped in the development of my project. Dan was an important resource and sounding board, and I much appreciate his help.

I especially want to thank the California State Senate and Don Moulds, Director of the Senate Office of Research for his support and encouragement. I greatly appreciate Don's willingness to allow me to pursue this fantastic opportunity. Thanks also to Donna Hershkowitz who not only supported my decision to apply for the fellowship, but also made sure to send me regular updates from California on related privacy issues. I would also like to thank my colleagues at the Senate Office of Research for their support of this opportunity and for covering for me in my absence.

A special thanks to my fellow Ian Axford Fellows, Linda Blumberg and Susan Coppedge. I truly enjoyed getting to know both of them and their families. Both Linda and Susan provided much-appreciated friendship and laughter, especially over a good bowl of kumara chips.

I would also like to thank the people of New Zealand and the many new friends and neighbours we have gotten to know here. Thanks also to my parents who traveled to the far side of the world to share my New Zealand adventure.

I owe a very special thank you to my husband Hudson Sangree who never wavers in his support, encouragement and friendship. Hudson made professional sacrifices so that we could spend six months in New Zealand and for that I am extremely grateful. I especially appreciated his company and warm meals during long hours of report-writing.

Saskia Kim
Wellington, July 2006

EXECUTIVE SUMMARY

Introduction and Background

New Zealand's Privacy Act 1993 has been called the most comprehensive national privacy law outside of Europe. The heart of the Act is contained in twelve information privacy principles that relate to the collection, use and disclosure of personal information by both public and private-sector entities. New Zealand's comprehensive approach is not the only model for privacy protection, however. Sectoral legislation and self-regulation, both relied upon by the United States and in turn California, are two other significant approaches. Under a sectoral approach legislation is enacted to deal with a specific problem (unwanted telemarketing sales calls, for example) or sector (the banking industry or health care providers). Self-regulatory schemes, on the other hand, avoid legislation and instead afford industry groups the opportunity to establish best-practice guidelines and self-police compliance.

These three approaches to privacy protection are not necessarily exclusive of each other. In fact many countries, including New Zealand and the United States, employ more than one approach. New Zealand uses all three approaches, while California relies on sectoral legislation and self-regulation. Some believe that the countries that most effectively protect privacy utilise all three approaches together.

Each approach by itself has its strengths and weaknesses. Comprehensive privacy protection regimes provide a baseline level of protection because they are broad-based. Critics of the model argue that it has the potential to lead to overly-bureaucratic systems and out-of-control compliance costs. They worry that comprehensive principle-based approaches, like New Zealand's Privacy Act, are vague and do not provide certainty.

Proponents of the sectoral approach argue that it avoids overly-burdensome regulation and can narrowly target a specific problem. Critics, on the other hand, argue that the approach's lack of a single oversight agency is problematic, and enforcement can be lax. Others raise concerns that sectoral legislation is not flexible enough to deal with the latest developments and additional legislation must be introduced to address each new problem as it arises.

Self-regulation, on the other hand, would appear to be more flexible as businesses can tailor guidelines to their business practices. Criticism of the approach focuses on the argument that industry standards are often insufficient to protect privacy, and the regime lacks an assertive enforcement scheme.

Challenges of Technology

New uses of technologies enable the collection, aggregation and disclosure of significant amounts of personal information and can challenge all three approaches to privacy protection. For example, do new technological applications come within the scope of a comprehensive law, which by its nature is general, broad and potentially vague? Is sectoral legislation the best approach because it can specifically target the unscrupulous practice? What if the practice changes and no longer fits within the scope of the specific law? Are sectoral laws immediately obsolete? Is self-regulation a

better approach when dealing with new and evolving technologies that are dynamic in nature?

Key Criteria and a Case Study

This report seeks to apply an objective framework to the debate. It does this by applying seven key criteria to each approach to privacy protection and evaluating the strengths and weaknesses of each regime using radio frequency identification (RFID) technology as a case study. The report uses the following criteria as guiding principles because they are critical to any privacy protection regime: trust, openness, choice, control, balance, flexibility and certainty.

Although the report lists trust as a criterion it is arguably more a measure of the success of a privacy protection regime, and each of the other criteria – while important in their own right – underpins it. When individuals have *trust* and confidence in a system they are more likely to feel comfortable providing their personal information to take advantage of a service or purchase a product. An entity that collects personal information from an individual should be *open* about the collection thus implicating important issues of transparency such as the fact that personal information is being collected and the purpose of the collection. Ideally individuals will have a *choice* as to whether to disclose their personal information, although choice is necessarily fragile, and individuals may often find themselves in a coerced environment. People should have *control* over what happens to their personal information and who is able to access it. The privacy protection regime should strike the appropriate *balance* between an individual's right to privacy and other competing interests. The regime should be *flexible* enough to deal with new developments and provide *certainty* for participants so that they know how to behave.

RFID technology provides an ideal case study to evaluate how each approach measures up to the seven criteria. RFID identification systems automatically and uniquely identify people or objects using radio waves that are transmitted between a microchip and antenna (often called a "tag") and a reader. The tag and reader do not have to be touching in order to communicate, and the distance between them can vary depending on various factors. The ability to communicate without contact raises potential privacy issues for some who worry that information will be covertly collected from a tag. Currently RFID tags are used most often in the supply chain where businesses use the technology to track goods by tagging pallets and cartons which are then scanned to confirm a shipment's arrival. Plans are underway to use RFID to uniquely identify consumer goods and link information about an item such as the date and place of manufacture to a computer database. Privacy advocates raise concerns that the ubiquitous placement of tags in everyday products could potentially lead to tracking, profiling and the aggregation of massive amounts of personal information in computer databases. Industry experts, on the other hand, argue that many of the privacy issues have been overstated, and technologies like RFID can actually enhance security.

RFID technology is already used in many consumer products. In the United States, Chase Bank's RFID-enabled "Blink" card permits consumers to pay for goods by simply waving their card near a reader. The ExxonMobil Speedpass card similarly uses RFID to allow consumers to pay for gas without swiping a card or using a PIN.

Many motorists use RFID-enabled passes to electronically charge their accounts when traveling on toll roads or over bridges or through tunnels. Amusement parks have also begun offering RFID-tagged wristbands so that parents can keep track of where their children are in the park. RFID has even been implanted in humans. In the medical context some patients have had a chip implanted in their arm in order to permit a physician to easily access their medical record if they are unconscious. Others have been more enterprising; bar patrons in Spain have had a chip implanted in order to gain access to VIP areas and run electronic bar tabs. In at least one case an employer has used RFID implantations to restrict employee access to secure facilities.

All of these different applications of the technology have the potential to raise issues under the criteria. For example, openness is particularly important in the case of RFID because of the possibility of covert collection, and, even if an individual knows that her tag is being scanned by a reader, she does not necessarily know what information is actually being conveyed. If a consumer's personal information is collected from an RFID tag and stored in a database, having control over what happens to that information and who gets to see it is critical. This report evaluates how each approach to privacy protection addresses the privacy issues raised by RFID technology and how they each might further the goals of trust, openness, choice, control, balance, flexibility and certainty.

Findings and Recommendations

The findings in this report have implications for both New Zealand and California. Among the findings specific to each privacy protection approach are the following:

- A comprehensive approach, such as New Zealand's Privacy Act 1993, most effectively promotes the goals of openness, control and flexibility thus building consumer trust. The Act does not promote the goal of choice in the way that some sectoral legislation attempts to do. Instead, it recognises that choice is necessarily limited and provides individuals with openness, transparency and control.

- After addressing a threshold definitional issue that has been raised concerning New Zealand's Privacy Act, radio frequency identification technology falls within the scope of the Privacy Act.

- Sectoral legislation can best achieve choice. It can be drafted, for example, to require that individuals be given the choice to decide whether or not to purchase a product with an RFID tag. Sectoral legislation can also be written to most robustly further the goals of openness, control, balance and certainty thus helping to foster trust and confidence. In most cases with respect to RFID, however, legislation attempting to achieve these goals has not yet been enacted in the United States and California. Because no baseline protection exists there is a gap in practice and little to protect people in the meantime.

- In analysing self-regulation, it is important to place the approach in a larger framework. In New Zealand this means considering the Privacy Act 1993 which provides a floor of privacy protections. Self-regulatory proposals in this context are another layer of protection rather than the only layer as in the United States.

Yet there is nothing to stop self-regulation efforts from providing more protections than those provided under the Privacy Act.

Among the key lessons for both New Zealand and California are the following:

- A comprehensive approach to privacy, such as New Zealand's Privacy Act 1993, can provide a baseline floor of protection with sectoral legislation (in particular codes of practice) and self-regulation helping to fill in the details.

- Trust is a measure of the success of a privacy protection regime and is critically important to the uptake of new technologies like RFID. While important in their own right, the other criteria – openness, choice, control, balance, flexibility and certainty – all underpin trust. Each of the criteria can thus be used as a tool to evaluate whether the privacy regime has achieved trust and consumer confidence in the system.

- The analytical framework provided in this report is a model for future analyses of other technologies, such as biometrics, global positioning systems (GPS) and electronic databases. At its most basic level the analysis asks fundamental questions which can be asked of any technology:

    - Why is the criterion particularly important in the context of this technology?
    - What are the privacy issues raised by this technology with respect to the criterion?
    - How does the policy addressing these privacy issues further the goals of the criterion?
    - If the policy is violated, how is the criterion undermined?

Structure of Report

Chapter One of this report briefly introduces the three major approaches to privacy protection, the challenges posed by new technologies, and the objectives and scope of the report. The chapter also describes in more detail the objective criteria used to evaluate the strengths and weaknesses of each approach. Chapter Two provides a brief overview of issues relating to privacy law, and Chapter Three details the three major approaches to privacy protection, providing examples of each.

Chapter Four introduces radio frequency identification and provides examples of current and future applications of the technology. The chapter also contains discussion of the privacy issues surrounding the technology, efforts undertaken in New Zealand and California to regulate it and several threshold definitional issues concerning RFID and New Zealand's Privacy Act 1993. The heart of Chapter Four, and the report, is an evaluation of the strengths and weaknesses of each approach applying the objective criteria and using RFID technology as a case study. Chapter Five draws conclusions and offers policy recommendations and suggestions.

TABLE OF CONTENTS

1 INTRODUCTION

Varying Approaches to Protection of Personal Information

Different countries have taken different approaches to privacy protection. The three major approaches are often referred to as comprehensive, sectoral and self-regulation. Comprehensive regulatory schemes, like New Zealand's Privacy Act, are made up of a general law concerning the collection, use and disclosure of personal information by both the public and private sectors. Sectoral regulation includes specific regulation dealing with a particular problem or sector, and self-regulation is generally when industry groups establish best practice guidelines and self-police compliance. The three approaches are not necessarily exclusive of each other. In fact many countries, including both New Zealand and the United States, employ more than one approach. It has been said that the countries that protect privacy most effectively utilise all the approaches together.[1]

New Zealand's fundamental privacy protection scheme is the Privacy Act 1993 which applies to both the public and the private sectors. The Act lays out twelve information privacy principles concerning the collection, use, retention and disclosure of personal information. Oversight is maintained in the Office of the Privacy Commissioner and individuals may make complaints to that office. New Zealand also uses the sectoral approach to privacy protection, proposing bills on spam and intimate covert filming, and the self-regulation approach, including GS1 New Zealand's "EPC/RFID Consumer Protection Code of Practice."

In contrast to New Zealand, the United States (and California in turn) has predominantly relied on sectoral and self-regulation.[2] In California the state constitution provides its residents with an inalienable right to pursue and obtain privacy, allowing the state to enact measures to protect that right. Even so, such proposals have been sectoral, or piecemeal. For example, California enacted an anti-spam law in 2003, and there have been legislative efforts to increase e-mail privacy and regulate radio frequency identification (RFID) and the use of global positioning systems (GPS) to track individuals. Unlike the Privacy Act in New Zealand, California's Information Practices Act, which regulates the collection, maintenance and disclosure of personal information, applies only to state entities and not to private entities.

Challenges of Technology

We live in a technological world, and many believe our privacy rights become more threatened as new technologies emerge, bringing with them the capacity for collecting, aggregating and disclosing substantial amounts of personally identifiable data, sometimes without the knowledge of the individual to whom the information pertains. Protection of personal information has come to take on new meanings in

[1] Electronic Privacy Information Center (2001), p.3

[2] It is important to mention here the role of the courts and litigation in the United States in remedying harm. The U.S. Supreme Court, however, has yet to hold that the federal Constitution protects a right to privacy of personal information. Gindin (1997).

such a world. Although the technologies at issue are themselves neutral, it is their application which many believe has the most potential to threaten privacy rights. Proponents of technological advances highlight the efficiencies and security that technologies, such as RFID and biometrics, can provide. They also note that consumers often benefit from these advances, particularly with respect to services and conveniences. Privacy advocates, on the other hand, raise concerns about who might have access to the often-sensitive personal information collected by the technology as well as the purposes for which the information might be used.

Many individuals both in the United States and New Zealand worry that their personal privacy is threatened by new technologies. According to a poll by Roy Morgan International released in May 2006, 70 percent of Americans and 57 percent of New Zealanders are worried about "the invasion of privacy through new technology."[3]

As new technologies become more widely used the varying approaches to privacy protection have the potential to become more challenged. Comprehensive laws are by their nature general and broad in order to encompass a variety of circumstances and practices. That breadth however, has the potential to result in vagueness, and as a result the question becomes whether new technological applications will come within the scope of the law. Sectoral laws, on the other hand, can narrowly target the technology and the offending practice, but they raise the potential for immediate obsolescence as technology changes and no longer fits within the scope of the specific law. To the extent self-regulatory efforts target a particular technology they may also raise similar issues. Furthermore, some technologies may simply be too broad for just one sectoral law. RFID technology has many different applications which raise different potential privacy issues. Must there then be a different sectoral law for each different application? For example, should there be a sectoral law dealing with human implantation of RFID and another law for the use of RFID in the retail context. Or can one sectoral law cover different applications? Which approach can best meet all of these challenges? The answers have important policy implications for both New Zealand and California.

Objectives of this Report

My research compared the differing approaches to privacy protection using RFID as a case study. The objectives were as follows:

- ✓ Compare the varying approaches to privacy protection applying objective criteria and using RFID as a case study to evaluate the strengths and weaknesses of each regime
- ✓ Evaluate whether existing statutory schemes are sufficient to protect privacy
- ✓ Learn how New Zealand is handling the privacy implications of emerging technologies
- ✓ Identify lessons to take back to California

[3] 'Five countries review privacy, technology', 17 May 2006

This report provides an introduction to the policy issues surrounding privacy and new technologies and details the existing legal and statutory framework. The report then evaluates the strengths and weaknesses of the three major approaches to privacy protection using seven objective criteria and RFID as a case study. These criteria, which are discussed in more detail just below, are: trust, openness, choice, control, balance, flexibility and certainty. This analysis provides a framework for analysing other technologies as well. The report then concludes with key findings related to each approach and makes several recommendations.

Scope of this Report

One of the things I have learned over the years working on privacy issues and have had confirmed for me in New Zealand is that privacy is complex and requires an understanding of competing societal demands. Privacy also encompasses many different issues. For example, during my short time in New Zealand privacy often claimed headlines in the newspaper such as when the first known incident of skimming hit New Zealand ATMs. In other news reports, a judge ruled that a convicted paedophile's privacy had been breached when the police distributed a flyer containing his photograph, criminal history and the street he lived in, and the Law Commission released a draft report on access to court records. While all of these issues interest me I have had to restrain myself and limit the scope of the research and this report. For example, it is generally thought that there are several aspects, or categories, of privacy: physical (bodily) privacy, territorial privacy, privacy of personal behaviour, privacy of communications and information privacy (these are described in more detail in the "Background on Privacy" section of this report). Although the others are all important and vital, this report largely concerns only the last aspect of privacy, information privacy.[4] Furthermore, the report is limited by focusing on only one type of technology, RFID, as a means to provide a case study for evaluation of the different approaches to privacy protection.

Finally, although the use of emerging technologies by law enforcement officials has potentially profound implications for privacy rights, the research did not focus on this particular application. Instead the report looks at the technologies' impacts on consumers from a data protection perspective.

Criteria Used to Assess Each Privacy Protection Regime

In a comparative study it is helpful to measure the subjects of the study against objective criteria so that the strengths and weaknesses of each become apparent. In my evaluations of the different approaches to privacy protection I used the following criteria as guiding principles because they are critical to any privacy protection regime: trust, openness, choice, control, balance, flexibility and certainty.

In a world in which privacy is respected:

- Individuals will have *trust* in the system of data collection and this trust will not be misplaced.

[4] As noted later in this report, however, the categories overlap and as a result some of the discussion will necessarily implicate other aspects as well.

Although trust is listed as one of the criteria it is more accurately a measure of the success of a privacy protection regime. The other criteria are all important in their own right but they also all underpin trust. They are subsets of creating trust, or consumer confidence. For example, people are more likely to trust an agency that has been open and transparent about its data collection efforts. Similarly, if individuals have control over their information once it has been collected, they are more likely to trust those who hold it. Each of the criteria can thus be used as a tool to evaluate whether the privacy regime has achieved trust and confidence in the system.

Trust is also critically important to the uptake of new technologies like RFID; a lack of trust could hinder its development and consumer acceptance. RFID technology has the potential to trigger many trust issues because of the prospect of covert collection and use of databases to store possibly vast amounts of personal information. Trust is important both in terms of the technology itself as well as trust in the system that oversees its use. In the United States several legislative efforts restricting the use of RFID have stalled in part because of interest group pressures. Arguably, however, industry groups need trust to operate and develop RFID technologies and privacy advocates need to trust that a regime will confidently safeguard privacy. Trust is an underlying interest of both groups.

Consumer confidence in businesses' ability to safeguard personal information has declined over the past few years, particularly in the United States, as a result of, among other things, security breaches, identity theft and credit card fraud.[5] According to the Privacy Rights Clearinghouse, "over 88 million data records of U.S. residents have been exposed due to security breaches since February 2005."[6] In New Zealand a study on trust and information privacy found that privacy breaches appear to have an adverse effect on individuals' trust in the organization.[7] Unfortunately New Zealanders have now also become victims of skimming[8] and phishing.[9]

At the same time that consumer confidence is declining many people place increased importance on the ability of businesses to maintain the security of their personal information. In New Zealand for example, a recent public opinion survey conducted for the Privacy Commissioner revealed that 93 percent of those polled considered "respect for, and protection of, their personal information" to be important when dealing with a business; this figure included 74 percent who said it was "very important" to them.[10] The highest levels of concern regarding privacy issues related to the security of personal information on the Internet: 84 percent of those polled were concerned about this issue, including 63 percent who were "very concerned."[11]

---

[5] Significant security breaches over the years include the disclosure of the personal information of 163,000 consumers by U.S. data broker ChoicePoint which resulted in at least 800 cases of identity theft (U.S. Federal Trade Commission, 26 January 2006) and, more recently, the breach of the personal information of 28.6 million U.S. veterans. (Privacy Rights Clearinghouse, n.d.). For a listing of data breaches see 'A chronology of data breaches reported since the ChoicePoint incident' at http://www.privacyrights.org/ar/ChronDataBreaches.htm

[6] Privacy Rights Clearinghouse (n.d.)

[7] Reilly (January 2006), p.56

[8] Mulrooney, Paul, *The Dominion Post*, 30 March 2006

[9] Binning, Elizabeth, *The New Zealand Herald*, 12 June 2006

[10] Privacy Commissioner (February 2006), UMR Research Limited

[11] Id.

Demonstrating a lack of trust and confidence with respect to online privacy, in October 2005 a Consumer Reports WebWatch research report indicated that nearly nine out of ten Internet users (86 percent) have "made at least one change in their behaviour because of fears of identity theft" and 53 percent of Internet users "say they have stopped giving out personal information on the Internet."[12] Furthermore, 88 percent of those surveyed said that "keeping personal information safe and secure is very important for a Web site they visit."[13]

Consumers have also shown that they are willing to take their business elsewhere when they feel that a company has failed to adequately protect their personal information. Karen Curtis, Federal Privacy Commissioner of Australia, recently made this point in her keynote address to the 2006 Privacy Issues Forum entitled "Good Privacy is Good Business."[14] She noted a recent *Register* article which reported that "[o]ne in five US consumers quizzed by Ponemon Institute said they immediately terminated their accounts with vendors that lost their information. An additional 40 per cent polled by the organisation's *National Survey on Data Security Breach Notification* considered taking their business elsewhere after receiving notifications of information mishandling."[15]

- An entity that collects personal information from an individual will be *open* about the collection.

Openness underpins trust and promotes privacy; the more open an entity has been about data collection, the more likely individuals will trust it. The converse is also true; the less open an entity has been with an individual, the less likely the individual will trust it.

Openness includes important issues of transparency such as: the fact that personal information is being collected, what information is being collected, the purpose of the collection, and who is able to see the information and what will eventually happen to it. These details are important to help consumers make choices about their personal information, including whether and to whom to disclose. Openness also relates to issues of access; a system is more open and transparent when individuals can see what information it has about them.

In the case of RFID specifically, recent workshops held by the European Commission to seek public input on an RFID policy indicate that consumers demand the right to know how the technology is being used and whether RFID tags will still be readable after a consumer purchases an item and leaves the store.[16] Participants also encouraged transparency by recommending that the technology should be explained and made understandable to consumers.[17]

- Individuals will have a *choice* as to whether to disclose their personal information.

[12] Consumer Reports WebWatch (26 October 2005)
[13] Id.
[14] Curtis, Karen (30 March 2006)
[15] Leyden, John *The Register*, (15 November 2005)
[16] European Commission (n.d.), pp.9-10
[17] Id. at 10

Choice is the ability to decide whether or not to disclose personal information at the time of collection. This is distinguished from "control" which, for purposes of this report, means having power over personal information once it has been collected. Choice also furthers privacy and underpins trust; if we have a choice as to whether to disclose personal information, we are arguably more likely to trust those who gave us the choice.

The European Commission's current public workshops on RFID indicate that consumers want the right to have choices regarding the technology.[18] Participants indicated that solutions should be developed to give consumers control over whether or not to disclose their information and suggested examples such as deactivating tags, breaking the antenna to reduce the read range or allowing the consumer to switch off the RFID functions.[19]

While providing choice is an ideal and therefore included as one of the criteria, it is fragile because the reality of many situations is that individuals find themselves without choice or without a real choice. Employment situations are one such example. Choice in this setting is likely to be limited as many people simply need to work to earn a living. In other cases we have to give up personal information in order to obtain a product or service; we do not have a choice. Some regimes, such as New Zealand's Privacy Act, recognise the limitations of choice and provide individuals with other rights instead such as notice that personal information is being collected and control over the information.

The concepts of authorisation and consent may come up with respect to choice. Consent is not as strong as authorisation which "more clearly denotes a positive and conscious act by the individual."[20] Consent on the other hand, can be implied.[21] The Privacy Commissioner considered the issue in a case in which a couple complained that their bank had conducted an unauthorised credit check, writing "I did not consider that a failure to object amounted to an authorisation. I consider that authorisation requires a positive act."[22]

- Individuals will have *control* over what happens to their personal information and who is able to access it.

Giving people control over their personal information is more likely to lead to trust in the privacy protection regime. If individuals have control over their information once it has been collected, they are more likely to trust those who hold it.

Control is also a critical issue with respect to information privacy. It has been said that people have a right to "exercise some control over the circulation of information relating to them. The underlying assumption appears to be that such information is fundamentally the property of the individual to whom it relates."[23] Control

[18] European Commission (n.d.), pp.9-10
[19] Id. at 10
[20] Roth, *Privacy Law and Practice*, para 1006.11A
[21] Id.
[22] Case Note 2976 [1996] NZPrivCmr 1 (1 November 1996)
[23] Longworth (1994), p.3

encompasses not just control over what happens to personal information and who gets to see it, but also how long it is retained and whether it is ultimately destroyed.

People increasingly feel that they have little control over their personal information. A 1999 survey of consumer attitudes toward privacy conducted by Louis Harris & Associates found that a "majority of British consumers (68%) agree strongly or somewhat with the statement that 'consumers have lost all control over how personal information is collected and used by companies'."[24] In New Zealand a survey performed for the Office of the Privacy Commissioner by UMR Research in February 2006 found that 89 percent of those polled were concerned (including 75 percent who were very concerned) if a business they don't know gets hold of their personal information, indicating a loss of control.[25]

- The privacy protection regime will strike the appropriate *balance* between an individual's right to privacy and other competing interests.

The right to privacy is not absolute; it must be balanced against other, often competing, interests.[26] Sometimes privacy competes with another interest important to the individual such as quick access to credit.[27] At other times it competes with an interest important to society, such as protection of the public against security threats or encouraging the free flow of information. Privacy protection is about appropriately balancing these interests.[28] People are more likely to trust a privacy regime that is balanced and does not favor one side too much over the other.

- The regime will be *flexible* enough to deal with new developments.

Flexibility is a particularly important criterion, especially with respect to technology. It often seems that new applications of a technology are introduced on an almost daily basis. What once seemed impossible or unheard of is now attainable and, as time goes by, affordable and more accessible. Examples include cameras in cell phones, biometric security systems that identify people by body odour and RFID-tagged bracelets that keep track of children at amusement parks and patients in hospital.

While many can agree that there are advantages to these particular advances, in other instances new technologies are more destructive and even devious. Examples include: spamming, phishing, skimming, spyware, malware and keystroke logging. All of these technologies have become a part of our vocabulary and, unfortunately, in many cases have wreaked havoc with our identities, computers and bank accounts.

The need for the law to keep pace with technological developments is an important requirement for any privacy protection scheme and is important for trust. Flexibility in the law can be challenging; a statute prohibiting a particular practice or restricting a particular technology can become obsolete if the defined practice or technology changes and no longer fits within the scope of the law. On this point Blair Stewart, Assistant Privacy Commissioner has noted, "[t]he elastic character of privacy,

[24] IBM Multi-National Consumer Privacy Survey (October 1999), p.164
[25] Privacy Commissioner (February 2006), UMR Research Limited
[26] See, e.g., Longworth (1994), p.4 and Clarke (2005)
[27] Clarke (2005)
[28] Id.

dynamic nature of technology and globalisation of information handling, make rigid and prescriptive solutions very difficult (and usually undesirable)."[29] Yet a privacy protection regime that is flexible and can meet different needs and apply to different uses is more trustworthy because we know that it will not quickly become obsolete.

- The regime will provide *certainty* for participants.

Certainty is important to many people who want to know how to comply. They wish for clear, unambiguous rules to tell them how to behave and what is expected of them. For the purposes of this report, certainty asks whether a privacy protection scheme tells those subject to it what to do and how to act. Certainty is important in the case of evolving technologies. As new applications are introduced the people using them need to know whether the rules apply to them and, if so, what they require of them. Certainty is also important to evaluating whether a privacy regime has achieved trust. If the regime provides certainty, the people using it can trust it because they know what to do and how to act within its structure.

[29] Stewart, Blair (24 November 2005)

2 BACKGROUND ON PRIVACY[30]

What is Privacy?

Privacy is a fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.[31]

The right to privacy has been recognised in the Universal Declaration of Human Rights 1948 which provides "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[32] Article 17 of the International Covenant on Civil and Political Rights 1966 also recognises the right to privacy and contains substantially similar language.[33]

The United States Supreme Court has recognised an individual's right to privacy implicit in the Constitution with respect to certain rights, including among others, the safeguards for freedom of expression and association under the First Amendment, the protections against unreasonable search and seizure consistent with the Fourth Amendment and the freedom from self-incrimination under the Fifth Amendment.[34] Individuals are protected in this regard against intrusive governmental activities.

The California Constitution expressly states that all people have an inalienable right to pursue and obtain privacy,[35] giving Californians greater privacy protections than those recognised by the U.S. Constitution. For example, whereas federal protections apply only to government action, California's right to privacy protects individuals from actions by both the government and private actors.[36] The California Supreme Court has held that the California Constitution in and of itself "creates a legal and enforceable right of privacy for every Californian."[37]

In the United States Dean William Prosser argued that common law privacy doctrine had evolved to provide for four distinct invasion of privacy torts.[38] These invasions, which were incorporated into the Second Restatement of Torts, include: unreasonable intrusion upon the seclusion of another, appropriation of another's name or likeness, public disclosure of private facts and publicity that unreasonably places another in a false light in the public eye.[39] In New Zealand a common law remedy in tort for

[30] The following background is an overview of issues relating to privacy law; it is not intended to be exhaustive.
[31] Electronic Privacy Information Center (2001), p.1
[32] Universal Declaration of Human Rights (1948), Art.12
[33] International Covenant on Civil and Political Rights (1966), Art.17
[34] Koppe (2002), p.25
[35] California Constitution, Art.1, Section 1
[36] See, e.g., *American Academy of Pediatrics v. Lungren*, 16 Cal. 4th 307, 326, citing *Skinner v Railway Labor Executives' Assn.* (1989) 489 U.S. 602; *Hill v National Collegiate Athletic Association* (1994) 7 Cal. 4th 1, 15-20
[37] *White v Davis* (1975) 13 Cal. 3d 757, 775
[38] Gindin (1997), citing William L. Prosser, *Privacy*, 48 Cal. L. Rev 383, 389 (1960)
[39] Restatement (Second) of Torts, §§ 652A – 652E

interference with privacy is in the early stages of development.[40] In March 2004 the Court of Appeal held in *Hosking v Runting* that in order to bring a successful claim for breach of privacy the following two requirements must be met: "(1) the existence of facts in respect of which there is a reasonable expectation of privacy; and (2) publicity given to those private facts that would be considered highly offensive to an objective reasonable person."[41]

Privacy advocates generally speak of the right to privacy as having several aspects or categories: physical privacy, territorial privacy, privacy of personal behaviour, privacy of communications and information privacy.[42]

- *Physical privacy*, also called "privacy of the person"[43] or "bodily privacy,"[44] concerns the "protection of people's physical selves against invasive procedures."[45] The concept includes concerns surrounding issues such as compulsory drug or DNA testing and cavity searches.

- *Territorial privacy* refers to the "setting of limits on intrusion into the domestic and other environments such as the workplace or public space."[46] The right is considered a critical privacy principle, giving people "the right to private space in which to conduct their personal affairs."[47]

- *Privacy of personal behaviour* relates "to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices."[48]

- *Privacy of communications* involves the ability to communicate securely and privately.[49] This category covers communications by mail, telephone, e-mail and other forms of communication.[50]

- *Information privacy* comprises the "establishment of rules governing the collection and handling of personal data"[51] and "the notion that individuals are entitled to exercise some control over the circulation of information relating to them."[52] The concept embraces the idea that personal information "should not be automatically available" to others and, when another party holds it, the individual to whom the information pertains should be able to "exercise a substantial degree of control over that data and its use."[53]

---

[40] Law Commission (June 2004)
[41] Id. See, also Hosking v Runting (2005) 1 NZLR 1 (CA)
[42] Longworth (1994), p.3. See, also Electronic Privacy Information Center (2001), p.3 and Clarke (2005)
[43] Clarke (2005)
[44] Electronic Privacy Information Center (2001), p.3
[45] Id.
[46] Id.
[47] Longworth (1994), p.3
[48] Clarke (2005)
[49] Electronic Privacy Information Center (2001), p.3
[50] Id.
[51] Id.
[52] Longworth (1994), p.3
[53] Clarke (2005)

While this report largely concerns only the last aspect of privacy, information privacy, some of the discussion contained here will also have implications for other aspects; there is overlap among the categories. For example, if an RFID-enabled identification badge is used by an employee to access a restricted area, a record is created of that use including the time, date and location of the access. This information arguably relates to "information privacy" because it is information about the person, but it would also seem to implicate "privacy of personal behaviour" since it relates to the individual's activities and whereabouts. Perhaps it may also raise issues under "territorial privacy" to the extent that it deals with limits on intrusion into the workplace.

Why is Privacy Important?

In 1890 Samuel Warren and Louis Brandeis famously spoke of privacy as the "right to be let alone" in a seminal law review article on the subject.[54] Since that time there has been much discourse on the need for privacy and its functions in a modern democratic state. Alan Westin has written of four functions of privacy: personal autonomy, emotional release, self-evaluation and limited and protected communication.[55] They allow individuals to "choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others."[56] Roger Clarke has also provided a brief overview of the reasons why privacy is important:

- Privacy is *psychologically* important: "People need private space. . . . We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing."[57]

- Privacy is *sociologically* important: "People need to be free to behave and to associate with others, subject to broad social mores, but without the continual threat of being observed."[58]

- Privacy is *economically* important: "People need to be free to innovate. International competition is fierce, so countries with high labour-costs need to be clever if they want to sustain their standard-of-living. And cleverness has to be continually reinvented."[59]

- Privacy is *politically* important: "People need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy."[60]

Likewise, in a 2004 speech Privacy Commissioner Marie Shroff noted that "Each of us as an individual needs to freely form, develop and maintain our identity and sense of self; we need a personal safety zone, in order to provide that freedom."[61]

---

[54] Warren (1890), citing Thomas C. Cooley (1888) *Law of Torts*, 2d ed.
[55] Westin (1967), p.32
[56] Electronic Privacy Information Center (2001), p.2
[57] Clarke (2005)
[58] Id.
[59] Id.
[60] Id.
[61] Shroff (2004)

3 LEGAL AND STATUTORY FRAMEWORK

This chapter describes three major approaches to privacy protection – comprehensive, sectoral and self-regulation – and provides examples of each. More detailed discussion of each approach, including their benefits and limitations, can be found later in this report.

Comprehensive Approach

Description of Comprehensive Approach

Comprehensive privacy protection regimes are general laws that govern the collection, use, retention and disclosure of personal information by the private and public sector.[62] Compliance is then ensured by an oversight body.[63] Comprehensive regimes are said to provide a baseline level of privacy protection[64] and promote transparency. Comprehensive schemes can be more rule-based and prescriptive, like the European Union's Data Protection Directives, or principle-based, like New Zealand's Privacy Act 1993. In a speech at the IIR Minimising Risks and Costs of Privacy Requirements Conference in Melbourne, New Zealand Assistant Privacy Commissioner Blair Stewart noted that some critics of comprehensive regimes have argued that such legislation could lead to an "overly-bureaucratic system or spiraling compliance costs."[65] They also argue that comprehensive, principle-based approaches like the Privacy Act are vague and do not provide certainty.[66]

Examples of Comprehensive Approach

New Zealand: The Privacy Act 1993

In 1993 New Zealand adopted a comprehensive approach to privacy protection, enacting the Privacy Act 1993.[67] The long title of the Act provides that it is an act "to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."[68] The Act contains provisions establishing how both public and private sector agencies may collect, store, use, retain and disclose personal information[69] and provides for a Privacy Commissioner whose legislated functions include the investigation of complaints, education and a monitoring role.[70] The Act also requires each agency to have a privacy officer who is responsible for

---

[62] Electronic Privacy Information Center (2001), p.3
[63] Id.
[64] Id. at 10
[65] Stewart, Blair (31 May 1999). For more on compliance costs under the Privacy Act 1993, see Harding, Emma 'Compliance Costs and the Privacy Act 1993: Perception or Reality for Organisations in New Zealand?' (2005) 36 *Victoria University of Wellington Law Review* 529
[66] See, for example Palmer, Sir Geoffrey (1997), p.235
[67] For complete text of the Privacy Act 1993 see: http://www.legislation.govt.nz. See Appendix for Part 2 (information privacy principles) of the Act.
[68] Privacy Act 1993
[69] Id.
[70] Privacy Act 1993, s 13 and s 69

encouraging agency compliance with the Act, dealing with Privacy Act requests and working with the Privacy Commissioner on investigations related to the agency.[71]

The Privacy Act requires the Privacy Commissioner to periodically review the operation of the Act, consider whether any amendments are necessary or desirable and report to the Minister of Justice with any recommendations.[72] In 1998 the previous Privacy Commissioner Bruce Slane submitted his report entitled "Necessary and Desirable: Privacy Act 1993 Review".[73] Three supplementary reports have been issued in April 2000, January 2003 and December 2003 which contain further amendment suggestions and updates on earlier recommendations. At the opening of Parliament the Government indicated that reform of the Privacy Act was one of its legislative and policy priorities for the coming parliamentary session as mentioned in the Governor-General's address.[74]

Scope of Act

The Privacy Act defines "agency" to mean any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector.[75] The Act specifically excludes certain entities, including among others the Sovereign, the Governor-General or the Administrator of the Government, the House of Representatives, a member of Parliament in his or her official capacity, a court or tribunal in relation to its judicial functions or any news medium in relation to its news activities.[76] Furthermore, although an individual may be considered to be an agency under the Act, Section 56 exempts the collection or holding of personal information by an individual where the personal information is collected or held by the individual "solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs."[77]

"Personal information" is defined to mean information about an identifiable individual,[78] and "individual" means a natural person but does not include a deceased natural person.[79] The Act specifies that "collect" does "not include the receipt of unsolicited information."[80]

Information Privacy Principles

The Privacy Act contains twelve information privacy principles which form the heart of the Act and establish guidelines concerning how agencies may collect, store, use, retain and disclose personal information.[81] The principles also deal with access to, and correction of, personal information and the assignment of unique identifiers by

[71] Privacy Act 1993, s 23
[72] Privacy Act 1993, s 26
[73] Privacy Commissioner (November 1998)
[74] (8 November 2005) 628 New Zealand Parliamentary Debates 14
[75] Privacy Act 1993, s 2(1)
[76] Id.
[77] Privacy Act 1993, s 56
[78] Privacy Act 1993, s 2(1)
[79] Id.
[80] Id.
[81] Privacy Act 1993, s 6

agencies.[82]

Principle 1: Purpose of collection of personal information

Principle 1 provides that agencies may not collect personal information unless the information is collected for a lawful purpose connected with a function or activity of the agency and the collection of the information is necessary for that purpose.[83]

Principle 2: Source of personal information

Under this principle when an agency collects personal information it must collect the information directly from the individual concerned.[84] There are several exceptions to this principle including when the agency believes on reasonable grounds that: (1) the information is publicly available, (2) the individual concerned has authorised the collection of information from someone else, or (3) non-compliance would not prejudice the interests of the individual.[85] Other exceptions to the principle include when the agency believes on reasonable grounds that:

- Non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention or investigation of offences, for the enforcement of a law imposing a pecuniary penalty, for the protection of the public revenue, or for the conduct of court or tribunal proceedings;

- Compliance would prejudice the purposes of the collection or compliance is not reasonably practicable in the circumstances of the particular case;

- The information will not be used in a form that identifies the individual or will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual; or

- The Privacy Commissioner has authorised the collection under Section 54 of the Act.

Principle 3: Collection of information from subject

Principle 3 provides that when an agency collects personal information directly from an individual the agency must take reasonable steps to ensure that the individual is aware of the following:

- The fact that information is being collected, the purpose for which the information is being collected and the intended recipients of the information;

- The name and address of the agency that is collecting the information and the agency that is holding the information;

[82] Id.
[83] Id.
[84] Id.
[85] Id.

- If the collection of the information is authorised or required by law, the particular law which requires or authorises the collection and whether or not the supply of the information is voluntary or mandatory;

- The consequences, if any, for the individual if all or any part of the information requested is not provided; and

- The individual's right to access and correct his or her personal information.[86]

Principle 3 requires that these steps must be taken before the information is collected, or, if this is not practicable, as soon as practicable after the information is collected.[87] However, an agency is not required to take these steps if the agency has already informed the individual in relation to the same information, or information of the same kind, on a recent previous occasion.[88] The principle contains exceptions to its requirements which are largely the same as those provided under Principle 2, described above.[89]

Principle 4: Manner of collection of personal information

Principle 4 regulates the manner of collection by prohibiting the collection of personal information by unlawful means or means that, in the circumstances of the case, are unfair or intrude to an unreasonable extent on the personal affairs of the individual concerned.[90]

Principle 5: Storage and security of personal information

Under Principle 5 agencies holding personal information must meet certain storage and security requirements. The agency must ensure that reasonable security safeguards are in place to protect the information from loss, misuse and unauthorised access, use, modification or disclosure.[91] Agencies must also ensure that if it is necessary to give the information to another person in connection with the provision of a service to the agency, everything reasonable is done to prevent unauthorised use or disclosure of the information.[92]

Principle 6: Access to personal information

Principle 6 provides individuals with a right of access to their personal information held by agencies when the information is "readily retrievable".[93] In such a case, an individual is entitled to obtain confirmation of whether or not the agency holds his or her personal information and to have access to that information.[94] The agency must also advise the individual that he or she may request correction of the information

[86] Id.
[87] Id.
[88] Id.
[89] Id.
[90] Id.
[91] Id.
[92] Id.
[93] Id.
[94] Id.

pursuant to Principle 7.[95]

The Privacy Act provides that agencies may refuse to disclose personal information in certain circumstances, including when disclosure would be likely to prejudice the security or defence of New Zealand, prejudice the investigation of criminal offences or endanger the safety of an individual.[96] Other permissible reasons for a refusal to disclose personal information include among others, if: (1) disclosure would involve the unwarranted disclosure of another's affairs; (2) disclosure would be contrary to the interests of an individual under the age of 16 or would breach legal professional privilege; or (3) the request is frivolous or vexatious.[97] Agencies may also refuse an access request if the information requested does not exist or cannot be found.[98] The Act also contains procedural provisions concerning access and correction of personal information,[99] including specified timeframes within which an agency must respond to a request[100] and a requirement that the reason for refusal of an access or correction request be provided to the individual.[101]

Principle 7: Correction of personal information

This principle requires that when an agency holds personal information the individual concerned is entitled to request correction of the information and request that, if it is not corrected, a statement be attached to the information explaining the correction that was sought but not made.[102] An agency must also take reasonable steps to correct the information to ensure that the information is accurate, up to date, complete and not misleading and, if the agency determines that correction is not appropriate, it must attach the individual's statement concerning the requested correction to his or her personal information.[103] When an agency corrects information or attaches an individual's statement concerning a correction sought but not made, the agency must if reasonably practicable, inform each person or agency who has received the information of these actions.[104]

Principle 8: Accuracy, etc, of personal information to be checked before use

Principle 8 requires agencies that hold personal information to take reasonable steps before using the information to ensure that the information is accurate, up to date, complete, relevant and not misleading.[105]

Principle 9: Agency not to keep personal information for longer than necessary

Principle 9 provides that an agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may

[95] Id.
[96] Privacy Act 1993, s 27
[97] Privacy Act 1993, s 29(1)
[98] Privacy Act 1993, s 29(2)
[99] Privacy Act 1993, Part 5
[100] Privacy Act 1993, s 40
[101] Privacy Act 1993, s 44
[102] Privacy Act 1993, s 6
[103] Id.
[104] Id.
[105] Id.

lawfully be used.[106]

Principle 10: Limits on use of personal information

Under Principle 10 an agency that holds personal information obtained in connection with one purpose may not use the information for any other purpose.[107] The principle contains exceptions to its requirements which are substantially similar to those provided under Principle 2, described above.[108] Additional exceptions permit the agency to use personal information for another purpose if: (1) the use of that information for the other purpose is necessary to prevent or lessen a serious and imminent threat to public health or safety or the life or health of the individual concerned or another individual; or (2) the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained.[109]

Principle 11: Limits on disclosure of personal information

Principle 11 provides that an agency that holds personal information may not disclose the information to another person or body or agency unless the agency reasonably believes that: (1) disclosure is either one of the purposes in connection with which the information was obtained or is directly related to those purposes or the source of the information is a publicly available publication; (2) the disclosure is to the individual concerned or authorised by the individual or is necessary to prevent or lessen a serious and imminent threat to public health or safety or the life or health of the individual concerned or another individual; or (3) disclosure is necessary to facilitate the sale of a business as a going concern.[110] Disclosure is also permitted for several of the same reasons permitted under Principle 2, described above.

Principle 12: Unique identifiers

Principle 12 provides that an agency shall not assign a unique identifier to an individual unless the assignment of the identifier is necessary to enable the agency to carry out one or more of its functions efficiently.[111] The principle also prohibits an agency from assigning a unique identifier to an individual that, to the agency's knowledge, has already been assigned to the individual by another agency.[112] Agencies that assign unique identifiers to individuals must take all reasonable steps to ensure that they are assigned only to individuals whose identity is clearly established.[113] Agencies may not require individuals to disclose their unique identifiers unless the disclosure is for one of the purposes, or directly related to one of the purposes, for which the identifier was assigned.[114]

---

[106] Id.
[107] Id.
[108] Id.
[109] Id.
[110] Id.
[111] Id.
[112] Id.
[113] Id.
[114] Id.

Privacy Commissioner

The Privacy Act establishes the Privacy Commissioner, an independent Crown entity.[115] The Act contains various enumerated functions of the Commissioner which include among others:

- Promotion of an understanding of the information privacy principles by education and publicity;

- Monitoring the use of unique identifiers and developments in data processing and computer technology to ensure that any adverse privacy effects of such developments are minimised; and

- Examining proposals for information-matching legislation or any other proposed legislation that the Commissioner considers may affect the privacy of individuals, and making inquiries into any matter, including any enactment, law or practice, if it appears that the privacy of individuals is being infringed.[116]

The Privacy Act permits any person to make a complaint to the Privacy Commissioner alleging that an action is an interference with his or her privacy.[117] The Act gives the Commissioner the ability to investigate any action that is or appears to be an interference with the privacy of an individual, upon a complaint or on her own initiative, and to act as conciliator in such actions.[118] The Act also gives the Commissioner the power to decide to take no action on a complaint for specified reasons[119] and contains more detailed provisions concerning complaints procedures.[120]

The Commissioner may issue codes of practice which can modify the application of the information privacy principles by prescribing standards that are more or less stringent than the standards in the principles or exempting any action from a principle.[121] Codes of practice may apply to specified information, agencies, activities or industries, but they may not limit an individual's right to access or correct his or her personal information held by a public sector agency.[122] The Act outlines the procedure to be followed for the issuance of a code of practice[123] including a requirement that public notice be given.[124] Failure to comply with a code is considered a breach of an information privacy principle.[125]

Enforcement Provisions[126]

The information privacy principles do not confer on any person any legal right that is

[115] Privacy Act 1993, s 12
[116] Privacy Act 1993, s 13
[117] Privacy Act 1993, s 67
[118] Privacy Act 1993, s 69
[119] Privacy Act 1993, s 71
[120] Privacy Act 1993, Part 8
[121] Privacy Act 1993, s 46(2)
[122] Privacy Act 1993, s 46(3) and s 46(5)
[123] Privacy Act 1993, Part 6
[124] Privacy Act 1993, s 48(1)
[125] Privacy Act 1993, s 53
[126] For a more detailed discussion of remedies available under the Privacy Act, see Evans (2005)

enforceable in a court of law except for the right to access personal information held by a public sector agency.[127] The Act defines an "interference with privacy" as an action that breaches an information privacy principle or code of practice *and*, in the opinion of the Privacy Commissioner or the Tribunal the action has: (1) caused, or may cause, loss, detriment, damage or injury to the individual; (2) adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or (3) resulted in, or may result in, significant humiliation, significant loss of dignity or significant injury to the individual's feelings.[128]

These requirements do not have to be met for violations of Principles 6 or 7.[129] Instead the Act provides that an action is an interference with an individual's privacy if the agency refuses to make information available in response to an access request or refuses to correct personal information *and* the Privacy Commissioner or the Human Rights Review Tribunal finds that there was no proper basis for that decision.[130]

California: The Information Practices Act of 1977

California has adopted a more limited "comprehensive" approach in the Information Practices Act which places restrictions on the collection, maintenance and disclosure of personal information held by state agencies.[131] The Act applies only to state agencies and provides some limited notification requirements as well as access and correction rights. The Act also does not establish an oversight officer similar to the Privacy Act's Privacy Commissioner.

Scope of Act

Unlike New Zealand's Privacy Act 1993, California's Information Practices Act applies only to state agencies.[132] The term "agency" is defined to mean every state office, officer, department, division, bureau, board, commission or other state agency, but does not include the California Legislature, courts established under Article VI of the California Constitution, the State Compensation Insurance Fund, except with respect to employment records, or local agencies, as specified.[133]

The Act defines "personal information" as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.[134] Personal information includes statements made by, or attributed to, the individual.[135] "Maintain" is defined to include maintain, acquire, use or disclose,[136] and "individual" means a natural person which, unlike the Privacy Act 1993, includes a corporation,

---

[127] Privacy Act 1993, s 11
[128] Privacy Act 1993, s 66(1)(b)
[129] *Winter v Jans* (6 April 2004) HC HAM CIV-2003-419-854
[130] Privacy Act 1993, s 66(2)(a) and (b)
[131] California Civil Code Section 1798 et seq. All California statutory and constitutional provisions may be obtained from www.leginfo.ca.gov
[132] California Civil Code Section 1798.3(b)
[133] Id.
[134] California Civil Code Section 1798.3(a)
[135] Id.
[136] California Civil Code Section 1798.3(e)

partnership, limited liability company, firm or association.[137]

Collection and Notice Requirements

The Information Practices Act also requires state agencies to collect personal information to the greatest extent practicable directly from the individual concerned rather than from another source.[138] Under the Act state agencies must provide notice concerning the purpose of the collection, the name of the agency requesting the information, the statutory, regulatory or executive authority which authorises the collection, whether submission is mandatory or voluntary and the consequences of not providing the requested information.[139] The notice must also include the title, business address and telephone number of the person responsible for the agency's system of records, any known or foreseeable disclosures of the information and the individual's right of access to his or her records maintained by the agency.[140] This notice must be provided "on or with any form used to collect personal information from individuals,"[141] a much narrower requirement than Principle 3 of New Zealand's Privacy Act which requires the notice in all instances in which the agency collects personal information directly from the individual.

Agency's Records

The Information Practices Act provides that state agencies shall maintain in their records only personal information that is relevant and necessary to accomplish an authorised purpose.[142] Each agency must maintain all records to the maximum extent possible, with accuracy, relevance, timeliness and completeness, although this standard needs only to be met when the records are used to make a determination about the individual.[143] If the agency transfers a record outside of state government it must correct, update, withhold or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely.[144] This requirement does not appear to apply when the information is transferred from one state agency to another state agency. Agencies must establish appropriate and reasonable administrative, technical and physical safeguards to ensure compliance with the Act, and to ensure the security and confidentiality of the records and protect against "anticipated threats or hazards to their security or integrity which could result in any injury."[145]

Disclosure Limitations

Under the Information Practices Act, state agencies are prohibited from disclosing any personal information in a manner that would link the information to the individual concerned, unless the disclosure is among other things, with the consent of the individual, pursuant to the Public Records Act or a search warrant, or to a

[137] California Civil Code Sections 1798.3(d) and (f)
[138] California Civil Code Section 1798.15
[139] California Civil Code Section 1798.17
[140] Id.
[141] Id.
[142] California Civil Code Section 1798.14
[143] California Civil Code Section 1798.18
[144] Id.
[145] California Civil Code Section 1798.21

governmental agency when required by state or federal law.[146] Agencies are required to keep accurate accountings of the date, nature and purpose of each disclosure of a record and the name, title and business address of the person or agency to whom the disclosure was made.[147] Additionally, if a record containing personal information is corrected or a dispute is noted, an agency must notify any person or agency to whom the record was disclosed during the preceding three years of the correction or notation of dispute.[148] This requirement applies only if an accounting was required, the information contains the name of the person or agency to whom the disclosure was made or the individual concerned provides the name of the person or state agency who received the information.[149] The Act specifically provides that an agency may not distribute individuals' names and addresses for commercial purposes or sell or rent names and addresses unless such action is specifically authorised by law.[150] Nothing in the Act prohibits the release of the names and addresses of individuals possessing licenses to engage in a professional occupation.[151]

Access and Correction Rights

The Information Practices Act provides individuals with the right to inquire and be notified as to whether an agency maintains a record about him or her.[152] An agency may charge a fee for the copying of the record which may not exceed ten cents ($0.10) per page, unless another statute establishes the agency fee for copying.[153] Agencies must respond to an individual's request for inspection within a specified timeframe.[154] The Act provides that an agency may refuse to disclose personal information to an individual for specified reasons including among others, if the information is compiled for the purposes of a criminal investigation of suspected criminal activities or is maintained for the purposes of an investigation of the individual's fitness for licensure or public employment or a grievance or complaint.[155]

State agencies must allow individuals to request that their record be amended and, within 30 days of the receipt of such a request, must either make the requested correction or inform the individual of the agency's refusal to amend the record, the reason for the refusal and the agency's procedures to request review of the decision.[156] If the record is not amended, an individual may file a statement explaining the reasons he or she believes the record should be amended.[157] This statement shall be included in disclosures of the record.[158]

[146] California Civil Code Section 1798.24
[147] California Civil Code Section 1798.25
[148] California Civil Code Section 1798.28
[149] Id.
[150] California Civil Code Section 1798.60
[151] California Civil Code Section 1798.61
[152] California Civil Code Section 1798.32
[153] California Civil Code Section 1798.33
[154] California Civil Code Section 1798.34
[155] California Civil Code Section 1798.40
[156] California Civil Code Section 1798.35
[157] California Civil Code Section 1798.36
[158] California Civil Code Section 1798.37

Enforcement Provisions

Although the Information Practices Act does not establish an oversight officer similar to the New Zealand Privacy Act's Privacy Commissioner, it does contain other provisions for remedying violations of its requirements. For example, the Act specifically provides that an individual may bring a civil action against a state agency if the agency does any of the following:

1) Refuses to comply with an individual's lawful request to access his or her information.

2) Fails to maintain an individual's record with such accuracy, relevancy, timeliness and completeness as is necessary to assure fairness in a determination relating to the qualifications, character, rights, opportunities of or benefits to the individual that is made on the basis of the record and, as a proximate result of the failure, a determination is made which is adverse to the individual.

3) Fails to comply with any provision of the Act and that non-compliance has an adverse effect on the individual.[159]

In any suit brought pursuant to 2) and 3) above, an agency is liable to the individual in an amount equal to the sum of actual damages sustained by the individual, including damages for mental suffering and the costs of the action and reasonable attorney's fees as determined by the court.[160] A failure to comply with any provision of the Act may be enjoined by a court .[161]

Privacy Act of 1974

In 1974 the U.S. Congress enacted the Privacy Act which regulates the collection, maintenance, use and disclosure of personal information by federal executive branch agencies.[162] The Act grants individuals some access and correction rights and restricts disclosure of personal information.[163] The Act is of limited utility however, with even the federal Office of Management and Budget noting that, "the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored."[164]

Sectoral Approach

Description of Sectoral Approach

Some countries, most prominently the United States, have avoided enacting an overall comprehensive privacy regime and instead enact specific regulation to deal with a

[159] California Civil Code Section 1798.45
[160] California Civil Code Section 1798.48
[161] California Civil Code Section 1798.47
[162] Privacy Act, 5 U.S.C. 552a
[163] Id.
[164] U.S. Office of Management and Budget (May 2004)

particular problem or sector.[165] As described in more detail below, in California sectoral examples include restrictions on rental car companies' use of technology to track renters, or regulation of financial privacy. At the federal level, sectoral legislation regulates the collection of information by consumer credit reporting agencies[166] and restricts unwanted telemarketing sales calls through the national "Do Not Call" Registry.[167] Sectoral privacy legislation uses various mechanisms for oversight and enforcement including federal agencies such as the Federal Trade Commission, state attorneys general or other public prosecutors such as district attorneys or individual citizens through a private right of action. Critics argue that the approach's lack of a single oversight agency is problematic[168] and enforcement can be lax.[169]

Other criticisms include the concern that the approach is not flexible enough to deal with developments, particularly technological developments, and so additional legislation must be introduced to address new problems.[170] This problem is arguably compounded in California where high-tech industry lobbyists have often successfully argued that legislative solutions should not ban technology, but instead should ban bad behaviour,[171] resulting in statutes that specifically define a prohibited practice. If the practice changes however, the statute may no longer apply and protections necessarily lag behind.

Examples of Sectoral Approach

New Zealand

Unsolicited Electronic Messages Bill

In May 2004 the government issued a discussion paper entitled "Legislating Against Spam'.[172] Forty-three submissions were received in response to the paper,[173] and on 28 July 2005 Information Technology Minister David Cunliffe introduced the Unsolicited Electronic Messages Bill.[174] At the time of this writing, the bill is being considered by the Commerce Select Committee which heard submissions on 4 May 2006 and 11 May 2006 and also considered the bill on 29 June 2006. The Select Committee's report on the bill originally due 13 June 2006, is now due 31 August 2006.[175] The following description of the bill reflects its provisions as introduced.

The proposed bill applies to spam that is originated in New Zealand or where the computer used to access the message is located in New Zealand. The bill includes

[165] Electronic Privacy Information Center (2001), p.4
[166] Fair Credit Reporting Act, Section 601, 15 U.S.C. 1681 et seq.
[167] Telemarketing Sales Rule, 16 C.F.R. Part 310
[168] Electronic Privacy Information Center (2001), p.4
[169] Gellman, Robert (2000), p.74
[170] Electronic Privacy Information Center (2001), p.4
[171] AeA (20 May 2006)
[172] Cunliffe, Hon David (1 May 2004)
[173] Ministry of Economic Development (August 2004)
[174] Cunliffe, Hon David (28 July 2005)
[175] See, http://publications.clerk.parliament.govt.nz.clients.intergen.net.nz/BillsBeforeSelect Committees.aspx. Unfortunately the Select Committee's report comes due after the deadline for this report.

both an opt-in and opt-out approach, depending on the type of message that is sent. For example, the bill prohibits commercial e-mail messages from being sent to people who have not given their prior consent to receiving the messages (opt-in).[176] The bill also prohibits the sending of promotional e-mail messages to a person who has withdrawn consent to receiving those messages (opt-out).[177] The bill contains related definitions of commercial and promotional e-mail messages.[178]

Under the proposed bill all commercial and promotional e-mail messages must include accurate information about the person who authorised the sending of the e-mail and must also include a functional unsubscribe option.[179] The bill also prohibits address-harvesting software and the use of any electronic address list produced by that software.[180] Complaints for violation may be made to the relevant internet service provider or the High Court which is empowered to issue an injunction.[181] If an individual suffers loss or damage as a result of the violation, he or she may seek an injunction from the High Court, make an application to the High Court for compensation or damages or apply to join any Court action initiative by the enforcement department.[182]

Crimes (Intimate Covert Filming) Amendment Bill

In 2003 the New Zealand Government asked the Law Commission to review the issues relating to covert filming and make legislative recommendations.[183] As part of its review the Law Commission considered whether existing laws might already address the issue which had taken on new importance with the advent of miniature cameras and mobile phone cameras. In its review of the Privacy Act with respect to this matter, the Law Commission wrote "the Privacy Act 1993 can provide an avenue to address some instances of intimate covert filming and distribution," but also noted that the Act did not fully deal with the matter for two reasons.[184] First, while Principle 3 requires an agency to inform an individual of the fact of collection, its purpose and who will receive the collected information, the principle contains an exception if the information will not be used in a form in which the individual is identified.[185] The Law Commission explained that this exception was problematic in the case of intimate covert filming because "such filming often focuses on body parts and may not result in images of an 'identifiable' person."[186]

Furthermore, the Law Commission found the Privacy Act insufficient to fully address intimate covert filming because of the Act's exception for personal information relating to domestic affairs.[187] That exception provides that nothing in the information

[176] Unsolicited Electronic Messages Act 2005, available from http://www.knowledge-basket.co.nz/gpprint/docs/bills/20052811.txt
[177] Id.
[178] Id.
[179] Id.
[180] Id.
[181] Id.
[182] Id.
[183] Hon Phil Goff, Minister of Justice (5 May 2005), 625 New Zealand Parliamentary Debates 20322
[184] Law Commission (June 2004), para 3.48
[185] Privacy Act 1993, s 6
[186] Law Commission (June 2004), para 3.24
[187] Id. at para 3.30

privacy principles applies to an individual's collection or holding of personal information where "that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs."[188] With respect to this exception the Law Commission remarked that the provisions appear to provide exemptions for "an individual who covertly films another for his or her own gratification" and "an individual if retaining covertly filmed images for his or her own use."[189]

As a result of the Law Commission's findings, the government introduced the Crimes (Intimate Covert Filming) Amendment Bill which proposed amendments to the Crimes Act "to create new offences in line with the Law Commission's recommendations."[190] As reported from the Government Administration Committee, the proposed bill deals with the making of surreptitious visual records of another person without that person's knowledge or consent and in circumstances that the person would reasonably expect to be private.[191] The bill prohibits the intentional or reckless making of an intimate visual recording as well as the possession and publication of such a recording.[192] The bill has had its second reading and is currently before Parliament.

Credit Reporting Privacy Code 2004

Prior to implementation of the Credit Reporting Privacy Code 2004 the New Zealand Privacy Act's information privacy principles controlled the handling of credit information by credit reporting agencies. Although these provisions provided people with key protections, "difficulties were encountered"[193] and "the previous Privacy Commissioner concluded that there would be merit in a code of practice. The current Commissioner, having studied the matter and the submissions on the code, agrees and believes that the code she has now issued will bring benefits to individuals and business alike."[194]

Fully implemented on 1 April 2006, the Credit Reporting Privacy Code 2004 takes the place of the information privacy principles with respect to credit reporting agencies.[195] The code requires credit reporters to provide individuals, upon request, with free copies of their credit information held by the credit reporter.[196] Under the code credit reporting agencies must ensure that the information they hold is regularly updated and linked to the correct individual.[197]

If a debt is disputed by an individual the code requires credit reporting agencies to either suppress the disputed information or clearly identify the information as disputed while it is being checked for accuracy.[198] The code also limits the amount of time that

[188] Privacy Act 1993, s 56
[189] Law Commission (June 2004), para 3.31
[190] Hon Phil Goff, Minister of Justice (5 May 2005), 625 New Zealand Parliamentary Debates 20322
[191] Government Administration Committee (1 August 2005)
[192] Id.
[193] Privacy Commissioner (n.d.)
[194] Id.
[195] Privacy Commissioner (6 December 2004)
[196] Id.
[197] Id.
[198] Id.

information may be held, as specified, and places restrictions on the agencies to which information may be disclosed.[199] The code requires credit reporting agencies to maintain an access log in order to safeguard credit information against unauthorised access or misuse.[200]

Health Information Privacy Code 1994

The Health Information Privacy Code 1994 was issued by the Privacy Commissioner only one month after the Privacy Act 1993 came into effect.[201] The code, which applies to agencies in the health sector, concerns the collection, use, holding and disclosure of health information about identifiable individuals.[202] The code substitutes for the information privacy principles for health sector agencies,[203] and it requires that such agencies inform individuals of the fact that their health information is being collected, the purpose of the collection and the intended recipients of the information.[204] Under the code health agencies may retain health information if it is necessary or desirable to do so for the purposes of providing health or disability services to the individual.[205]

California

Electronic Surveillance Technology: Rental Cars

In response to reports that rental car companies were using global positioning systems (GPS) to monitor the routes and driving habits of their customers, California law prohibits rental car companies from using any information relating to a renter's use of the rental vehicle that was obtained using electronic surveillance technology, such as GPS, wireless technology or location-based technology.[206] The law provides for certain exceptions including if the rental car is stolen, law enforcement requests the information pursuant to a subpoena or search warrant, or the renter requests that the vehicle be remotely locked or unlocked.[207]

Direct Marketing: Disclosure of Personal Information

California law requires a business that discloses personal information for marketing purposes to either: (1) disclose to customers, upon request, a list of the categories of personal information (for example, name, address, telephone number, social security number, e-mail address, or occupation) the business has disclosed to third parties for marketing purposes and the names and addresses of those third parties; or (2) provide customers with the opportunity to prevent information sharing for marketing purposes through either an opt-in or opt-out approach.[208]

---

[199] Id.
[200] Id.
[201] Longworth (1994), p.165
[202] Privacy Commissioner (28 June 1994)
[203] Id.
[204] Id.
[205] Id.
[206] California Civil Code Sections 1936(o) and (p)
[207] Id.
[208] California Civil Code Section 1798.83

Financial Privacy

The California Financial Information Privacy Act places restrictions on the sharing of consumers' nonpublic personal information by financial institutions.[209] A financial institution must first obtain the consent of a consumer before it may disclose or share the consumer's nonpublic personal information with any nonaffiliated third party (known as an "opt-in").[210] And before disclosing nonpublic personal information to an affiliate, a financial institution must give a consumer an opportunity to direct that his or her information not be disclosed (known as an "opt-out").[211]

Unless a consumer has opted out, a financial institution may share the consumer's personal information with another financial institution when they enter into a joint marketing agreement to offer a financial product or service that meets specified requirements.[212] The unrestricted sharing of nonpublic personal information between a financial institution and its wholly owned financial-institution subsidiaries in the same line of business is also permitted, irrespective of any consumer choice, provided that specified requirements are met.[213]

Confidentiality of Medical Information Act

California's Confidentiality of Medical Information Act (CMIA) prohibits a health-care provider, health-care service plan, or contractor from disclosing medical information regarding a patient, enrollee, or subscriber of a health-care service plan without first obtaining authorization, except as specified.[214] Notwithstanding this prohibition medical information must be disclosed if required by a court order or search warrant, among other things.[215] In other specified circumstances disclosure is discretionary.[216] Violations of CMIA are enforceable by administrative fines or civil penalties, misdemeanor criminal penalties and a private right of action for compensatory and punitive damages.[217]

Self-Regulation

Description of Self-Regulation

Under a self-regulatory scheme industry groups establish best practice guidelines and self-police compliance.[218] The United States is the most obvious adherent of this approach with respect to privacy protection. Proponents of self-regulation argue that it allows business experts to tailor guidelines to their business practices, keeps costs down and is "unhindered by bureaucratic legal procedures."[219] Some say another

[209] California Financial Code Section 4053
[210] Id.
[211] Id. This provision was successfully challenged by representatives of the banking industry on the basis that it was pre-empted by the federal Fair Credit Reporting Act (FCRA). An appeal is pending.
[212] Id.
[213] Id.
[214] California Civil Code Section 56.10(a)
[215] California Civil Code Section 56.10(b)
[216] California Civil Code Section 56.10(c)
[217] California Civil Code Sections 56.35 and 56.36
[218] Electronic Privacy Information Center (2001), p.4
[219] Clarke, Steve (August 2001)

advantage of self-regulation is its flexibility, "each organization can be left to comply in the most beneficial way."[220] With respect to RFID specifically, some participants in recent workshops held by the European Commission to seek public input on an RFID policy argued that many technologies, like RFID, are in the early stages of deployment and regulators should therefore take a hands-off, "regulatory-light" approach.[221]

Criticism of self-regulation has focused on whether or not the industry standards are sufficient to protect privacy (critics insist they are not) and the lack of an assertive enforcement scheme.[222] Others have also argued that "the private sector lacks the experience, the motivation and the public trust to regulate itself."[223] In New Zealand David Russell, Chief Executive of the Consumers' Institute, has argued that industry-led regulation can only be successful if there is an underpinning of government regulation.[224] Mr Russell supports a two-part system of self-regulation in which: (1) an industry group demonstrates that it can exercise control over its members and develops guidelines to which they adhere, and (2) a legislative backstop, such as the Privacy Act 1993, underlies the industry-led regulation.[225]

Examples of Self-Regulation

GS1 New Zealand "EPC/RFID Consumer Protection Code of Practice"

In March 2005 GS1 New Zealand (also called "GS1 NZ") issued the "EPC/RFID Consumer Protection Code of Practice".[226] The code, described in greater detail later in this report, "is administered by GS1 NZ, supported by the retail sector, and provides the mechanism for the industry to self-regulate in the context of general legislation."[227] The code is intended to be used by retailers who stock products containing RFID tags; it does not cover use in the supply chain.[228] The code is voluntary and administered by the "Code of Practice development committee" which must meet at least annually to make recommendations to the Board of GS1 New Zealand regarding any changes to the code or the issuing of guidelines.[229] The code, which provides for some notice requirements, provides for a complaints resolution process should a dispute arise.[230]

Code of Practice for Direct Marketing in New Zealand

The New Zealand Marketing Association is a strong proponent of self-regulation, and one of its principal objectives is the promotion of "a self-regulatory environment with government, legislators and other stakeholders."[231] The Marketing Association has

[220] Bennett, Colin (1992), p.155
[221] European Commission (n.d.), p.11
[222] Electronic Privacy Information Center (2001), p.4
[223] Papakonstantinou, Vagelis (2002), p.152
[224] Interview with David Russell, Chief Executive, Consumers' Institute (Wellington, 26 April 2006)
[225] Id.
[226] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[227] Id.
[228] Id.
[229] Id.
[230] Id.
[231] Marketing Association of New Zealand (n.d.), Codes of Practice

adopted a "Code of Practice for Direct Marketing in New Zealand" which, among other things, requires marketers who are members of the Association to check its "Name Removal Register" which contains the contact details of individuals who do not wish to receive unsolicited mail, telephone calls or facsimiles before sending any unsolicited mailing campaigns.[232]

The code also requires marketers to have a system in place allowing people the ability to opt-out of receiving unsolicited marketing information and requires that the marketer protect personal and payment information using sound security systems.[233] The code requires marketers to have fair and effective procedures in place to handle complaints within a reasonable time and requires that they tell people how to contact the Marketing Association and the Electronic Marketing Standards Authority.[234] Again, these requirements apply only to Marketing Association members who, according to the Association, account for "90% plus of all outbound mailing."[235]

The Marketing Association has also issued best practice guidelines in a number of areas, including e-mail marketing, direct marketing data, search engine marketing and fax marketing. While members of the Association are required to adhere to its codes of practice, the best practice guidelines are "recommended methodology".[236]

[232] E-mail correspondence from Keith Norris, Chief Executive, Marketing Association of New Zealand (27 June 2006)
[233] Marketing Association of New Zealand (n.d.), Codes of Practice
[234] Id.
[235] E-mail correspondence from Keith Norris, Chief Executive, Marketing Association of New Zealand (27 June 2006)
[236] Id.

4 RADIO FREQUENCY IDENTIFICATION (RFID): A CASE STUDY

Explanation of RFID Technology

Radio frequency identification systems automatically and uniquely identify people or objects using radio waves.[237] The systems are made up of a microchip which contains information about the person or object to which it is attached and an antenna which relays that information, using radio waves of varying frequencies, to a reader.[238] The microchip and antenna together are often referred to as an RFID "transponder" or "tag"[239] and can be as small as half a grain of sand.[240] The reader communicates with the tag and conveys the information to a database which stores the information.[241]

Tags and readers do not have to be touching in order to communicate; their communication is "contact-less". Tags and readers also do not have to be within each other's line of sight in order to communicate with each other.[242] These features are often cited as some of the significant improvements of RFID tags over the universal product code (UPC) or bar code which requires that a scanner "see" the bar code in order to read it.[243] In addition, unlike bar code scanners RFID readers can read more than one item at a time again resulting in beneficial efficiencies over bar codes.[244]

RFID tags can be either "passive" or "active". Passive tags are simpler and do not have their own power source, receiving their power from the reader.[245] They "do not initiate communication"[246] but instead draw their power from a reader or, more precisely, "the electromagnetic waves emitted by readers that induce a current in the tags."[247] Once "awakened" the tag then transmits the information stored on it to the reader which is then able to identify the person or item to which the tag is attached.[248] Because they do not contain their own power supply passive tags have a longer life and are smaller and cheaper than active tags, but their read ranges (the maximum distance a tag can interact with a reader) are not as great.[249] Active tags, on the other hand, contain their own power supply, typically a battery which can shorten their life.[250] Active tags "either broadcast their information without being interrogated by the reader, or stay quiet until triggered by a reader."[251] Their read ranges are

[237] *RFID Journal* (n.d.)
[238] U.S. Federal Trade Commission (March 2005), pp.3-4
[239] Id.at 4
[240] Brown, Russell, *Listener*, 8 February 2003, p.39
[241] U.S. Federal Trade Commission (March 2005), p.4
[242] Id.
[243] *RFID Journal* (n.d.)
[244] *RFID Gazette* (28 June 2004)
[245] *RFID Journal* (n.d.)
[246] U.S. Federal Trade Commission (March 2005), p.6
[247] Center for Democracy and Technology (1 May 2006)
[248] Id.
[249] Roberts (2006), p.19. Generally, passive tags can be read from a range of about 10 to 20 feet, depending on the size of the antenna, radio frequency used, power of the reader and physical conditions. U.S. Government Accountability Office (May 2005), p.6
[250] Although the battery contained in an active tag can shorten its life, current battery technology can still mean that a tag is active for as much as 10 years. Roberts (2006), p.19
[251] Article 29 Data Protection Working Party (19 January 2005), p.3

substantially greater; 100 feet or more, compared with less than 20 feet for passive tags.[252]

RFID tags can hold more information than bar codes and, depending on the tag, can be re-writeable, allowing the information contained on the tag to be erased or rewritten.[253] The information contained on read-only tags, which have minimal memory capacity, cannot be changed.[254] Read-write tags on the other hand have larger storage capacity and the information contained on these tags can be altered.[255] RFID tags can be deactivated or "killed" when a reader sends a code to the tag turning it off.[256] The EPCglobal standards require that an RFID tag must be able to be killed permanently and may not be reactivated.[257]

The development of RFID faces technical challenges as "conductive material such as metal or fluids reflect electromagnetic energy. This makes tagging metal surfaces such as metallic coffee cans and containers or shampoo bottles challenging and often results in decreased identification rates."[258] Other environmental factors such as wind can also affect read ranges.[259]

Examples of Current and Future Applications of RFID Technology

Technically, RFID technology is not a new "emerging" technology; it has been used since World War II when the allies needed to identify friendly aircraft from a distance.[260] New and novel applications of the technology, however, have thrust it into the limelight in recent years. Many new uses seek to take advantage of the contact-less nature of the technology. While some recent developments are currently in use, others are still only proposed. The following descriptions of RFID use are in no way exhaustive – announcements of new applications of the technology are made on a regular basis. Some applications raise obvious privacy concerns; others may raise few or no privacy concerns.

Use in the Supply Chain

Much RFID use is occurring in the supply chain. In 2003 in order to bring about supply chain efficiencies, U.S. retailer Wal-Mart required its major suppliers to use RFID tags on all pallets and cartons.[261] The technology is used to track goods through the supply chain to help identify deficiencies in the chain and deter theft.[262] Entire pallets and cartons may be scanned at one time to confirm that a shipment has arrived.[263] RFID tags may be combined with sensors to monitor refrigerated goods to

[252] *RFID Journal* (n.d.)
[253] U.S. Department of Commerce (April 2005), p.9
[254] U.S. Federal Trade Commission (March 2005), p.7
[255] U.S. Government Accountability Office (May 2005), p.7
[256] *RFID Journal* (n.d.)
[257] Interview with Gary Hartley, Manager for Strategic Initiatives, GS1 New Zealand (Wellington, 5 May 2006)
[258] U.S. Department of Commerce (April 2005), p.10
[259] U.S. Federal Trade Commission (March 2005), p.6
[260] Roussos (March 2006), p.25
[261] *RFID Gazette* (28 June 2004)
[262] *RFID Journal* (n.d.)
[263] *RFID Gazette* (28 June 2004)

ensure that their temperature is controlled.[264] The efficiency gains for retailers can be significant: Wal-Mart recently announced that the use of RFID technology in its supply chain had resulted in a 62 percent drop in the out-of-stock rate for certain items.[265]

In New Zealand, GS1 New Zealand recently announced a six to 12 month trial using RFID technology to track goods as they moved between manufacturers, transport companies and retailers. According to press reports the trial is expected to involve tagging pallets and cartons rather than individual items. The goal is to create a "mini-supply chain" that will be used to study the interoperability of the systems and benefits to the businesses.[266]

Also in New Zealand, the Warehouse discount chain announced a pilot project in February 2006 to test RFID technology in its stockrooms. The company plans to tag pallets and cartons once they are delivered by suppliers in order to better monitor and manage inventory levels.[267]

Smart Shelves

RFID technology can also be used to help retailers manage their inventory and monitor the level of stock on the shelf. The system alerts a retailer when stock of a particular item is low, helping the business to keep in-demand goods in stock.[268] In 2003 Germany's largest retailer, Metro AG, opened its "Store of the Future" designed to test RFID technology under "real-world" conditions.[269] In addition to RFID "smart shelves" and self-checkout systems, the store's shopping carts are RFID-tagged, allowing readers at the door to alert the store manager if there is an increase in the number of carts that have entered the store so that he or she can open additional checkout aisles.[270]

Item-Level Tagging and "The Internet of Things"

One of the most significant barriers to the widespread tagging of individual items with RFID chips has been the cost of the tag. Some cost estimates suggest that the tags can run between 25 and 30 cents each[271] while others have indicated that tag prices are currently in the five to seven cent range.[272] Within the next five to seven years however, the price of RFID tags is expected to drop to less than a penny each.[273] Some consider that to be the "magic point at which nearly anything we buy is likely to be tagged."[274] Often called the "Internet of Things," the systems will "connect the cyberworld and the physical world."[275] In addition to cost barriers, as noted earlier,

---

[264] Roberts (2006), p.21
[265] Johnson, John, *RFID Watch Weekly*, 17 May 2006
[266] Pullar-Strecker, Tom, *The Dominion Post*, 17 April 2006
[267] Pullar-Strecker, Tom, *The Dominion Post*, 27 February 2006
[268] *RFID Journal* (28 April 2003)
[269] Id.
[270] Id.
[271] Boucher Ferguson, Renee, *eWEEK.com*, 6 March 2006
[272] Bergstein, Brian, *Seattle Post-Intelligencer*, 20 May 2006
[273] *Consumer Reports* (June 2006), p.35
[274] Id.
[275] Id. at 34

technical challenges also exist; conductive material such as metal or fluids or environmental factors such as wind can all make tagging challenging.[276]

The Electronic Product Code (EPC) and the EPCglobal Network have been developed to uniquely identify items using RFID, connecting "everyday objects and devices to large databases and networks [including the Internet]."[277] The initiative is a global one, aimed at increasing the use of the EPC and RFID tagging and thus bringing the tags' cost down. Under the system each item is given a unique EPC number which is contained in an RFID tag attached to the item.[278] The tag communicates the EPC number to readers which are linked with a computer database that stores information about the item including the date and place of manufacture.[279] In this way the system uniquely identifies each individual package of soap, for example.

Despite the ambition of the EPCglobal Network, item-level RFID tagging appears to still be in an early stage. Several trials have been run, testing RFID technology on individual items. Most prominently U.K. retailer Marks & Spencer has since 2004 used RFID-tagged hang tag labels on particular clothing items to monitor inventory levels on the shop floor.[280] The tags, which contain only a number unique to the particular garment, are passive tags which do not emit a signal and instead respond to a reader passed near them during the stock take process.[281] The hang tags are removable and can be thrown away after purchase.[282] The company states that there is no link between the purchased item and the customer's details because the RFID tag is not scanned at the time of purchase.[283]

Recent reports indicate that Levi Strauss & Co. is testing RFID technology in removable hang tags attached to selected men's products.[284] The tags are being tested to help manage inventory in two of the company's franchise stores in Mexico and one U.S. retail store which Levi Strauss declined to identify, citing the store's request that it not be named until it decides to identify itself.[285]

For its newest bookstore in the Netherlands, Boekhandels Groep Nederland is tagging all of its books using a self-adhesive RFID label in order to allow for automated inventory control.[286] Initially the store will use a trolley with a reader mounted on it to take inventory and determine the location of books.[287] Eventually however, Boekhandels indicates that it hopes to use bookshelves enhanced with RFID readers to automate inventory control. RFID readers, which will be placed at the checkout counters, will read a book's tag when it is sold and then "kill" the tag.[288]

---

[276] U.S. Department of Commerce (April 2005), p.10 and U.S. Federal Trade Commission (March 2005), p.6
[277] International Telecommunication Union (November 2005), p.3
[278] EPCglobal (n.d.)
[279] Id.
[280] Marks & Spencer (18 February 2005)
[281] Id.
[282] Id.
[283] Id.
[284] Neff, Jack, *Advertising Age*, 28 April 2006
[285] Id.
[286] Collins, Jonathan, *RFID Journal*, 18 April 2006
[287] Id.
[288] Id.

Consumer Use

RFID technology is already in use in many consumer products. For example, in the United States ExxonMobil Speedpass uses RFID to allow consumers to pay for gas without swiping a card or using a PIN and, similarly, Chase Bank's "Blink" card permits consumers to pay for goods by simply waving their card near a scanner.[289] Many motorists use RFID-enabled passes such as FasTrak or E-Z Pass to electronically charge their accounts when traveling on toll roads or over bridges or through tunnels.[290]

Amusement parks have also begun offering RFID-tagged wristbands so that parents can keep track of where their children are in the park.[291] In addition to keeping tabs on their children, parents may use the wristbands as a cashless payment system, charging their credit or debit card in order to use the wristband to purchase items at the park's souvenir or concession stands.[292] According to recent press reports some systems also permit "parks to record and study the buying habits and activities of visitors, so the parks can offer customer loyalty programs, or incentives for underutilised games or attractions."[293]

Tracking Children

In Japan, children participated in a trial in which they wore tagged bracelets which tracked them while walking to and from school in an attempt to monitor their safety.[294] The tags sent a regular signal to various Wi-Fi access points (which functioned as readers) throughout the area allowing the children's whereabouts to be traced, and parents could be notified via e-mail or mobile phone when a child passed a particular access point.[295] The tags themselves contained only a unique identification number and did not contain any personal information about the child.[296] The readers were connected to a centralised database which contained personal information related to the unique identification number such as the child's name, home address and telephone number.[297]

In a controversial experiment students at a California middle school were required to wear RFID-tagged identification badges to take their attendance.[298] In Texas a Houston-area school district monitored the arrival and departure on school buses of 28,000 students using RFID tags in school badges.[299]

---

[289] *Consumer Reports* (June 2006), p.35
[290] Id. at 34
[291] Collins, Jonathan, *RFID Journal*, 28 April 2004
[292] *RFID Journal* (27 November 2002)
[293] Id.
[294] Swedberg, Claire (16 December 2005)
[295] Id.
[296] Id.
[297] Id.
[298] Lucas, Greg, *The San Francisco Chronicle*, 10 February 2005
[299] Richtel, Matt, *The New York Times*, 17 November 2004

Use in Humans

In October 2004 the U.S. Food and Drug Administration approved the use of VeriChip, an implantable computer chip about the size of a grain of rice that uses RFID technology to convey a unique identification code to a reader.[300] The identification code is then linked to the individual's personal information stored on a database.[301] According to recent press reports, about 2,500 chips have been sold by VeriChip Corporation worldwide for use in people, including 100 in the United States.[302]

In the medical context the chip is implanted under the skin of the upper arm using a large-bore needle and doctors then "scan patients like cans of soup at a grocery store. Instead of the price, the patient's medical record would pop up on a computer screen."[303] If a patient is unconscious doctors can use the device to access the medical record and learn what medications the patient is taking, his or her blood type or any drug allergies.

While VeriChip Corporation has marketed its human-implantable RFID microchip to hospitals and physicians for medical use, it also promotes the technology for other uses such as "access control," stating on its website:

> With VeriChip's patented, FDA-cleared, human-implantable RFID microchip technology, access control has achieved a new level of protection never offered before. Now, organizations can protect entire buildings, floors, or designated areas with the highest level of security available today and easily incorporate this into existing building control systems. Additionally, staff, visitors, and even assets can be tracked within the facility in real-time.[304]

Although the VeriChip is largely attracting interest as a way to provide doctors with quick access to a patient's medical records, it has also been used in other enterprising ways. Bar patrons in Spain have had a microchip implanted in order to gain entry to VIP areas and run electronic tabs.[305] Employers have also used the technology to restrict employee access to secure facilities. CityWatcher.com, a U.S. company based in Ohio, which stores footage from surveillance cameras around the country, inserted RFID tags into two employees to control access to a room holding video footage.[306] In July 2004 Mexico's attorney general announced that he and about 160 of his high-ranking officers had had an RFID chip implanted in order to control access to high-security offices.[307]

Finally, Belgian scientists have embedded an RFID chip into a tooth in an effort to help forensic scientists identify bodies after a natural disaster or terrorist attack.[308] A person's name, nationality, date of birth and gender could all be accessible using the tag which has been shown to withstand normal biting forces and temperatures of up to

[300] Stein, Rob, *The Washington Post*, 14 October 2004, p.A1
[301] Id.
[302] Stein, Rob, *The Washington Post*, 15 March 2006, p.A1
[303] Stein, Rob, *The Washington Post*, 14 October 2004, p.A1
[304] VeriChip Corporation (n.d.)
[305] *SiliconValley.com*, 13 October 2004
[306] Waters, Richard, *Financial Times*, 12 February 2006
[307] Stein, Rob, *The Washington Post*, 14 October 2004, p.A1
[308] 'RFID Chip Hides in Tooth', 3 March 2006

450 degrees Celsius although normal expansion and contraction of the tooth appears to still be problematic.[309]

Employment Use

Many employee identification cards use RFID technology to control access to buildings and workplaces. RFID-tagged identification cards are held up to a reader and, like a key, access is permitted when it is confirmed that the cardholder is authorised to access the facility.[310] Access control systems using RFID technology can be integrated with other systems such as closed-circuit TV (CCTV) cameras or a photo ID system in which the scanned identification card pulls up a photo in the database which a guard then uses to confirm identification.[311]

Pharmaceutical Industry

For the past few years the U.S. Food and Drug Administration (FDA) has encouraged the pharmaceutical industry to use RFID tags to help protect the safety and security of the nation's drug supply by tracking drugs through the supply chain.[312] The FDA hopes that such use of RFID technology will be common in the pharmaceutical industry by 2007.[313] Often referred to as an "electronic pedigree" (or "ePedigree"), the FDA envisions a system in which an electronic chain of custody is created for each individual drug product from the point of manufacture to the point of dispensing.[314] The FDA hopes that the use of RFID technology will enable manufacturers and retailers to quickly identify counterfeit drugs, conduct targeted recalls and verify the authenticity of a drug.[315] On 9 June 2006 the FDA announced that it will fully implement regulations which require drug distributors to document the chain of custody of drugs throughout the distribution system.[316]

Several pharmaceutical companies have already begun using RFID technology, beginning with drugs more susceptible to counterfeiting and theft such as Viagra, the painkiller OxyContin and the HIV drug Trizivir. Pfizer's use of RFID to tag Viagra is not an e-Pedigree system, but instead is intended to allow wholesalers and pharmacists to verify that a bottle of the drug is authentic.[317] GlaxoSmithKline on the other hand is piloting an ePedigree system to track each bottle of Trizivir through the supply chain.[318]

Passports

In February 2006 the United States government announced that it had begun issuing RFID-enabled passports (often called "e-passports") to diplomats on a trial basis and

[309] Libbenga, Jan, *The Register*, 20 March 2006
[310] Balkovich, Edward (2005), p.2
[311] Id. at 11
[312] U.S. Food and Drug Administration, *FDA Consumer Magazine*, March-April 2005
[313] Id.
[314] Id.
[315] Id.
[316] U.S. Food and Drug Administration (9 June 2006)
[317] *RFID Update*, 9 January 2006
[318] *RFID Update*, 24 March 2006

indicated that all new U.S. passports will contain RFID tags by the end of 2006.[319] The RFID chip contains the same data that is currently displayed in the passport: the holder's personal information (name, date and place of birth, nationality, gender, passport number, dates of issuance and expiration) and a digital photograph. According to the State Department the RFID tags are passive tags and are equipped with an encryption feature to prevent eavesdropping by a third party and the front covers of the passports contain an anti-skimming device to block radio waves.[320]

In September 2005 New Zealand began issuing e-passports which employ contact-less chip technology that uses radio frequency to communicate with the reader.[321] Along with Australia and Singapore, New Zealand took part in a three-month trial conducted at San Francisco Airport to test the e-passport systems.[322] The chips contain the holder's personal information already contained in passports and a digitised photograph.[323] All newly issued passports now contain the contact-less chip technology.[324]

Privacy Issues Concerning RFID Technologies

Many believe that it is not RFID technology in and of itself but rather its application that has the potential to raise privacy concerns. In early 2005 Blair Stewart, the Assistant Privacy Commissioner New Zealand, wrote "I suspect that like the introduction of most technologies, RFID chips will be neutral in their impact on privacy. It is the way that RFID is deployed that makes all the difference."[325]

While some applications of RFID technology do not raise any privacy issues, other applications implicate privacy in a number of ways of concern to privacy advocates. For example, most agree that RFID tagging of pallets and cartons and subsequent tracking throughout the supply chain raises few, if any, privacy concerns. On the other hand, implanting RFID chips in humans or embedding tags in clothing causes concern to many in the privacy community. In January 2005 the 25 Privacy Commissioners in the European Union expressed concern about "the possibility for some applications of RFID technology to violate human dignity as well as data protection rights" and in particular worried about the possibility of tracking and profiling, which are explained below.[326]

Most RFID use in the retail context has so far been confined to use in the supply chain and on the retail floor for inventory control and management. Pallets and cartons are tagged with passive tags to better monitor their movements through the chain. In those cases in which individual items are tagged, the tags used are removable and can be thrown away after purchase. Privacy advocates, however, worry that the next step will be to embed RFID tags in products themselves and therefore removal will not be an option. Embedded tags can also be quite small: Hitachi Europe has developed an

[319] Belopotosky, Danielle, *National Journal's Technology Daily*, 21 February 2006
[320] U.S. State Department, *The U.S. Electronic Passport Frequently Asked Questions*
[321] Phone conversation with David Philp, Manager, Passports, Department of Internal Affairs (Wellington, 21 June 2006)
[322] *Dominion Post*, 24 April 2006
[323] Tunnah, Helen, *New Zealand Herald*, (29 October 2005)
[324] David Philp (Wellington, 21 June 2006)
[325] Stewart, Blair (9 February 2005)
[326] Article 29 Data Protection Working Party (19 January 2005), p.2

RFID chip that is so small it can be embedded in a piece of paper.[327] It is not clear however what the read range of such a tag might be.

Tracking and monitoring

Many argue that the use of RFID technology where collected information is linked to a tag raises concerns about the potential for tracking or monitoring. In March 2006 the European Commission began holding a series of public hearings and meetings on the use of RFID tags in order to explore concerns about the technology.[328] The results are expected to be presented and discussed at a final conference in October 2006 and a final Communication from the European Commission to the European Parliament and Council is expected in December 2006.[329] In a speech detailing the inquiry Viviane Reding, European Commissioner for Information Society and Media, stated that "[t]he marriage between RFID and databases can indeed lead to micro-monitoring and widespread tracking of people's daily lives. The European Commission shares concerns about a future of ubiquitous surveillance, identity theft and low trust. User trust and confidence is a crucial element for the take-up of RFID."[330]

With respect to the issue of potential tracking, it is important to note that tracking is only possible where there are RFID readers to read compatible tags. As a result, unless readers are located on every street corner, it is more difficult to track individuals using RFID as compared to a global positioning system (GPS) which uses satellite technology to provide location data in real-time. As evidenced by the tracking of schoolchildren in Japan described above, however, it is possible to create a system in which RFID technology is used to track individuals within a defined area.

The issue then seems to be a concern for the potential of the ubiquitous use of RFID tags in everyday products and the subsequent linkage to larger information systems as explained by the Organisation for Economic Co-operation and Development (OECD): "In theory, RFID applications make it possible to track people through the RFID tags they carry with or on them. This will become more relevant if different RFID applications are integrated into a larger system. For example, the EPC Global system of tags creates globally unique identifiers for each tagged product."[331] Theoretically however, such a scenario would be unlikely if tags are deactivated at the point of sale.

In comments to the Department of Homeland Security regarding the draft report "The Use of RFID for Human Identification," the AeA (American Electronics Association) responds to concerns regarding the use of RFID to track people, arguing that "technology by itself cannot track people; only those who control the data may track people."[332] Furthermore, the organization writes, "because a number of remotely readable RF-enabled technologies can accommodate encryption and on-board processing of information, this technology would actually provide additional

[327] Vierria, Dan, *Sacramento Bee*, (12 May 2006)
[328] O'Brien, Kevin, *International Herald Tribune*, 15 May 2006 Also, see, Sayer, Peter, *Computerworld*, 20 March 2006
[329] European Commission (6 July 2006)
[330] Reding, Viviane (9 March 2006)
[331] Organisation for Economic Co-operation and Development (27 February 2006), p.21
[332] AeA (20 May 2006)

protections and security against unauthorized tracking."[333]

Profiling

Some argue that certain RFID use can lead to the possibility of profiling. Profiling raises privacy issues because of the possibility that collected information will be compiled into a database and disclosed without the knowledge of the individual to whom the information pertains. The OECD report raised this issue, among others, explaining: "An RFID application could collect large amounts of data. If a tagged item is for example paid for by credit card or in conjunction with use of a loyalty card, then it could be possible to tie the unique ID of that item to the identity of the purchaser. Personal data, obtained through RFID, could be used to create a profile of a person. Such a profile could then be used for various purposes, for example to evaluate a consumer's worth to a company."[334] Similar concerns were mentioned by Canada's Federal Privacy Commissioner in her 2005 annual report to Parliament on the Personal Information Protection and Electronic Documents Act in which she indicated an intention to develop guidelines.[335] Others have also raised concerns that profiling of consumers could lead to additional marketing or dynamic pricing.[336]

In November 2003 the International Conference of Data Protection and Privacy Commissioners approved a final resolution on RFID which highlighted "the need to consider data protection principles if RFID tags linked to personal information are to be introduced" and raised concerns about the potential for the technology to be used to "locate or profile persons possessing tagged objects" and trace individuals.[337]

Covert collection

A principal privacy concern regarding the use of RFID technology is the potential for the covert collection of information from the tag, a possibility because the tag and compatible reader do not have to be in contact in order to communicate using radio waves. The decreasing size of both tags and readers further complicates the issue. On this point the OECD report noted: "The potential invisibility of RFID tags as well as readers is considered to be one of the major privacy concerns with RFID. Hence, there may be a possibility to collect information about a certain product, and – depending on the circumstances – also about the person carrying the product, without the knowledge or consent of the individual carrying the product."[338] The final resolution approved in November 2003 by the International Conference of Data Protection and Privacy Commissioners also raised the issue, indicating concern about the "remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process."[339]

AeA argues that safeguards are available to protect against covert collection by unauthorised readers. For example, "on-board processing directly on the contactless

[333] Id.
[334] Organisation for Economic Co-operation and Development (27 February 2006), p.21
[335] Office of the Privacy Commissioner of Canada (May 2006)
[336] Article 29 Data Protection Working Party (19 January 2005), p.6
[337] International Conference of Data Protection and Privacy Commissioners (20 November 2003)
[338] Organisation for Economic Co-operation and Development (27 February 2006), p.21
[339] International Conference of Data Protection and Privacy Commissioners (20 November 2003)

integrated circuit (IC) of the chip"[340] permits credentials to be programmed to "choose which readers are authorized to read and/or collect all, some or none of the data contained in the credential."[341] Also, *RFID Journal* responded to the concern that criminals could decide which homes to rob by using high-powered readers to scan all the items in a home.[342] The journal stated: "That's very unlikely. For a reader to read passive tags through the walls of a home from the street, the power output would have to be so high that the popcorn in the cupboard would start popping. In addition, the criminal would obtain only a string of serial numbers, which might have no meaning unless it were [sic] a truly sophisticated criminal with access to EPC databases. And looking in windows would probably be a cheaper and more effective way of figuring out whether there are items in a house worth stealing."[343]

Identity theft: eavesdropping and skimming

The increased use of RFID technology also has the potential to raise identity theft concerns such as "skimming" in which information on a tag could be surreptitiously "read" by another person with a reader or "eavesdropping" where information transmitted between a tag and reader is secretly intercepted by another person.[344] Similar issues were raised in a draft report from the Department of Homeland Security's Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee. [345] AeA recommends that government agencies adopt specified privacy principles including that the "exchange of personal identifiable information between the ID and the reading device must be protected to prevent unauthorized capture and use of data to impersonate an individual."[346]

Databases

Others raise concerns that increased use of RFID technologies to collect information could lead to data aggregation requiring the "creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand."[347] Database security is also potentially a concern as has been illustrated by the many incidences of breaches in database security, particularly in the United States.

Efforts in New Zealand to Regulate RFID Technologies

In addition to the Privacy Act 1993 which is a broad, comprehensive statute that arguably regulates RFID technology,[348] more specific self-regulatory efforts have been undertaken in New Zealand. In March 2005 GS1 New Zealand issued the

[340] AeA (20 May 2006)
[341] Id.
[342] RFID Journal (n.d.)
[343] Id.
[344] Article 29 Data Protection Working Party (19 January 2005), p.6 and *Consumer Reports* (June 2006), p.36
[345] U.S. Department of Homeland Security (May 2006), p.9
[346] AeA (20 May 2006)
[347] 'RFID Position Statement of Consumer Privacy and Civil Liberties Organizations' (20 November 2003)
[348] For more discussion of this issue, see the later section of this report entitled "Privacy Act 1993: Threshold Definitional Questions"

"EPC/RFID Consumer Protection Code of Practice" which was prepared by a committee established by Standards New Zealand and was made up of representatives of a number of organizations, including the Consumers' Institute, GS1 NZ, Ministry of Consumer Affairs, New Zealand Retailers Association, NZ Food and Grocery Council (Colgate-Palmolive Ltd) and Pharmacy Guild.[349] The code is intended to be used by retailers who stock RFID-tagged products; it does not cover use in the supply chain.[350]

In the eyes of some, the code was an imperfect compromise as, on the one hand, it informs people of the use of RFID, but on the other hand, it does not provide for an explicit right for them to opt-in to the use of RFID technology before it is used.[351] The code which is voluntary, requires some notice to consumers of the retail use of RFID and applies only to items containing an RFID tag which is used for the purposes of "customer service".[352] Under the code retailers must provide at least 28 calendar days' notice to consumers of the pending activation of RFID technology either in the form of signage or other written material provided to consumers when they enter the store.[353] The code does not specify what information must be provided in the notice and presumes compliance with the notice requirements under Principle 3 of the Privacy Act.[354]

Efforts in California to Regulate RFID Technologies

With respect to RFID California's Information Privacy Act provides some protections. For example, individuals have a right to access information collected using RFID that is maintained in a state agency's records. As discussed earlier however, the Act's notification requirements do not appear to apply to the collection of information using RFID. Other, more RFID-specific efforts have been undertaken.

Legislative Efforts

As described in greater detail later in this report, there have been several legislative attempts in California to regulate or restrict the use of RFID technology. None have so far been successful.

In 2005 Senator Simitian introduced Senate Bill 682 (Simitian), a broad measure which would have prohibited government identification documents using RFID from transmitting or enabling the remote reading of any personal information other than a unique personal identifier number.[355] The bill would also have required the public agency issuing the RFID-tagged identification document to provide written notice of specified information to an individual as well as annual notice of any changes in the

[349] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[350] Id.
[351] Interview with David Russell, Chief Executive, Consumers' Institute (Wellington, 26 April 2006)
[352] *EPC/RFID Consumer Protection Code of Practice* (March 2005). The term 'customer service' is not defined in the code and arguably has the potential to be interpreted in an overly broad manner.
[353] Id.
[354] Interview with Gary Hartley, Manager for Strategic Initiatives, GS1 New Zealand (Wellington, 5 May 2006)
[355] Senate Bill 682 (Simitian), as amended 15 August 2005. These same provisions were inserted into Senate Bill 768 (Simitian), as amended 2 September 2005. All California bills may be obtained from www.leginfo.ca.gov

location of readers or the information collected or stored in the database.[356]

Senate Bill 682 was placed on the inactive file on the Assembly Floor, and the author subsequently introduced two narrower measures which are pending in the current legislative session. First, Senate Bill 433 (Simitian) prohibits the California Department of Motor Vehicles from issuing or renewing a driver's license or identification card using radio waves "to transmit personal information remotely or to enable personal information to be read from the license or card remotely."[357] Second, Senate Bill 1078 (Simitian) prohibits public schools from issuing any device to a pupil that uses radio waves to transmit personal information remotely or enable the remote reading of personal information in order to record the pupil's school attendance or establish or track the pupil's location on school grounds.[358] Both bills, which are opposed by the high tech industry, were recently amended to include a three-year sunset provision.[359]

In response to these other efforts restricting the use of RFID technology, the American Electronics Association (AeA) has sponsored Assembly Bill 2561 (Torrico) which requires the California Research Bureau (CRB) to report to the Legislature on security and privacy issues relating to government-issued "remotely readable identification credentials."[360] The bill requires the CRB to establish an advisory board made up of representatives of various organizations including the Office of Privacy Protection, Department of Motor Vehicles, California School Boards Association and industry and privacy groups.[361] The bill also requires the CRB to develop legislative policy options for "ensuring safety and security of information contained on remotely readable identification documents."[362] The measure is currently pending.

In 2004 Senate Bill 1834 (Bowen), as introduced, would have provided an individual with the right to access his or her personally identifiable information collected through an RFID system.[363] The bill would also have permitted an individual with the right to make corrections to that information. These provisions were deleted from the bill which later failed passage in the Assembly Business and Professions Committee.

At the federal level, at least one measure has been introduced to regulate the use of RFID in the retail context. In 2004 U.S. Representative Kleczka introduced H.R. 4673, the "Opt Out of ID Chips Act", which would have required warning labels on consumer products containing RFID.[364] The bill was referred to the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce, but no action was taken. Federal legislation restricting the use of RFID faces an uphill battle in the current Congress however, as demonstrated by the "Policy Agenda" of the Senate Republican High Tech Task Force. The agenda states that one of its goals is to "[p]rotect exciting new technologies from premature regulation or legislation in search of a problem. RFID holds tremendous promise for our economy,

[356] Id.
[357] Senate Bill 433 (Simitian), as amended 15 June 2006
[358] Senate Bill 1078 (Simitian), as amended 15 June 2006
[359] Senate Bill 433 (Simitian) and Senate Bill 1078 (Simitian), both amended 15 June 2006
[360] Assembly Bill 2561 (Torrico), as amended 2 May 2006
[361] Id.
[362] Id.
[363] Senate Bill 1834 (Bowen), as introduced
[364] Copies of all U.S. Congressional bills may be obtained from http://thomas.loc.gov

including military logistics and commercial inventory efficiencies, and should not be saddled prematurely with regulation."

Self-Regulatory Efforts

In May 2006 the Center for Democracy and Technology (CDT) issued best practice guidelines for the use of RFID in the U.S. commercial and private sector which it had developed with RFID vendors, corporate representatives and consumer groups.[365] The guidelines apply to those instances where RFID technology is used to collect information which is then linked to personal information.[366] Under the guidelines, which are described in greater detail later in this report, individuals must be given clear, conspicuous and concise notice specifying the presence of an RFID tag, the purposes for which the information is being collected, how the information will be used and whether the information may be used for additional or subsequent uses, such as marketing.[367]

Privacy Act 1993: Threshold Definitional Questions

Before analysing how each of the selected criteria might apply to New Zealand's Privacy Act 1993 in light of specific technologies, it is important to discuss threshold definitional questions which have been raised concerning the Act.

Whether information collected by an RFID tag is "personal information" under the Privacy Act 1993

The Privacy Act applies only to "personal information" which is defined as "information about an identifiable individual."[368] Some uses of RFID technology likely do not implicate the Privacy Act because there is no link between the information on the tag and an "identifiable individual". For example, the information collected from RFID tags used in the supply chain and attached to pallets or cartons to track shipments is arguably not "personal information" under the Act because it is not linked to an identifiable individual.[369]

In other instances however, information collected using RFID tags is linked to a specific individual via a database. In most cases, although RFID tags can hold additional information, at this point in time they generally contain only a unique number that is then linked to the database which identifies the object or person to which the tag is attached. As a result the question arises as to whether, if the information collected by the reader is simply a unique string of numbers, is this information "personal information" under the Privacy Act? In other words, does the Privacy Act apply to the collection of information using RFID technology if the information is simply a string of numbers?

---

[365] Center for Democracy and Technology (1 May 2006)
[366] Id.
[367] Id.
[368] Privacy Act 1993, s 2(1)
[369] In some instances information collected from RFID tags used in the supply chain might be linked to an identifiable individual and the Privacy Act would then apply. For example, if the information is used to monitor an employee's performance by linking a tagged pallet or carton to an identifiable individual. Roth (February 2006), p.12

As described in *Privacy Law and Practice*, another way to restate the issue is "whether the individual to whom the information relates must be identifiable from the information itself alone, or whether it is sufficient that identification can be made on the basis of a link identifying the individual, whether that link is supplied by the recipient's knowledge from other sources, or by other means, such as context, identification numbers and the like."[370]

A related issue was raised in *Proceedings Commissioner v Commissioner of Police* in which the Complaints Review Tribunal (now the Human Rights Review Tribunal) considered a case in which personal information about a woman was allegedly unlawfully disclosed to the news media by a police sergeant.[371] The Tribunal rejected the defendant's argument that there was no breach under the Privacy Act because the woman in question could only be identified by people who already knew her.[372] Instead the Tribunal held that information was "personal information" under the Privacy Act as long as it has the capacity to identify the individual to some members of the public[373] and further stated: "it is not necessary . . . that an individual should be able to be identified to the world. It is enough that they are able to be identified by anyone who can make an identification as a result of the receipt of personal information not previously known."[374]

Similarly, in the case of an RFID tag that contains only a unique number which is then linked via the database to a specific individual, one could certainly argue that the information collected using an RFID tag is personal information under the Privacy Act as it "has the capacity to identify" the individual on the basis of a link to the database.

In *Harder v Proceedings Commissioner*, the Court of Appeal commented in obiter dicta on the scope of the definition of personal information, suggesting that it should be read down.[375] The comments were considered surprising by many in the field as "personal information" had consistently been broadly interpreted by the Privacy Commissioner, Ombudsmen and the courts over the previous two decades.[376] In *Apostolakis v Sievwrights*, which is on appeal, the Human Rights Review Tribunal discussed the Court of Appeal's comments in the *Harder* case before finding that the letter in question did contain personal information about the plaintiff.[377] The issue of the scope of personal information is certainly one to monitor. While the definition of "personal information" might seem overly broad to some, there are other limitations in the Act which constrain it.[378]

---

[370] Roth, *Privacy Law and Practice*, para 1002.10
[371] *Proceedings Commissioner v Commissioner of Police* (16 December 1999) CRT 23/99, Decision No 37/99
[372] Human Rights Commission Case notes (April 2000)
[373] Roth, *Privacy Law and Practice*, para 1002.10
[374] *Proceedings Commissioner v Commissioner of Police* (16 December 1999) CRT 23/99, Decision No 37/99, p.7
[375] *Harder v Proceedings Commissioner* [2000] 3 NZLR 80; (2000) 6 HRNZ 173 (CA), para 23-24. See, also *Boyle v Manurewa RSA Inc* (12 June 2003) HRRT 29/02, Decision No 16/03
[376] Roth, *Privacy Law and Practice*, para 1002.10. See, also Evans (July 2001), pp.39-42
[377] *Apostolakis v Sievwrights* (14 February 2005) HRRT 44/03, Decision No 01/05, para 47-62
[378] Evans (July 2001), p.39

Although not directly on point to this issue, it is worth mentioning that it has been argued by some that "even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies."[379] In this case, would the Privacy Act apply since there is no link to personal information? Is this "information about an identifiable individual"? It is not clear, but the Human Rights Review Tribunal has found that "there is no 'bright line' test which separates that which is obviously personal information about an identifiable individual from that which is not. Much will depend in any given case on the context in which the information is found. There may be particular factors in different settings that compel a conclusion that, although the requesting individual is not named in the information, nonetheless there is a sufficient connection between the information and the requester to justify a conclusion that the information is personal information 'about' the requester."[380]

Whether, for purposes of Principles 1 – 4, RFID technology is covered by the Privacy Act 1993

Professor Paul Roth has raised questions as to whether or not RFID technology is covered by the Privacy Act, arguing that for purposes of Principles 1 – 4 the Act may not apply to RFID use because: (1) gathering information using an RFID tag is not a collection of personal information "directly from" the individual concerned and (2) as defined under the Act, "collection" does not include the receipt of unsolicited information.[381] Both of these issues arise only with respect to the collection principles.

1) Is gathering information using an RFID tag a collection of personal information "directly from" the individual concerned?

Because the Privacy Commissioner recommended in the "Third Supplement to the First Periodic Review of the Operation of the Privacy Act 1993" that the word "directly" should be deleted from Principle 3,[382] it is not necessary to discuss this issue at great length.

Briefly, Professor Roth has questioned whether information obtained using an RFID tag is collected "directly" from an individual or whether it is instead collected from the embedded RFID chip.[383] In related arguments concerning workplace surveillance and monitoring he has argued that "directly" in this case should be interpreted as concerning "the subject's awareness of the collection of information," or whether the collection is done openly or straightforwardly.[384] If the term is interpreted in this way, Professor Roth argues, there is a gap in the Privacy Act's coverage of video surveillance. Robert Stevens has written in response to this argument, suggesting instead that the better interpretation is one in which the word "directly" is interpreted "to indicate that the collection is from the individual himself or herself, without the

[379] Information and Privacy Commissioner/Ontario (February 2004), p.17, citing 'RFID Position Statement of Consumer Privacy and Civil Liberties Organizations' (20 November 2003)
[380] *CBN v McKenzie Associates* (30 September 2004) HRRT 020/04, Decision No 48/04, para 41
[381] Although these issues have been raised regarding RFID technology and surveillance cameras (Roth, *Privacy Law and Practice*, para 1002.6A and 1006.17), they may also apply to other technologies such as the collection of biometric information using facial recognition technology.
[382] Privacy Commissioner (18 December 2003), Recommendation 19A
[383] Roth (February 2006), p.12
[384] Roth (November 1997) , p.118

information passing through some intermediary."[385] Under this interpretation, Robert Stevens argues, there is no gap in coverage under the Privacy Act.

It is hopeful that the Privacy Commissioner's recommendation deleting "directly" from Principle 3 will be included as part of the Government's proposals to reform the Privacy Act, thus removing uncertainty on this point.

2) Is obtaining information using an RFID tag a "collection" under the Privacy Act 1993?

The second issue raised by Professor Roth questions whether obtaining information using an RFID tag is a "collection" under the Privacy Act because the Act specifically states "collect does not include receipt of unsolicited information."[386] With respect to this issue Professor Roth has stated: "Arguably, there is a question whether or not information obtained through RFID is 'solicited' from the individual, as it is automatically transmitted by the tag to the reader."[387]

In support of a similar argument that video cameras do not "collect" personal information under the Privacy Act, Professor Roth has cited the Court of Appeal's decision in *Harder v Proceedings Commissioner* in which the Court held that a surreptitious tape recording of a telephone conversation was not a "collection" under the Privacy Act where the information provided was unsolicited.[388] In doing so, the Court rejected the finding by the Complaints Review Tribunal that "when he switched on the tape recorder Mr Harder changed from being a passive recipient of unsolicited information to an active recorder 'and therefore collector' of the information . . . The unsolicited nature of the information was not affected by the fact that it was recorded or the way it was recorded."[389]

Admittedly the *Harder* decision has potentially thrown uncertainty on the question of whether information obtained using a technology such as RFID might be a collection under the Privacy Act. To the extent that the technology is similar to a tape recorder and the information on an RFID tag is not solicited from an individual but is instead passively received by the reader,[390] it could be argued that the information provided was unsolicited and therefore no "collection" occurred under the Privacy Act.

That would be an overly technical reading of the Act however, and ignore the spirit of the law which, according to its Long Title is to "promote and protect individual privacy in general accordance with the Recommendation of the Council of the

---

[385] Stevens (September 1998), p.116
[386] Privacy Act 1993, s 2(1)
[387] Roth (30 March 2006)
[388] Roth, *Privacy Law and Practice*, para 1002.6A and 1006.17; *Harder v Proceedings Commissioner* [2000] 3 NZLR 80; (2000) 6 HRNZ 173 (CA)
[389] Id. at para 25
[390] As described above however, RFID tags can be either passive or active. Passive tags receive their power from the reader and do not initiate communication. Some active tags, on the other hand, broadcast their information without the assistance of a reader. Arguably then, in the case of passive tags, the information provided could be seen as "solicited" because the tags "awaken" in response to a reader while in the case of certain active tags the information received is unsolicited. Determining whether there has been a "collection" under the Privacy Act depending on the type of tag involved, however, seems somewhat absurd and overly legalistic.

Organisation for Economic Co-operation and Development [OECD] Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."[391] It is significant that, in a recent report, the OECD has stated that RFID use linked to personal information is covered by the guidelines. The report noted that "Processing personal data through RFID technology is also subject to the principles contained in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."[392] Arguably then, "collection" under the Privacy Act should be interpreted broadly to include obtaining information using RFID technology in accord with the OECD Guidelines. Moreover, the Privacy Act deals with human rights issues, and it has been said that "legislation of that kind should be given a broad and liberal interpretation, rather than a narrow and restrictive one."[393]

Furthermore, the installation of an RFID system, including a tag, reader and database, certainly envisions the collection and solicitation of information. Indeed that is its whole purpose. The system is designed to obtain information from the tag and is installed to have a deliberate focus on certain individuals. For example, RFID-enabled building access cards are used at entrances to restrict access so that only those authorised to enter are permitted to do so.

Similarly, a recent decision by the Human Rights Review Tribunal contains discussion of when information is unsolicited and the extent of the word "collect" under the Privacy Act. Although not dispositive, the discussion may be helpful to the issue. In *Stevenson v Hastings District Council*, the Tribunal considered a case in which the District Council had set up monitoring devices around the plaintiff's property in order to record his barking dogs.[394] The Tribunal dismissed the plaintiff's claim that the Council had breached Principle 4, finding that he did not suffer any adverse consequences as a result of the Council's actions. After reaching this finding, which disposed of the case, the Tribunal went on to briefly discuss several other issues which had been raised, including whether the recording was a collection of information under the Privacy Act. With respect to this issue, the Tribunal distinguished the case from that in *Harder v Proceedings Commissioner* and stated in relevant part:

> In our view it is at least arguable that, even though the Council may not have set out to collect personal information about Mr Stevenson, the way in which it set up its devices was such that when it in fact collected information of that kind, the information was not 'unsolicited' in the sense intended by s.2.[395]

Finally, the purpose of excluding unsolicited information from a "collection" under the Privacy Act is to arguably deal with those situations in which an agency does not have control over a situation and how it is receiving information. It cannot define or set the factors or boundaries under which the information is received when someone simply volunteers the information. It is debatable whether using RFID technology to gather personal information raises these same kinds of issues when an agency purposely decides where to put a tag, where to place a reader, what information will

[391] Privacy Act 1993
[392] Organisation for Economic Co-operation and Development (27 February 2006), p.22
[393] *Apostolakis v Sievwrights* (14 February 2005) HRRT 44/03, Decision No 01/05, para 58
[394] *Stevenson v Hastings District Council* (14 March 2006) HRRT 29/04, Decision No 07/06
[395] Id. at para 89

be contained on the tag, how the information will be conveyed (e.g., using encryption or not) and who will be able to access the database containing the collected information.

Having made these arguments however, if there is any doubt as to whether RFID technology is covered by the Privacy Act (for purposes of the collection principles) in light of the *Harder* decision, then it is recommended that the issue should be clarified and included as part of the Government's proposals to reform the Privacy Act 1993.[396]

Application of Criteria to Each Approach

For purposes of the following analysis it is assumed that the Privacy Act 1993 applies to RFID technology notwithstanding the threshold definitional questions noted above.

Trust *– Individuals will have trust in the system of data collection and this trust will not be misplaced*

As a measure of the success of a privacy protection regime, trust plays an important role in this analysis. Although it is not quite a criterion like openness, choice, control, balance, flexibility or certainty, this section will evaluate how each of the privacy protection approaches furthers the goal of trust with respect to RFID technology.

Trust is particularly important in a system that uses RFID technology to collect personal information. RFID technology allows for the potential of covert collection of personal information, eroding consumer trust. Even when an individual knows that her information is being collected, it is not obvious precisely what information is being collected. Furthermore, RFID tags are linked to databases via the tag readers. Depending on the system, these databases can contain vast amounts of personal information. For example, the VeriChip used for human implantation can be linked to a database containing a patient's medical records.

Comprehensive Approach

Principle 3: Collection of Information from Subject

Trust and openness raise similar issues with respect to Principle 3, and many of these are detailed below in the openness section. By requiring agencies to provide notification of the fact that personal information is being collected, the purpose of the collection and who will be able to access the information, Principle 3 helps agencies build trust by furthering openness and transparency and thus promoting privacy. Agencies that use RFID to collect personal information can also help to build trust by going beyond the Privacy Act and telling consumers what information is being collected by the technology.

When he was Privacy Commissioner Bruce Slane noted that "[t]ransparency of purpose can be used by businesses to build up consumer trust and confidence. Being

[396] As mentioned earlier, although much of this discussion has focused on RFID, similar arguments regarding the scope of the Privacy Act could be made concerning other technologies like surveillance cameras (see Roth, *Privacy Law and Practice*, para 1002.6A and 1006.17) or biometrics collections like facial recognition technology.

open about why information is collected and how it will be used means consumers will not be surprised when it is used in that way. Consumers who trust a business are likely to return and to comment favourably on their experience to others."[397] Similarly, Federal Privacy Commissioner of Australia Karen Curtis' keynote address to the 2006 Privacy Issues Forum included examples in which consumers had ceased to trust a company and taken their business elsewhere because it had failed to adequately protect their personal information.[398]

Principle 4: Manner of Collection of Personal Information

Principle 4 provides that personal information shall not be collected by an agency by unlawful means or by means that, under the circumstances of the case, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.[399] In the case of the collection of personal information using RFID technology, the covert collection of information could arguably be "unfair" or "intrude to an unreasonable extent," depending on the context. For example, if a business told consumers it would not collect personal information from RFID tags and then did so covertly, it could be argued that this was an unfair means of collection.

To the extent that agencies are not engaging in a collection that could be in breach, they help to build consumer trust. If, instead, agencies engage in covert collection that meets the "unfair" and "intrusive" thresholds, and such collection becomes public knowledge, consumer confidence and trust will likely be eroded.

Principle 5: Storage and Security of Personal Information

Principle 5 is relevant to database security and RFID systems. The principle provides that an agency that holds personal information must employ reasonable security safeguards to ensure that the information is protected against loss and unauthorised access, use, modification or disclosure and other misuse.[400] As described earlier, the security of a database is closely linked to trust, and consumers arguably feel more secure, and trust a system more, knowing that their personal information is protected and not open to breach. If an agency does not comply with Principle 5 and personal information it holds is subject to loss or unauthorised access or use, the individuals to whom the information pertains are less likely to trust both the agency and, potentially, the privacy regime that oversees it.

In the case of RFID tags linked to a database, the agency holding the information collected from the tags would need to ensure that reasonable safeguards are in place to protect the information contained in the database. The Privacy Commissioner has written several case notes in instances in which a violation of Principle 5 has been alleged. While none of the cases appear to be specifically related to a breach in database security systems, they do concern unauthorised disclosure, access or misuse and loss and, as a result, the findings contained in the case notes are helpful to understanding how the principle may be applied to RFID systems.

[397] Slane, Bruce (9 April 1999)
[398] Curtis, Karen (30 March 2006)
[399] Privacy Act 1993, s 6
[400] Privacy Act 1993, s 6

The Privacy Commissioner has found that security safeguards under Principle 5 have to be "reasonable, not fail-safe."[401] In a case note detailing a complaint from a woman who had received another person's letter enclosed with her letter, the Privacy Commissioner listed the following factors relevant to whether security safeguards were reasonable under the circumstances: (1) the workability of the safeguards; (2) the cost of the safeguards; (3) the risks involved; (4) the sensitivity of the information; and (5) the other safeguards in place.[402]

In another case in which a union complained that a company's finger-scanning system constituted an interference with its members' privacy in part because it might be subject to misuse, the Privacy Commissioner noted the company's argument that "unauthorised tampering with the system would not be possible as the system used passwords and only authorised users would be able to gain access. The number of authorised users would be strictly limited." The Privacy Commissioner formed the provisional view that, in this case, the company had reasonable safeguards in place.[403]

Similarly, in the case of a system using RFID tags to collect personal information, whether or not security safeguards in place are reasonable will depend on various factors including what information is stored on the tag (e.g. whether it is personal information or not) and in the database, and the safeguards in place. Some safeguards which have been suggested in the context of RFID applications include restricting access to databases to authorised users only, requiring passwords, requiring that tags be "killed" or deactivated, employing encryption on information conveyed from tags to readers and utilizing shields or other devices to prevent collection from a tag.

Importantly, whether or not security safeguards are reasonable under the circumstances is only one part of an individual's claim of interference with his or her privacy. If the safeguards were not reasonable then a breach of Principle 5 could be found, but Section 66 of the Privacy Act still requires that the breach of the principle result in adverse consequences for the individual. If a database is breached and personal information contained in that database is disclosed as a result, what is the harm that flows from that disclosure? Does the individual have to first be a victim of identity theft based on the improperly disclosed information?

Principle 8: Accuracy of Personal Information to be Checked Before Use

Principle 8 furthers trust in the regime and supports privacy by providing that an agency that holds personal information shall not use the information without taking reasonable steps to ensure that it is accurate, up to date, complete, relevant and not misleading.[404] Consumers can certainly better trust a system if it is using accurate information. This is important to a system that uses RFID technology to collect personal information since people cannot see the information that is being collected and often cannot see the information contained in the database without exercising their access rights under Principle 6.

In the case of an RFID system, what steps must be taken to ensure accuracy and

[401] Case Note 6983 [1998] NZPrivCmr 8 (1 April 1998)
[402] Case Note 28351 [2003] NZPrivCmr 22 (1 September 2003)
[403] Case Note 33623 [2003] NZPrivCmr 5 (1 February 2003)
[404] Privacy Act 1993, s 6

completeness under the principle? Whether steps taken are reasonable will depend in part on the proposed use of the information and the potential for adverse consequences for the individual if the information is inaccurate. For example, if there is a theft in a restricted facility at the weekend, an employer might want to check to see which employees used their RFID-enabled identification card to enter the building during the particular timeframe in question. However, the system should not assume that employee Smith entered the facility just because his card was used at the entrance door; someone else could have used his card to gain access. In this case, because Smith faces being charged with a crime, it would be reasonable to expect the employer to verify that Smith did indeed access the facility. The employer could do this by checking the video surveillance system, if one is in place, or checking whether Smith had reported his identification card lost or stolen.

Sectoral Approach

Several general laws seek to build consumer confidence in the system. Like New Zealand's Privacy Act, a recently-enacted California law requires reasonable security protections over personal information. The statute requires businesses that own or license personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, in order to protect the personal information from unauthorised access, destruction, use, modification or disclosure.[405] The statute does not apply to financial institutions and health care providers who must meet similar requirements under other statutory provisions.[406] The statute defines "personal information" in a more limited manner, however, defining the term to mean an individual's first name or initial and last name in combination with any one or more of the following, when either is not encrypted or redacted: (1) social security number, (2) driver's license number, (3) account number, credit or debit card number, in combination with any code or password, and (4) medical information.[407] This definition is not only narrower than the definition of personal information in the Privacy Act but it is also narrower than other definitions of the same term contained in other California statutes.[408] California law does not contain one comprehensive definition of personal information.

Unlike New Zealand, at this point in time there is little guidance in California concerning what "reasonable security procedures and practices appropriate to the nature of the information" means. The legislative history of the measure indicates that it was drafted to permit businesses to determine, using their own judgment, appropriate levels of security, relying on the "reasonableness" standard well established in tort law. Enforcement of the statute might be of question. Although an individual would not necessarily need to show harm in order to show a violation under the statute, relief under the specific statute might be difficult to obtain.[409] In order to bring an action under California's Unfair Competition Law, an individual would need to have suffered injury in fact and lost money or property as a result of the unfair competition, although public prosecutors would be able to bring an action.[410]

[405] California Civil Code Section 1798.81.5(b)
[406] California Civil Code Section 1798.81.5(e)
[407] California Civil Code Section 1798.81.5(d)(1)
[408] See, e.g., California Civil Code Sections 1798.3(a) and 1798.80
[409] California Civil Code Section 1798.84
[410] California Business and Professions Code Section 17204

In 2002, California was the first state in the U.S. to pass a data breach law requiring private businesses and public agencies to notify California residents if their personal information held by the company is breached.[411] The law defines "breach" to mean the unauthorised acquisition of computerised data that compromises the security, confidentiality or integrity of personal information.[412] The definition of "personal information," which is much more limited than under the Privacy Act, is substantially similar to the same definition contained in the reasonable security procedures statute described above.[413] Like the reasonable security procedures statute, relief under the security breach statute may also be of question.[414]

At the time of this writing at least 23 states have passed security breach statutes,[415] and the U.S. Congress is considering a national data breach law. Although a recent breach involving the personal information of 28.6 million U.S. veterans[416] has highlighted the issue and may have helped spur congressional action, it is not clear that a national law will be passed before the Congress adjourns for the year in October. In addition, it is not yet clear what the national law might say and whether its standards might be lower than those contained in state laws. For example, California law requires that if there is a security breach in the data, then notice must be given. At least one proposal discussed at the national level, however, would require notice only if the security breach might result in identity theft. Several of the national proposals also contain pre-emption language which would override stricter state laws.

With respect to RFID in particular, Senate Bill 1834 (Bowen) also sought to build consumer trust and foster privacy by requiring that a person or entity using RFID technology to collect personally identifiable information take reasonable measures to ensure that any individual data collected is transmitted and stored in a secure manner.[417] The bill also would have restricted access to the data to those individuals needed to operate and maintain the RFID system.[418] These provisions were later deleted from the bill.

Self-Regulation

Several guidelines or "Best Practices" dealing with RFID have recently been introduced which could help to further consumer confidence. Most significantly, the notice provisions contained in GS1 New Zealand's 'EPC/RFID Consumer Protection Code of Practice' and the CDT guidelines described above could help to gain the trust of consumers by providing transparency in the system. The CDT guidelines contain

[411] Ironically, consumers in the U.S. may be more distrustful of businesses' ability to protect their personal information in part because of the recent press surrounding the various data breaches, many of which were made public because of California's data breach law. I chose to include these statutory provisions under the "Trust" criterion however, because data breach laws can help build trust if consumers trust that a company will tell them when something has gone wrong so that they can take protective action.
[412] California Civil Code Sections 1798.29 and 1798.82
[413] Id.
[414] California Civil Code Section 1798.84
[415] Privacy Rights Clearinghouse (n.d.)
[416] Id.
[417] Senate Bill 1834 (Bowen), as introduced
[418] Id.

provisions relating to security which could arguably help to engender trust in the system if followed. They provide that companies should:

1) Exercise reasonable and appropriate efforts to secure RFID tags, readers and any linked information from unauthorised reading, logging and tracking. In addition, companies should exercise reasonable and appropriate efforts to secure the linked information from unauthorised access, loss or tampering.

2) Establish and maintain an information security programme in keeping with industry standards, appropriate to the amount and sensitivity of the information stored on their system. The programme should include processes to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of linked information, and address those risks.

3) To the extent practicable, minimise the information stored on RFID tags themselves in order to enhance the security of information that may be transmitted between tags and reader.[419]

Although a self-regulatory scheme has the potential to engender consumer confidence and build privacy, many consumers, particularly Americans, do not trust industry to regulate itself. In the United States consumers have witnessed too many instances in which businesses have not sufficiently protected their personal information. For example in February 2005 U.S. data broker ChoicePoint acknowledged a security breach in which the company had disclosed the personal and financial information of almost 163,000 consumers to identity thieves posing as legitimate businesses.[420] At least 800 cases of identity theft resulted from the security breach.[421]

A recent study of New Zealanders found that some felt similarly distrustful of the private sector. The study, which focused on trust in government with respect to information privacy, found that more respondents trusted government organizations than private organizations to properly handle and adequately protect their personal information.[422]

This general distrust of industry may carry over to RFID use as well. Although some consumers may embrace the convenience of new RFID applications such as the ExxonMobil Speedpass or the Chase Bank "Blink" card, others are likely to be more reluctant about the use of the technology in everyday products such as cereal boxes. Part of this may be a lack of understanding about how the technology works and how a system functions, but in other cases industry itself may be reluctant to divulge uses of the technology. In the Levi Strauss example noted earlier, the U.S. store testing the technology in removable hang tags has not yet identified itself, possibly for fear of a backlash like that encountered when consumers threatened a boycott of Benetton clothing after the electronics company, Phillips, announced that it would ship 15 million RFID tags to the Italian retailer.[423]

---

[419] Center for Democracy and Technology (1 May 2006)
[420] U.S. Federal Trade Commission (26 January 2006)
[421] Id.
[422] Reilly (January 2006), p.28
[423] Heisenberg (2005), p.151

Trust Conclusion

All three approaches to privacy protection have the ability to promote privacy and build consumer trust, although self-regulation by itself faces the most hurdles in this regard. In the United States consumer distrust of businesses' ability to safeguard personal information is considerable and, in the case of new applications of a technology with which many people are not familiar, reliance on industry to regulate itself contains too many deficiencies to achieve a proper comfort level. Sectoral regulation, however, could certainly help to engender consumer trust, although how well the approach furthers that goal depends of course on what the regulation requires. For example, consumers are not likely to further trust the systems in place if the U.S. Congress approves a national data breach law riddled with loopholes. Also, enforcement and remedies issues may be of concern with respect to the above-noted Civil Code sections.

Openness *– An entity that collects personal information from an individual will be open about the collection*

Openness helps to create trust and further privacy because entities that collect personal information from individuals openly and transparently are more likely to be trusted. Openness includes important issues of transparency such as: (1) the fact that personal information is being collected, (2) what information is being collected, (3) the purpose of the collection, and (4) who is able to see the information and what will eventually happen to it. Openness also relates to issues of access; a system is more open and transparent when individuals can see what information it has about them.

Openness is a particularly important criterion in the case of RFID technology because of the possibility of covert collection. Communications between an RFID tag and a reader are contact-less; the tag and reader do not need to be touching in order to communicate. The read range can be anywhere from just inches to over 100 feet or more, depending on the type and strength of the tag. As a result, it is possible that an RFID-embedded tag could be read from a measurable distance away without the tag holder's knowledge. In addition, as the technology advances the size of RFID tags is decreasing. For example, tiny RFID chips which can be embedded in a piece of paper are being developed. Privacy advocates worry that tags will become so small that consumers will not necessarily even know that they are carrying items containing them. Readers can also be unseen, their presence undetectable.[424] Another concern with respect to openness and RFID technology is the fact that even if a person knows that his or her RFID tag is being scanned by a reader, he or she does not necessarily know what information is actually being conveyed.[425]

Comprehensive Approach

If the goal is that entities are open about their collection of personal information, then a comprehensive approach such as New Zealand's Privacy Act would certainly appear

[424] Organisation for Economic Co-operation and Development (27 February 2006), p.21
[425] U.S. Department of Homeland Security (May 2006), p.8

to further that goal.[426] The Act contains a number of provisions relating to openness.

Principle 1: Purpose of Collection of Personal Information

Principle 1 provides that an agency may not collect personal information unless the collection is for a lawful purpose connected with a function or activity of the agency and the collection is necessary for that purpose.[427] The Act thus requires an agency to define the purpose of the collection.[428] For example, with respect to RFID, an agency might define the purpose of collecting personal information using RFID-embedded employee identification badges to be controlling access to facilities. The agency would then have to determine whether the collection of the personal information was necessary for that purpose.[429]

Information Privacy Principle 3: Collection of Information from Subject

Under Principle 3(1), the identified purpose of collection and other specified information such as the fact that personal information is being collected, the intended recipients of the information and the rights of access and correction must be conveyed to the individual when the agency collects personal information directly from him or her.[430] In the case of collection of personal information using an RFID tag, Principle 3 would appear to prohibit covert collection because notice of the fact that information is being collected is required. The question then becomes how will consumers be notified? One answer is through signage at the point of collection although some have questioned whether this would be sufficient.[431] It is also not clear whether a privacy policy posted on an agency's website notifying consumers of the collection of personal information using RFID would be adequate. Arguably, it would not as the notification is so distant from the point of collection.

Although it contains other important notification requirements, Principle 3 does not require that an agency notify a consumer *what* information is being collected. This is important in the context of RFID because the consumer cannot see what information is actually being conveyed between a tag and a reader.

---

[426] This finding, along with many others in this report, presumes compliance with the statutory requirements. The research did not analyse whether agencies are properly complying with the Privacy Act (a topic of study for another day), and it is the author's hope that this is not an improbable assumption and that agencies are indeed complying with the Act.

[427] Privacy Act 1993, s 6

[428] The requirement that an agency "self-define" its purpose has been criticized by some who argue that it has the potential to allow agencies to construct information-sharing practices that can lead to privacy adverse outcomes without violating the Privacy Act. (Interview with John Edwards, Barrister & Solicitor, Wellington, 2 May 2006)

[429] According to Professor Roth, interpretations of the necessity test in New Zealand have not subjected it to a particularly high threshold, and the standard does not appear to be whether there might be less intrusive means to collect the personal information. (Roth, *Privacy Law and Practice*, para 1006.6A) See, also para 1006.6A for Privacy Commissioner case notes illustrating "the apparent laxness of the necessity test."

[430] Privacy Act 1993, s 6. While Principle 3(1) provides that the agency must take reasonable steps to "ensure that the individual concerned is aware of" the specified items of information, for purposes of this discussion the term "notice" is used to encapsulate this concept.

[431] See Heisenberg (2005), p.152 in which the author writes: "It is a legal question, however, if simply posting signs saying 'In this store we use RFID to monitor your shopping behavior to better serve your shopping needs' would suffice."

Principle 3(2) provides that such notice is required before the information is collected, or if that is not practicable, then as soon as practicable after the information is collected. Although a strict reading of this provision could be read to require that notice or signage is required at each RFID reader, it is not likely that such a reading would be a correct one as Principle 3(2) requires that notice be provided *before* the information is collected, but not necessarily *at the time* of the collection.[432]

Under Principle 3(3), an agency is not required to provide the described notice if it has already given notice to the individual when collecting "the same information or information of the same kind on a recent previous occasion." As a result, an agency could be said to be in compliance provided that the individual was previously made aware of the collection of information (perhaps the first time that the RFID-embedded card was used or when it was issued).

Exemptions under Principle 3

Principle 3 contains several exemptions which could potentially be problematic, or at least raise questions, with respect to RFID use. For example Principle 3(4)(a) provides that an agency does not need to comply with Principle 3(1) if it believes, on reasonable grounds, that the individual concerned has authorised non-compliance. In the case of an employee's RFID-embedded identification badge, it is likely to be argued that an employee authorised the use of the badge as a condition of employment or part of a contract negotiation.[433] This could raise issues of choice as the employee may not have had a true choice in authorising non-compliance owing to the power relationship between the employer and employee. Importantly, the Privacy Act provides that authorisation must be obtained from the individual concerned in order for this particular exemption to apply. As discussed earlier, authorisation is stronger than consent, cannot be implied and requires a positive act.[434]

Principle 3(4)(e) provides that non-compliance is permitted if compliance is "not reasonably practicable in the circumstances of the particular case."[435] Depending on the particular circumstances of the RFID application, it is possible that this exception might be triggered. For example, if the technology is being used to monitor an individual's behaviour and it would not be practicable to alert the individual to the monitoring because it was intended to detect unlawful behaviour.

Harm Requirement for Violation of Principle 3

One issue that may arise with respect to RFID use and the provisions furthering openness is the requirement that there be harm, or adverse consequences, for a breach of Principle 3 concerning notice.

Under Section 66 of the Privacy Act, an interference with privacy requires that the

[432] See, e.g., *AB v Accident Compensation Corporation* (24 December 2002) HRRT 40/02, Decision No 17/02, para 37 in which the Human Rights Review Tribunal considered a substantially similar provision in the Health Information Privacy Code 1994
[433] Roth (February 2006), p.12
[434] Roth, *Privacy Law and Practice*, para 1006.11A
[435] Privacy Act 1993, s 6

action meet one of the following criteria:

1) It has caused, or may cause, loss, detriment, damage or injury to the individual;

2) It has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or

3) It has resulted in, or may result in, significant humiliation, significant loss of dignity or significant injury to the individual's feelings.[436]

In the case of RFID use and the requirement of Principle 3 that a consumer be notified of collection, it is potentially questionable that there is harm when a consumer's RFID tag is scanned without notice. For example, if a consumer is carrying an RFID-embedded handbag which is, unbeknownst to the consumer, scanned by a reader when he or she walks into a store, what are the actual or possible adverse consequences that flow from such an incident?

Furthermore, there must be a clear causal link between the action and the harm or adverse consequences before damages may be awarded. In *Hamilton v the Deanery*, the Human Rights Review Tribunal awarded the plaintiff the highest amount of compensation ever awarded for humiliation, loss of dignity and injury to feelings ($40,000), but not before first declining to award her the $200,000 she had sought because the Tribunal was "not satisfied that any sufficient connection between the sums claimed and the act of interference with privacy has been established."[437]

Despite these points it is important to note that a breach of Principle 3 (or any of the Principles) can still trigger the Privacy Commissioner's other powers and functions even though there has been no harm or adverse consequence to the individual. For example the Privacy Commissioner could inquire into a practice if it appears to her that the privacy of the individual is being, or may be, infringed upon, irrespective of whether the individual was harmed.[438]

Principles 6 and 7: Access to, and Correction of, Personal Information

The Privacy Act contains other provisions which also further the goal of openness and help to build trust and protect privacy. For example Principles 6 and 7 provide that an individual is entitled to access his or her personal information held by an agency and request correction of that information. The access rights under Principle 6(1) apply when "an agency holds personal information in such a way that it can *readily be retrieved.*"[439] In the case of RFID use that is linked to personal information, it is likely that such information would be contained in a database and therefore readily retrievable, but perhaps this may not be the case.[440]

[436] Privacy Act 1993, s 66(1)(b)
[437] *Hamilton v the Deanery* (29 August 2003) HRRT 28/03, Decision No 36/02, para 44
[438] Privacy Act 1993, s 13(1)(m)
[439] Privacy Act 1993, s 6
[440] Professor Roth has argued that in the employment context, "[i]t will be likely to prove cumbersome for employers to supply this information upon request to employees." (Roth (February 2006), p.13)

Whether or not such access in the context of RFID is meaningful could be of question. For example, if a consumer's RFID-embedded handbag is scanned by a reader at various times over an extended time period it could be difficult for the consumer to remember where she had been during this timeframe. Because an RFID system logs when and where a particular tag has been, it may require an individual who is highly cognizant of his or her whereabouts to make sense of a listing of their information. Despite this, access is still important as it helps individuals to know what information, such as their whereabouts, the agency holds about them.

Principle 11: Limits on Disclosure of Personal Information

Principle 11 of the Privacy Act prohibits an agency that holds personal information from disclosing the information to a person or body or agency except in certain circumstances such as when the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purpose.[441] Such a requirement arguably furthers openness and therefore builds trust because as long as an agency notifies individuals of the purpose of the collection and tells them who they disclose to, they can disclose without fear of violating the Act.

Sectoral Approach

Sectoral approaches can further the goal of requiring entities to be open about their collection of personal information, depending on how they are drafted.

Legislative Proposals

In 2004 Senate Bill 1834 (Bowen), as introduced, would have provided an individual with the right to access his or her personally identifiable information collected through an RFID system.[442] The bill would also have permitted an individual to make corrections to that information. These provisions were deleted from the bill which later failed passage in the Assembly Business and Professions Committee.

Another proposed measure, Senate Bill 682 (Simitian), also contained a number of provisions furthering the goal of openness. For example the bill would have prohibited government identification documents using RFID to transmit or enable the remote reading of any personal information other than a unique personal identifier number thus helping an individual to know what information is being transmitted.[443]

The proposed bill also would have required the public agency issuing the RFID-tagged identification document to tell an individual in writing the following:

1) That the identification document can transmit a unique personal identifier number or enable the number to be read remotely without the individual's knowledge;

2) The location of all readers used or intended to be used by the public agency to read the identification document. Alternatively, the public agency can satisfy

[441] Privacy Act 1993, s 6
[442] Senate Bill 1834 (Bowen), as introduced
[443] Senate Bill 682 (Simitian), as amended 15 August 2005

this requirement by providing a general description of the locations where readers are used (e.g. all building entrances or exits) and posting a sign at each reader's actual location notifying individuals of the collection of information; and

3) Any information that is being collected or stored regarding the individual in a database at the time the identification document is being read such as time and location.[444]

The bill would also have required the public agency to provide annual notice to individuals concerning any changes in the location of readers or the information collected or stored in the database.[445]

There have also been several legislative proposals to require transparency of RFID use in the retail context. For example, in 2004 U.S. Representative Kleczka introduced H.R. 4673, the "Opt Out of ID Chips Act", which would have required warning labels on consumer products containing RFID.[446] Under the proposal, the warning labels must state that the product contains an RFID tag and the tag can be used to track the product and transmit unique identification information to a reader both before and after purchase. The label must also notify the consumer that he or she may have the device removed from the product or permanently disabled at the time of purchase. No action was taken on the bill which was referred to the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce.

California Information Practices Act of 1977

The California Information Practices Act contains provisions similar to Principle 3 with respect to notification, although the Act is much more limited in scope, applying only to state agencies.[447] Like Principle 3, under the Information Practices Act state agencies must provide notice concerning the purpose of the collection, the name of the agency requesting the information, the statutory, regulatory or executive authority which authorises the collection, whether submission is mandatory or voluntary and the consequences of not providing the requested information. The Information Practices Act is narrower with respect to when the notification must be provided, however: it requires state agencies to provide the specified notice *on any form* used to collect personal information.[448] Clearly this type of collection reflects its time and does not envision collection using technologies like RFID.

Self-Regulation

Self-regulation can further the goal of openness depending on the regulation. The GS1 New Zealand and CDT guidelines each contain some notice requirement, aiming to make RFID use more transparent to consumers, thereby encouraging confidence.

---

[444] Id.
[445] Id.
[446] Copies of all U.S. Congressional bills may be obtained from http://thomas.loc.gov
[447] California Civil Code Section 1798 et seq.
[448] California Civil Code Section 1798.17

GS1 New Zealand's "EPC/RFID Consumer Protection Code of Practice" requires some notice to consumers of the retail use of RFID.[449] The voluntary code applies only to retailers who have adopted it and only to items containing an RFID tag which is used for the purposes of "customer service".[450] The GS1 NZ code requires that retailers provide at least 28 calendar days' notice to consumers of the pending activation of RFID technology either in the form of signage or other written material provided to consumers when they enter the store.[451] While the GS1 NZ code does not specify what information must be provided in the notice, it is presumed that the notice requirements of Principle 3 of the Privacy Act would apply,[452] and the code also states that retailers should recognise their obligations under the Privacy Act.[453]

The Center for Democracy and Technology's (CDT) best practice guidelines for the use of RFID in the commercial and private sector are intended to cover instances where information is collected using RFID and then linked to personal information.[454] The voluntary guidelines provide that consumers be given clear, conspicuous and concise notice specifying the presence of an RFID tag, the purposes for which the information is being collected, how the information will be used, and whether the information may be used for additional or subsequent uses, such as marketing.[455] The CDT guidelines suggest that the notice be given prior to the completion of the transaction whenever practicable and that individual readers be identified.[456] The guidelines provide more enhanced notice requirements than the GS1 New Zealand guidelines, which presume that Principle 3 of the Privacy Act will apply. This important distinction, however, reflects their larger frameworks. The CDT guidelines were drafted for use in the United States where there is no comprehensive privacy statute providing a baseline floor of protections such as the Privacy Act 1993.

Also of note, the Information and Privacy Commissioner of Ontario recently issued voluntary "Privacy Guidelines for RFID Systems" which aim to serve as "best practices guidance."[457] The guidelines, which are based on "fair information practices," aim to preserve openness by providing that organizations "should not collect or link an RFID tag to personally identifiable information indiscriminately or covertly, or through deception or misleading purposes."[458]

Openness Conclusion

All three approaches to privacy protection can further the goal of openness and encourage entities to be open about their collection of personal information, thus building trust and promoting privacy. In the case of sectoral legislation and self-regulation however, how well the approaches further the goal depends on what is required. Furthermore, both of these approaches suffer from significant failings. In the

[449] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[450] Id.
[451] Id.
[452] Interview with Gary Hartley, Manager for Strategic Initiatives, GS1 New Zealand (Wellington, 5 May 2006)
[453] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[454] Center for Democracy and Technology (1 May 2006)
[455] Id.
[456] Id.
[457] Information and Privacy Commissioner/Ontario (June 2006)
[458] Id.

case of the sectoral approach, none of the legislative proposals described have been signed into law, leaving a gap in practice and little to protect people in the meantime. While California's Information Practices Act provides some protections, it is far more limited in its scope and does not appear to be sufficiently technology-neutral. With respect to self-regulation, the codes and guidelines proposed are all voluntary, which raises the question of who will follow them and how they will be enforced.

With respect to the comprehensive approach, certainly one of the underlying premises of the Privacy Act is the notion of openness and transparency and the information privacy principles reflect that. Despite its important notification requirements, Principle 3 does not require that a person be told *what* information is being collected. This is important in the context of RFID because the consumer cannot see what information is actually being conveyed between a tag and a reader. There may also be some question as to how the exemptions to Principle 3 might apply to RFID technology and how the harm requirement under Section 66 might be met in this regard. Additionally, there may be some question as to whether access in the context of RFID might be fully meaningful, although it is still important as it helps individuals to know what information the agency holds about them.

Choice *– Individuals will have a choice as to whether to disclose their personal information*

As used in this report, "choice" means the ability to decide whether to disclose personal information at the time of collection. This is distinguished from "control" which, for purposes of this report, means having power over your personal information once it has been collected. As discussed earlier, choice is fragile and, in many situations, individuals find themselves without choice or without a real choice. As a result, choice can often feel "coerced." Ideally, having a choice as to whether or not to disclose personal information most achieves trust and protects privacy because individuals are more likely to trust those who hold their information if they made the choice to disclose.

Many of the current uses of RFID technology which link to personal information allow the consumer the choice to decide whether or not to take part in the system. Chase Bank's "Blink" card, the ExxonMobil Speedpass, and the use of RFID-tagged wristbands at amusement parks are all voluntary consumer uses. Some might even argue that the use of RFID-tagged identification badges in the employment context is voluntary since an individual does not *have* to take, or keep, a particular job, although this ignores obvious potential power imbalances.

As RFID use becomes ubiquitous and the EPCglobal Network and item-level tagging becomes more of a reality, however, consumers may no longer have a choice as to whether a product they purchase contains an RFID tag. At this point in time the EPC number is not linked to personal information although there are concerns that it could be at the time of purchase. EPCglobal has indicated however that any such linkage would only be with the consumer's permission.[459]

[459] E-mail correspondence from Elizabeth Board, Executive Director, EPCglobal Public Policy Steering Committee (23 May 2006)

With respect to human implantation of RFID tags, it would seem that most use of this particular application is currently voluntary. Patients in the United States are deciding to implant themselves so that their medical records are easily accessible in hospitals that have readers. Bar patrons in Spain have microchips implanted in order to gain access to VIP areas and run electronic tabs. The potential for increased use of human-implanted RFID tags in the employment context could be a disturbing phenomenon however, as the question arises as to whether employees truly have choice.

Furthermore, the Chairman of the Board of VeriChip Corporation recently proposed implanting RFID microchips in immigrant and guest workers.[460] In an interview on national television Scott Silverman was quoted responding "to the Bush administration's call to know 'who is in our country and why they are here'"[461] and proposed "using VeriChip RFID implants to register workers at the border, and then verify their identities in the workplace."[462] Silverman added, "[w]e have talked to many people in Washington about using it."[463] Shortly after this development Wisconsin became the first state in the United States to ban the forcible implantation of RFID microchips into humans.[464]

Comprehensive Approach

The Privacy Act 1993 recognises the limitations of choice and provides individuals with other rights instead such as notice that personal information is being collected (Principle 3) and control over the information (Principles 6 and 7). The Act also mentions choice in other ways. For example, under Principle 3 if the collection of personal information is authorised or required by or under law, agencies must ensure that the individual is aware of whether or not providing the information is voluntary or mandatory.[465] The agency must also tell the individual the consequences, if any, if all or any part of the requested information is not provided.[466]

While the Privacy Act does not require that people be offered the choice as to whether or not they provide their personal information, the Act does contain safeguards should that lack of choice become problematic. For example, if an agency required individuals to be implanted with an RFID microchip that collection could be deemed to be a violation of Principle 4 which prohibits agencies from collecting personal information by means that, in the circumstances, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.[467] Although there are no cases directly on point the Privacy Commissioner discussed the issue of microchipping in general in a recent speech, stating:

> To return to the question I posed earlier: should all of us be microchipped with our medical history? Clearly there are advantages and disadvantages. If this was a real "modest proposal" – and remember it is in some eyes just an

[460] Christensen, Bill (1 June 2005)
[461] Id.
[462] Id.
[463] Id.
[464] Songini, Marc, *Computerworld*, 12 June 2006
[465] Privacy Act 1993, s 6
[466] Id.
[467] Certainly, forced implantation by a public agency could also raise issues under the New Zealand Bill of Rights Act, an issue beyond the scope of this report

> improved version of a Medic Alert bracelet – my office would ask some questions: Will there be a real choice? Will individuals have any real control? How will the information be kept up to date and accurate? Who will be able to access it? Will it work? Is there a better or cheaper way? How could it be misused? What protections are there? Is it really important and effective - will its advantages outweigh disadvantages?[468]

With respect to a related issue, the Privacy Commissioner has formed the view that a company's finger-scanning system was not a violation of Principle 4 based on the circumstances of the case.[469] The company had complied with Principles 1 and 3 and the Privacy Commissioner found that there was insufficient evidence "that the fingerscanning would be unfair, or intrude to an unreasonable extent on the personal affairs of the employees."[470]

In addition the Privacy Commissioner has several powers available to her that could help to ameliorate concerns regarding the forced implantation hypothetical. The Privacy Act provides that the Privacy Commissioner may "inquire generally into any matter, including any . . . practice or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby."[471] This ability to look into infringements, or possible infringements, on privacy would appear to be broader than the language required to show an interference with privacy under Section 66 of the Act and also does not require that a complaint first be made.

The Privacy Act also permits the Privacy Commissioner to "undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring."[472] The Privacy Commissioner can also report directly to the Prime Minister on "any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual"[473] as well as "any other matter relating to privacy that, in the Commissioner's opinion, should be drawn to the Prime Minister's attention."[474] All of these provisions are arguably safeguards should the lack of choice become problematic, whether it is the forced implantation of RFID chips or the ubiquitous use of item-level tagging linked to personal information.

Sectoral Approach

Depending on the proposal a sectoral approach can certainly promote choice and thereby help to protect privacy and foster trust. Several proposals have been introduced to give consumers choice regarding the collection of personal information using RFID tags. For example, Senate Bill 1834 (Bowen) of 2004 would have

[468] Shroff, Marie (11 August 2004)
[469] Case Note 33623 [2003] NZPrivCmr 5 (1 February 2003)
[470] Id.
[471] Privacy Act 1993, s 13(1)(m)
[472] Privacy Act 1993, s 13(1)(n)
[473] Privacy Act 1993, s 13(1)(p)
[474] Privacy Act 1993, s 13(1)(r)

required an entity using an RFID system to first obtain written consent from an individual before his or her personal information could be attached to or stored with data collected via the RFID system.[475] This provision was later deleted.

Another proposed measure, Senate Bill 682 (Simitian) of 2005, contained a number of provisions furthering choice with respect to use by public agencies. The bill would have required identification documents containing RFID tags to implement at least one of several specified safeguards in order "to ensure that the holder of the identification document affirmatively consents to each reading of the identification document," including the use of a shield device to prevent any communication between the tag and reader.[476] The bill would have also required an entity issuing an RFID-enabled identification document to tell an individual receiving the document that countermeasures such as shield devices can be used to help "control the risk that his or her unique personal identifier number will be broadcast or read remotely without his or her knowledge."[477]

Self-Regulation

With regard to choice, GS1 New Zealand's "EPC/RFID Consumer Protection Code of Practice" does not require retailers to provide consumers with the choice not to provide their personal information, and it does not require that consumers be given the choice to disable the tag. Instead, the Code states that consumers "shall be advised of the retailers' policy with respect to retaining, disabling or removing RFID tags from the products they purchase. Consumers shall be advised of this policy on entering the store."[478] On the one hand, such information could be helpful to consumers who will learn the retailer's policy. On the other hand, the retailer's policy could simply be that consumers have *no* choice with respect to retaining, disabling or removing RFID tags, and there would be no violation of the GS1 NZ Code.

The CDT best practice guidelines contain similar language, providing that the consumer "should be informed in a clear, conspicuous and concise manner when there is an option to remove, de-activate, or destroy a tag and, when there is, how that option may be exercised."[479] The guidelines further provide that if a consumer exercises the choice to remove, deactivate or destroy a tag, his or her ability to return an item or benefit from a warranty or the protections of local law should not be compromised.[480]

Under the CDT guidelines, consumers have choice regarding the use of their personal information "collected on the tag or associated with the RFID number" depending on how the linked personal information is to be used. If it is used "solely to enable the functioning of the device the consumer has purchased or delivery of the service for which the consumer has contracted or to facilitate completion of the commercial business's transaction with the consumer," then the consumer's consent or choice

[475] Senate Bill 1834 (Bowen), as introduced
[476] Senate Bill 682 (Simitian), as amended 15 August 2005
[477] Id.
[478] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[479] Center for Democracy and Technology (1 May 2006)
[480] Id.

about the use of his or her personal information does not need to be solicited.[481] If the linked information is instead used for other purposes (e.g. marketing or sharing personal information with a third party), then the guidelines recommend that the consumer be "notified and given the opportunity to consent to such uses."[482]

It should be noted that the GS1 New Zealand code also contains a provision concerning the collection of information from other RFID tags. Specifically, the provision states that "[r]etailers shall not intentionally record information from RFID tags obtained by consumers from other businesses without the consumers' consent."[483]

Neither of these efforts to self-regulate truly offer choice in the sense that they require users of RFID systems to provide consumers with the ability to say no to the collection of their personal information. Nothing in these regimes requires agencies to provide consumers with a choice; the agencies just have to let them know what their choices are, if they have any. On the other hand, self-regulation efforts could be written to provide choice and therefore better help to promote confidence. Also, as noted earlier, both guidelines are voluntary and enforcement and oversight may thus be an issue.

The voluntary RFID guidelines issued by the Information and Privacy Commissioner of Ontario are based on "fair information practices" and contain several provisions regarding choice. For example, they provide that organizations should seek individual consent before collecting, using or disclosing personal information linked to an RFID tag.[484] The guidelines specify that in order to be valid, "consent must be based upon an informed understanding of the existence, type, locations, purposes and actions of the RFID technologies and information used by the organization."[485] Under the guidelines consumers should be able to remove, disable or deactivate item-level RFID tags, without penalty.[486] Finally, with respect to choice, the guidelines provide that organizations "must obtain additional individual consent to use, disclose or link to personal information for any new purposes."[487]

Choice Conclusion

With respect to promoting choice, the sectoral approach would appear to be the best suited as it can most robustly provide consumers with choice by, for example, requiring that RFID users first obtain written consent before collecting personal information. On the other hand, proposals can be drafted to be more limited. For example Senate Bill 682 relates only to RFID use by government agencies; it does not apply to private sector use of RFID systems.

While the Privacy Act does not specifically provide such consumer choice, its comprehensive nature means that it is important to look to other areas of the Act for

---

[481] Id.
[482] Id.
[483] *EPC/RFID Consumer Protection Code of Practice* (March 2005)
[484] Information and Privacy Commissioner/Ontario (June 2006)
[485] Id.
[486] Id.
[487] Id.

safeguards if the lack of choice becomes problematic. As noted, the Privacy Commissioner has other functions which she can exercise in her discretion, including inquiring into practices if it appears that individuals' privacy is being infringed upon, monitoring the development of technologies for privacy impacts or reporting directly to the Prime Minister on any privacy matter. Furthermore, the Privacy Act arguably recognises the limitations of choice and instead provides individuals with other rights.

Neither of the self-regulation efforts appear to truly offer choice in that they do not require users of RFID systems to provide consumers with the ability to say no to the collection of their personal information. On the other hand, self-regulation could be drafted to provide choice, thus better furthering confidence. While the sectoral approach may be best suited to help provide consumer choice, it is of course worth noting that none of the sectoral proposals described above has yet been enacted and become law.

Control *– Individuals will have control over what happens to their personal information and who is able to access it*

As previously noted, "control" means having power over your personal information once it has been collected. This is distinguished from "choice" which, for purposes of this report, means the ability to decide whether to disclose personal information at the time of collection. A privacy regime that gives individuals control over their personal information helps to build trust and confidence in those who hold the information.

Control has particular meaning with respect to RFID technology. RFID databases have the potential to collect vast amounts of personal information if linked to identifiable individuals. For example, if a consumer is linked to a pair of jeans at the time of purchase and the RFID tag is not deactivated, then every time that she wears the jeans and comes within the read range of a scanner that can read the tag on her jeans, her location and the time and date could be recorded. In considering control issues, the following questions are relevant: What power do I have over my information once it has been collected? Who gets to see that information and what later happens to it? How long is the information retained? Is it eventually destroyed?

Comprehensive Approach

The Privacy Act contains several provisions which promote an individual's control over his or her own personal information, a hallmark of human rights legislation.

Principle 3: Collection of Information from Subject

Principle 3 provides for notification to a consumer concerning the fact that personal information is being collected, the intended recipients of the information and the rights of access and correction. Such notification gives individuals some control over their information because they know how the information will be used and who will see it. As previously mentioned, Principle 3 contains several exemptions which could potentially be problematic, or at least raise questions, with respect to RFID use. These include Principle 3(4)(a) which provides that an agency does not need to comply if it believes, on reasonable grounds, that the individual concerned has authorised non-compliance, and Principle 3(4)(e) which provides that non-compliance is permitted if

compliance is "not reasonably practicable in the circumstances of the particular case."

Principles 6 and 7: Access to, and Correction of, Personal Information

Principles 6 and 7 strike at the heart of the control issue by providing an individual with the right to access his or her personal information held by an agency and request correction of that information. The right to access personal information applies when the agency "holds personal information in such a way that it can *readily be retrieved.*"[488] The Privacy Act also specifies permissible reasons for refusing access to personal information, including that an agency may refuse an access request if the information requested is not readily retrievable.[489] In the case of RFID use that is linked to personal information, it is likely that such information would be contained in a database and therefore readily retrievable, but whether or not the information would be meaningful could be of question. As noted above, because an RFID system logs when and where a particular tag has been, it may require that individuals be highly cognizant of their whereabouts to understand their information. Furthermore, it is not clear how an individual might correct information contained in an RFID system. For example, if someone else uses another person's RFID-enabled identification card to gain entry to a restricted area, it could be difficult to correct that information.

The Privacy Act contains provisions dealing with situations in which the requested information is contained in a document, specifically providing that the information be made available in a specified manner.[490] The Act also defines the term "document" in a manner that would appear to include RFID technology, providing that the term "means a document in any form; and includes . . . (b) any information recorded or stored by means of any tape-recorder, computer, or other device; and any material subsequently derived from information so recorded or stored."[491]

Interference with an Individual's Privacy: Principles 6 and 7

Harm is not required to prove an interference with privacy on the basis of a violation of Principles 6 or 7.[492] The Privacy Act provides that an action is an interference with an individual's privacy if the agency refuses to make information available in response to an access request or refuses to correct personal information *and* the Privacy Commissioner or the Human Rights Review Tribunal finds that there was no proper basis for that decision.[493] As a result, if an agency claimed that the requested information was not readily retrievable and the Privacy Commissioner or, depending on the case, the Human Rights Review Tribunal, found that there was no proper basis for that decision, then the refusal to provide the information would be deemed to be an interference with the individual's privacy under Section 66(2) of the Privacy Act.

Principle 9 (Agency Not to Keep Personal Information for Longer Than Necessary) and Principle 10 (Limits on Use of Personal Information)

[488] Privacy Act 1993, s 6
[489] Privacy Act 1993, s 29(2)(a)
[490] Privacy Act 1993, s 42(1)
[491] Privacy Act 1993, s 2(1)
[492] *Winter v Jans* (6 April 2004) HC HAM CIV-2003-419-854
[493] Privacy Act 1993, s 66(2)(a) and (b)

Principle 9 provides consumers some measure of control by attempting to ensure that their personal information will not be kept "for longer than is required for the purposes for which the information may lawfully be used."[494] Whether or not a use is lawful will require some consideration of Principle 10 which provides that an "agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose."[495] There are several exemptions to this principle, including if the agency believes, on reasonable grounds, that "the use of the information for that other purpose is authorised by the individual concerned" or that "the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained."[496]

In the case of the collection of personal information using RFID technology, the purpose defined by the agency under Principle 1 will be critical as it will determine how long the agency may hold onto the personal information and whether later uses are permissible under Principle 10. For example, in designing an information-collection system using RFID, an agency could define its purpose as "customer service," a potentially overly broad purpose that can encompass many other uses not necessarily envisioned by the individual whose information is being collected. For instance, some agencies may argue that using personal information collected by RFID technology for marketing purposes is "directly related" to the purpose of customer service and therefore a permissible use under Principle 10.

Sectoral Approach

While at least one sectoral proposal has attempted to promote consumer control for the most part the approach in the United States has been sorely lacking in providing consumers with control over their personal information.

With respect to access and correction rights, Californians have some rights to access, and to request correction of, information about them held by state agencies under the Information Practices Act.[497] In addition, in 2005 a legislative proposal was introduced to require a data broker (a company that compiles data files on consumers and then sells those files to non-affiliated third parties) to disclose to a consumer all information about him or her compiled or maintained by the broker.[498] The bill, which was opposed by the data broker industry, also would have required a data broker to allow an individual the right to request and receive prompt correction of errors in his or her consumer data file.[499] These provisions were deleted from the measure, which now deals with an unrelated privacy issue.[500]

Proposed Senate Bill 1834 (Bowen) of 2004 would have also helped to promote consumer control by requiring an entity using an RFID system to obtain separate written consent from the consumer before any of his or her personal information

[494] Privacy Act 1993, s 6
[495] Id.
[496] Id.
[497] California Civil Code Sections 1798.32, 1798.34 and 1798.35
[498] Senate Bill 550 (Speier), as amended 28 June 2005
[499] Id.
[500] Senate Bill 550 (Speier), as amended 26 June 2006

collected using RFID is shared with a third party.[501] The bill would also have granted individuals the right to access their personal information collected using RFID and the opportunity to make corrections to that information.[502] These provisions were deleted from the bill.

Self-Regulation

GS1 New Zealand's "EPC/RFID Consumer Protection Code of Practice" does not in and of itself contain language regarding consumer control over personal information collected using RFID technology. Instead the code envisions that agencies will comply with the Privacy Act, thus providing control by granting consumers access to, and correction of, their personal information held in the agency's system under Principles 6 and 7.

Unlike the GS1 NZ code, the CDT best practice guidelines cannot rely on the provisions of a comprehensive statute like the Privacy Act 1993 to help give consumers control over their personal information. The CDT guidelines provide consumers with some control when their personal information is to be used for purposes such as marketing by recommending that the consumer be "notified and given the opportunity to consent to such uses."[503] While the guidelines provide that consumers should have "reasonable access" to personal information maintained on the RFID tag itself, they do not specify whether consumers should have access to personal information collected using an RFID tag which is maintained in a database, unless the individual "receives an adverse decision based on linked information about him or herself."[504] They do, however, provide that: "As a general principle, it is *desirable* to provide consumers with, if cost effective and efficient, reasonable access to personally identifiable information, including location information, collected using RFID technology (emphasis added)."[505] It is important to note that this general principle expresses only a "desire" that consumers be provided access whereas other provisions of the CDT guidelines have used stronger language. Furthermore, it is not clear what "reasonable access" means.

Control Conclusion

As described above, the comprehensive approach of the Privacy Act would appear to most fully promote control over personal information collected using RFID and thus best help to foster trust and protect privacy. An individual's control over his or her personal information is one of the significant underpinnings of the Act. As described above, the collection of personal information using RFID has the potential to raise possible issues concerning exemptions to Principle 3, what access and correction rights mean in the context of a log of RFID-collected information, and how Principles 9 and 10 provide protections.

Both the sectoral and some self-regulation approaches appear to have significant failings, as noted above. Under a sectoral approach, Californians in particular have

[501] Senate Bill 1834 (Bowen), as introduced
[502] Id.
[503] Center for Democracy and Technology (1 May 2006)
[504] Id.
[505] Id.

some access rights to their personal information but this right is limited to information held by state agencies. Legislative proposals to extend this right to other industries have so far stalled. Current self-regulatory schemes like the CDT guidelines do not appear to provide consumers with robust control over their collected personal information. They provide only that it is "desirable" to provide consumers with access which should be "reasonable." It is not clear what these terms mean. Self-regulation does not appear to lend itself to consumer control.

Balance *– The privacy protection regime will strike the appropriate balance between an individual's right to privacy and other competing interests*

Without a doubt when it comes to RFID technology, there are certainly many interests competing with privacy. The technology is used to control access to restricted facilities, ensuring security. Physicians can access the medical records of unconscious RFID-chipped patients, helping to provide proper medical care and perhaps save a life. Governments can use the technology to ensure the authenticity of passports, and businesses can take advantage of supply chain efficiencies brought about by the use of RFID. Retailers lose an estimated US $40 billion in annual sales because of out-of-stock merchandise and other supply-chain inefficiencies; it is hoped that RFID will reduce that figure.[506] While striking the appropriate balance between these competing interests can be difficult, the statutory regime can help provide the framework and thus help to encourage consumer confidence.

Comprehensive Approach

While the Privacy Act recognises an individual's privacy interest, it also recognises that there may be other desirable social interests that compete with privacy. The Act attempts to balance these competing interests in a number of ways, although one way in particular could be problematic, as described below.

Section 7 Savings Provision

The Privacy Act contains a savings provision which provides that provisions in other statutes relating to personal information take precedence over the information privacy principles.[507] This provision has the potential to significantly limit the scope of the Privacy Act as there are "at least several hundred" other enactments to which the Principles of the Privacy Act are subject.[508] On the one hand, the savings provision provides balance as it permits Parliament to decide to elevate other competing interests over privacy in a particular case. On the other hand, the provision has the potential to undercut many of the protections of the privacy principles.

For example, in March 2006 news reports indicated that the Government was examining a proposal to issue individual identification numbers to children which would be stored in a central database in an effort to stem child abuse and failure at school.[509] On the face of it, such a proposal would appear to potentially violate Principle 12's restrictions on unique identifiers, but the Section 7 savings provision

[506] *Consumer Reports* (June 2006), p.35
[507] Longworth (1994), p.34. Also see Privacy Act 1993, s 7
[508] Roth, *Privacy Law and Practice*, para 1007.4
[509] Chalmers, Anna, *The Dominion Post*, 20 March 2006

would arguably permit the enactment. With respect to RFID, agencies could seek other enactments to permit the collection, use, retention and disclosure of personal information collected using RFID technology, and then none of the protections of the Principles described in this report would apply.

Importantly in this regard, the Privacy Commissioner's statutory functions include a legislative monitoring role, including examining information matching proposals by public sector agencies to collect, or disclose to other public sector agencies, personal information.[510] The Privacy Commissioner is also required to examine "proposed legislation (including subordinate legislation) or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the responsible Minister the results of that examination."[511] The Privacy Commissioner recognised the importance of this role in light of the section 7 savings provision in 1988, stating that "it is important that the opportunity be taken to provide privacy input into the enactment of new laws and the review of existing ones."[512] In this way, it is hopeful that significant undercutting of the Principles will be mitigated.

Privacy Commissioner to Have Due Regard for Other Competing Interests

The Privacy Act also requires balance in other ways. For example, the Act requires the Privacy Commissioner, in the performance of his or her functions and the exercise of his or her powers, to "have due regard for the protection of important human rights and social interests that compete with privacy including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way."[513] In the case of an RFID system, this provision could require the Privacy Commissioner to consider other interests such as efficiencies resulting from the use of the technology.

Exceptions to Information Privacy Principles and "Agency" Definition

Several exceptions to the information privacy principles demonstrate an effort to balance competing interests. For example Principles 2, 3, 10 and 11 each provide that an agency does not need to comply with the principle if non-compliance is necessary "to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences."[514] In such cases the Privacy Act's principles concerning collecting information directly from an individual, providing notice to the individual, limiting use of the information to the purpose for which it was collected and not disclosing the information to others, might not apply where RFID technology is used, or information collected using RFID technology is sought in a law enforcement investigation. The Privacy Act also recognises the news media's "special role in a democratic society"[515] by exempting any news medium, in relation to its news activities, from the definition

[510] Privacy Act 1993, s 13(1)(f)
[511] Privacy Act 1993, s 13(1)(o)
[512] Privacy Commissioner (November 1998), p.126
[513] Privacy Act 1993, s 14(a)
[514] Privacy Act 1993, s 6
[515] Roth, *Privacy Law and Practice*, para 1002.5

of "agency."[516] The Privacy Act does, however, apply to the media's non-news activities such as advertising, employment and subscription lists.[517]

Good Reasons for Refusing Access to Personal Information and Complaints Mechanism

The Privacy Act also contains provisions detailing "good reasons for refusing access to personal information" under Principle 6. The permissible reasons demonstrate an attempt to balance privacy against other competing societal interests such as security, defence or international relations,[518] trade secrets,[519] and protecting the "unwarranted disclosure of the affairs of another individual."[520]

Regarding complaints, the Privacy Act provides for a complaints mechanism that is low-cost and emphasises investigation and conciliation.[521] Complaints are investigated and can be mediated to achieve a settlement acceptable to the parties.[522] The Privacy Commissioner does not have the ability to award damages or fine agencies. In her 2005 annual report the Privacy Commissioner explained that the Privacy Act "encourages education and self-resolution of problems for citizens, and mediation and positive outcomes in an informal, non-punitive environment. The Act focuses on promoting compliance by business and government, with formal sanctions as a last resort. Cooperation, education and self resolution, both domestically and internationally, are its guiding themes."[523] Arguably, this approach helps to maintain balance and guard against overuse of the dispute resolutions system.

Sectoral Approach

California's Information Practices Act contains several provisions which attempt to balance other interests with privacy. For example the statute provides that it does not require an agency to disclose personal information to an individual if the information is compiled for the purpose of a criminal investigation of suspected criminal activities or pertains to the physical or psychological condition of the individual if the agency determines that disclosure would be detrimental to the individual.[524] The Act also provides that its provisions shall not be deemed to abridge or limit the rights of litigants under the laws of discovery.[525] Interestingly, the Information Practices Act also contains language which emphasises the importance of the privacy interest, providing that its provisions are to be "liberally construed so as to protect the rights of privacy arising under [the Act] or under the Federal or State Constitution."[526]

Some statutes enacting the sectoral approach have attempted to balance varying interests. California's law requiring businesses to implement reasonable security

[516] Privacy Act 1993, s2(1)
[517] Roth, *Privacy Law and Practice*, para 1002.5
[518] Privacy Act 1993, s 27
[519] Privacy Act 1993, s 28
[520] Privacy Act 1993, s 29(1)(a)
[521] Evans (2005), p.478
[522] Id. at 479
[523] Privacy Commissioner (November 2005)
[524] California Civil Code Section 1798.40
[525] California Civil Code Section 1798.71
[526] California Civil Code Section 1798.63

procedures and practices to protect personal information is one such example. The statute attempts to balance the protection of personal information with the needs and practices of businesses by providing that the procedures in place only need to be "reasonable" and "appropriate to the nature of the information."[527]

In general, however, sectoral proposals tend to be less balanced because they target a specific behaviour and, usually, prohibit it. For example Senate Bill 433 (Simitian) of 2005 prohibits the California Department of Motor Vehicles from issuing or renewing a driver's license or identification card using radio waves "to transmit personal information remotely or to enable personal information to be read from the license or card remotely."[528] Senate Bill 1078 (Simitian) of 2005 prohibits public schools from issuing any device to a pupil that uses radio waves to transmit personal information remotely or enable the remote reading of personal information in order to record the pupil's school attendance or establish or track the pupil's location on school grounds.[529] The balancing of privacy against other competing interests often plays out with respect to sectoral proposals in the legislative process when bills are amended to reflect those other interests. For example both of the proposals noted above were recently amended to include a three-year sunset provision so that the Legislature might revisit the issue in the future.[530]

Self-Regulation

Because they are often drafted by industry members, self-regulatory schemes would seem the most likely to balance privacy protections against competing interests such as the needs of business and existing business practices. This would seem to be the case with the CDT guidelines which were developed with industry representatives and a few consumer groups. For example the guidelines provide that, "as a general principle, it is desirable to provide consumers with, if cost effective and efficient, reasonable access to personally identifiable information, including location information, collected using RFID technology."[531] There are several acts of balancing within this scheme, including that the provision is "desirable" and that the access be "reasonable" and "cost effective and efficient." Some might argue that such language is a sign of imbalance, however, and does not provide adequate privacy protection.

Balance Conclusion

Each of the approaches attempts to be balanced, recognising that there are other important societal interests in addition to privacy. Sometimes the balance arguably goes too far in one direction, potentially undermining privacy and trust. For example the CDT guidelines use language that might allow other interests to too often trump privacy. On the other hand, others may argue that sectoral legislation improperly balances competing interests by being too prohibitive. The Privacy Act contains the most substantive attempts to balance privacy against other competing interests, including that the Privacy Commissioner have due regard for other interests and exceptions to the information privacy principles and related definitions. Most

[527] California Civil Code Section 1798.81.5
[528] Senate Bill 433 (Simitian), as amended 6 April 2006
[529] Senate Bill 1078 (Simitian), as amended 6 April 2006
[530] Senate Bill 433 (Simitian) and Senate Bill 1078 (Simitian), both amended 15 June 2006
[531] Center for Democracy and Technology (1 May 2006)

worryingly Section 7 of the Act, which provides balance in allowing other interests to be elevated above privacy in an enactment, arguably has the potential to undercut many of the Act's protections. The Privacy Commissioner's role in monitoring legislation is therefore critical to avoid undercutting the Act's protections.

Flexibility *– The regime will be flexible enough to deal with new developments*

The need for the law to be flexible and keep pace with technological developments is an important requirement for any privacy protection scheme and can help to promote confidence in the system. RFID technologies are evolving quickly and new applications are introduced or announced on a regular basis. Since the technology was first introduced read ranges have increased, microchips have gotten smaller and the price of the tags has decreased. All of these developments have the potential to challenge privacy protection schemes which seek to regulate the technology.

Comprehensive Approach

New Zealand's Privacy Act is principles-based, and as such is intended to be flexible and adaptable. The Act differs from a rules-based approach in that it does not specify strict rules that must be followed in each particular situation; rather, the Act outlines guiding principles or "norms of conduct."[532]

The Privacy Act is also designed to be technology-neutral. The information privacy principles focus on the collection of personal information and what an agency does with the information once it collects it. It does not matter *how* the agency obtained the information; whether on a paper form, in a verbal request or using RFID technology. Furthermore, it is irrelevant whether an RFID tag is big, bulky and clearly visible or is so small that an individual does not know that it is there. In either case an agency collecting the personal information using the tag must make sure that the person is aware of the collection and its purpose pursuant to Principle 3. The Act provides flexibility by allowing agencies to define their own purpose under Principle 1, letting them use their own business model or practices to help them in the definition.

The Privacy Act contains other provisions to help ensure that it keeps pace with technological change. For example, as previously mentioned, one of the Privacy Commissioner's enumerated functions is to "undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring."[533]

With respect to flexibility, the Act provides that the Privacy Commissioner may issue codes of practice which can modify the application of the information privacy principles by "prescribing standards that are more stringent or less stringent" than the principles.[534] The code may also exempt any action from a principle or prescribe how a principle is to be applied or complied with.[535] Parliament established codes of practice under the Privacy Act in part because "the process of promoting or changing

[532] Roth, *Privacy Law and Practice*, para 102
[533] Privacy Act 1993, s 13(1)(n)
[534] Privacy Act 1993, s 46(2)
[535] Id.

Acts of Parliament is expensive, intricate and generally very slow."[536] Codes of practice are seen as providing a greater degree of flexibility and ability for detail where the statute can provide a broad outline of the law.[537] On the other hand, codes of practice have been criticised overseas for, among other things, "lessening Parliament's control over the setting of legal standards," "taking a very long time to develop" and being "used to avoid stronger laws which would better protect public or individual interests."[538] In a 1998 report the Privacy Commissioner notes, however, that these "criticisms have generally been made where the codes do not have the backing of legislation and where they have been produced to avoid regulation."[539]

Under the Privacy Act codes of practice may apply to specified information, agencies, activities, industries or professions.[540] As a result, should the need and desire arise the Privacy Commissioner could develop a code of practice that relates, for example, to the general collection of personal information using RFID technology or that relates to a particular kind of RFID use.

Sectoral Approach

Sectoral laws have the most potential to raise concerns with respect to flexibility as they are often drafted to target a particular problem or practice. In the United States industry representatives have lobbied against broader consumer privacy measures, arguing that proposals should not ban technologies, but instead should focus on banning bad behaviour. As a result statutes often prescribe a specific practice, but in doing so, they have the potential to become obsolete if the defined practice changes and no longer fits within the scope of the law. Or, as David Russell, Chief Executive of Consumers' Institute, stated: "As soon as you start to define, you confine."[541]

Statutes can be drafted to attempt to deal with the possibility of technological change. For example Senate Bill 682 (Simitian) requires state-issued identification documents that use RFID to implement safety standards to prevent the transmission of information between tags and unauthorised readers that are at least as strong as a specific "mutual authentication" standard.[542] The proposed bill contains language should this technical standard change, providing "[i]n the event that the card authentication standard used in an identification document is found to be no longer capable of protecting against the transmission of information between identification documents and unauthorized readers, a stronger card authentication standard that will ensure protection shall be implemented."[543]

Other California statutes may not be as successful in ensuring flexibility, at least with respect to application to RFID technology. For example California law contains an anti-skimming provision, prohibiting the use of a scanning device to access or read information encoded on the magnetic strip of a credit or debit card.[544] This language is

[536] Privacy Commissioner (November 1998), p.205
[537] Id.
[538] Id.
[539] Id.
[540] Privacy Act 1993, s 46(3)
[541] Interview with David Russell, Chief Executive, Consumers' Institute (Wellington, 26 April 2006)
[542] Senate Bill 682 (Simitian), as amended 15 August 2005
[543] Id.
[544] California Penal Code Section 502.6

restrictive enough that it will not apply to the skimming of information from an RFID tag. Another statutory provision prohibits the use of an "electronic tracking device" to determine another person's location or movement, but defines "electronic tracking device" to mean "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals."[545] The provision seems focused on use on vehicles, and does not appear to extend to the use of RFID tags and readers to determine a person's location. It is also not clear how the term "movable thing" might be interpreted.

Self-Regulation

In the United States the CDT guidelines are intended to be read as principles and thus seek to maintain flexibility in their application. The guidelines specifically state: "These guidelines have been designed at the principles level in consideration of the wide variety and versatility of current RFID systems, the breadth of applications, and the speed at which the technology is developing."[546] The CDT guidelines are flexible so that they can apply across different industry sectors which might provide notice, for example, in a different manner depending on "the nature of a given RFID application, the company's business model, and the environment in which both are deployed."[547] Furthermore, the guidelines note that they may "need to be revisited as RFID technology continues to develop and as more is learned about its impact on privacy."[548] Likewise, GS1 New Zealand's "EPC/RFID Consumer Protection Code of Practice" is intended to be a first cut which may be revisited and revised as the technology advances or consumer demands change.[549]

The voluntary RFID guidelines issued by the Information and Privacy Commissioner of Ontario serve as "best practices guidance"[550] and apply to organizations that operate information systems "involving the use of RFID technology on consumer products involving or potentially linking to, personally identifiable information."[551] The guidelines specifically acknowledge the need for flexibility, providing that they are "voluntary, consensus-based guidance that recognizes the great variety of uses and applications for RFID technologies and information systems. Because of this heterogeneity, a degree of flexibility in its interpretation and application may be necessary."[552]

Flexibility Conclusion

The comprehensive approach reflected in New Zealand's Privacy Act would seem to most achieve the goal of flexibility as its principles-based nature and technology-neutral approach seek to provide adaptability to varying sectors and practices. The Privacy Commissioner's power to issue codes of practice is also an important component of this flexibility as it permits the targeting of particular practices or

[545] California Penal Code Section 637.7
[546] Center for Democracy and Technology (1 May 2006)
[547] Id.
[548] Id.
[549] Interview with Gary Hartley, Manager for Strategic Initiatives, GS1 New Zealand (Wellington, 5 May 2006)
[550] Information and Privacy Commissioner/Ontario (June 2006)
[551] Id.
[552] Id.

industries for additional regulation, if necessary. Sectoral laws face the potential of obsolescence because they target a defined problem or practice which may not be covered by the statute if the problem or practice changes and no longer fits within the scope of the law. Some sectoral laws have attempted to deal with this possibility by writing flexibility into the statute as legislators cannot possibly anticipate every situation. Current guidelines taking a self-regulatory approach seek to remain flexible, but, as with most self-regulation, compliance is voluntary. Self-regulatory guidelines, however, are often drafted by industry members familiar with their own business practices and are therefore likely to include flexibility as a component.

Certainty – *The regime will provide certainty for participants*

For the purposes of this report, certainty asks whether a privacy protection scheme tells those subject to it what to do and how to act. Most people like certainty; they want to know what the rules are and how to comply. They will also be more likely to trust a privacy protection regime that provides certainty. Certainty is important in the case of evolving technologies like RFID. As new applications are introduced, the people using them need to know whether the rules apply to them and, if so, what the rules require of them.

Comprehensive Approach

As previously noted, a principles-based approach like the Privacy Act requires people to apply the principles to their particular situation, taking into account how their business operates and how the technology is being used. In doing so, it requires discretion and, as a result is open to criticism that it does not provide certainty. On this point Sir Geoffrey Palmer has written: "The application of these principles is no easy matter and sometimes they are not necessarily consistent with one another. It is difficult to advise, on a particular set of facts, what the answer will be. This has led to quite a deal of public confusion about what the statute does and how it applies. The Privacy Commissioner has called it a 'uniquely flexible law,' but its very flexibility produces vagueness and a lack of certainty."[553]

There are others who have instead argued that the broad coverage of the Privacy Act actually creates certainty and "gives the confidence that it applies in nearly all circumstances,"[554] although whether this is truly the case given the potential breadth of the Section 7 savings provision is debatable. That section provides that other enactments take precedence over the information privacy principles. As discussed earlier, there are "at least several hundred"[555] other enactments to which the privacy principles of the Privacy Act are subject, meaning that there are many instances in which the principles do not apply.

With respect to providing certainty concerning RFID technology and users of such systems, a critical question is whether the Privacy Act applies to the particular collection at issue. While these matters are discussed in greater detail in the section entitled "Privacy Act 1993: Threshold Definitional Issues," there are several issues

[553] Palmer (1997), p.235
[554] Koppe (2002), p.48
[555] Roth, *Privacy Law and Practice*, para 1007.4

arising on this point. The first issue raises the question as to whether information collected using RFID is "information about an identifiable individual" if it is simply a string of numbers that is later linked to a database. Such information is arguably "personal information" under the Act because it has the "capacity to identify" the individual. Other issues of application include whether the gathering of information using an RFID tag is a collection of personal information "directly from" the individual concerned, and whether obtaining information using an RFID tag is a "collection" under the Privacy Act. Regarding the former, the Privacy Commissioner has recommended deleting "directly" from Principle 3 in order to remove uncertainty on this point, and it is hopeful that this recommendation will be included as part of the Government's proposals to reform the Privacy Act. In respect of the latter issue, it is suggested that, if there is any doubt as to whether RFID technology is covered by the Privacy Act in light of the decision in *Harder v Proceedings Commissioner*, then the issue should be clarified and included as part of the Government's proposals to reform the Privacy Act in order to provide certainty on this point.

Sectoral Approach

While sectoral approaches are thought to provide more certainty because they tend to be rules-based and more prescriptive, this is not always the case. In the United States the legislative process and any resulting statutes necessarily reflect the interests of its many participants. Sometimes that can lead to a lack of clarity in the statute because compromises have to be made as the bill moves through the process. Other times, the statutory language may intentionally provide for some uncertainty in an effort to be flexible. Or, a statute's potential application may be questioned at a later date.

For example California law requiring businesses to protect personal information from unauthorised access, use or disclosure includes several discretionary terms. The security procedures and practices must be "reasonable" and "appropriate to the nature of the information,"[556] although it may be uncertain what these terms mean. Also, there have been recent legislative efforts to expand California's security breach law to include breaches of non-computerised data after some questions arose as to the scope of the statute.[557]

Self-Regulation

The CDT guidelines are intended to be read as principles and therefore raise many of the same certainty issues as the comprehensive, principle-based approach of the Privacy Act discussed above. On the other hand, the CDT guidelines as well as those issued by GS1 New Zealand and the Information and Privacy Commissioner/Ontario, provide more certainty in terms of their application. They are RFID-specific guidelines focused on the particular technology as compared with a broader, comprehensive statute like the Privacy Act. As a result, questions such as whether the guidelines apply to the technology are not at issue.

[556] California Civil Code Section 1798.81.5(b)
[557] Senate Bill 1279 (Bowen), as amended 16 April 2004, and Senate Bill 852 (Bowen), as introduced

Certainty Conclusion

Sectoral, rules-based schemes may provide more certainty, although in some cases the certainty they provide may only be a false illusion because statutes can be drafted to contain discretion or flexibility in their application. To the extent that the current examples of self-regulation concerning the use of RFID technology use a principles-based approach, they may raise some of the same certainty issues as the comprehensive Privacy Act. Also, the voluntary nature of self-regulatory schemes means that not everyone will follow its provisions. Because the guidelines are voluntary and there is no established monitoring agency, the consequences of non-compliance are quite different as compared to a statute that requires adherence.

5 CONCLUSION

This report has applied objective criteria to the three major approaches to privacy protection and evaluated the strengths and weaknesses of each using RFID technology as a case study. In doing so, it has become clear that none of the regimes, by themselves, completely protects the privacy of individuals' personal information in every case. Each of the regimes has its strengths and weaknesses, some more than others. The following summarises the findings related to each approach and recommendations for policymakers in New Zealand and California and agencies using RFID. Key conclusions and thoughts for looking ahead are also detailed.

Comprehensive Approach

- A comprehensive approach, such as New Zealand's Privacy Act 1993, most robustly promotes the goals of openness, control and flexibility, thus helping to build consumer trust. The Act does not promote the goal of choice in the way that some sectoral legislation attempts to do. Instead, it recognises that choice is necessarily limited and provides individuals with openness, transparency and control.

- The Privacy Act contains the most substantive attempts to balance privacy against other competing interests by requiring that the Privacy Commissioner have due regard for other interests, exempting certain kinds of collections, uses or disclosures from the information privacy principles and specifying permissible reasons for refusing access to information. The Act contains a balancing provision that is potentially problematic, however, allowing other enactments to take precedence over the information privacy principles. The provision has the potential to undercut many of the protections of the principles, making the Privacy Commissioner's legislative monitoring role critical.

- Radio frequency identification technology is covered by the Privacy Act. The information collected using RFID technology is "personal information" under the Act because it has the capacity to identify the individual. And, the collection of information using RFID technology is not unsolicited and therefore comes within the scope of the Act.

Sectoral Approach

- Sectoral legislation can best achieve choice as it can be drafted, for example, to require that individuals be given a choice as to whether or not to purchase a product with an RFID tag in it or allow the collection of their personal information using RFID.

- Sectoral legislation can also be written to most robustly further the goals of openness, choice, control, balance and certainty, thus helping to foster trust and confidence. In most cases with respect to RFID, however, legislation attempting to achieve these goals has not yet been enacted in the United States and California. Because no baseline protection exists, there is a gap in practice and little to protect people in the meantime.

- Some sectoral legislation, like California's Information Practices Act, provides control in the form of access and correction rights, but that statute is limited to collection by state agencies. Overall the approach in California has been lacking in providing consumers with control over their personal information.

Self-Regulation

- Because self-regulation is often drafted by industry members familiar with their own business practices, it is most likely to include flexibility as a component. It also has the potential to further openness as notice and transparency can be included in the drafting. The voluntary nature of self-regulatory schemes, however, means that not everyone will adopt its provisions. With no established monitoring agency, enforcement may also become an issue.

- In analysing self-regulation, it is important to place the approach in a larger framework. Coming from the United States, it is often easy to criticise self-regulation because there is no baseline level of privacy protection and, in many instances, self-regulation is the only, or the principal, regulation applicable to a particular practice. In New Zealand however, the Privacy Act 1993 provides a floor of privacy protections and therefore self-regulatory proposals are another layer of protection rather than the only layer.

- There is nothing to stop self-regulation efforts from providing more protections than those provided under New Zealand's Privacy Act 1993. For example, rather than relying on the baseline of the Privacy Act, the GS1 New Zealand "EPC/RFID Consumer Protection Code of Practice" could have required retailers to provide consumers with a choice as to whether or not to provide their personal information or disable a tag.

Recommendations for Policymakers

The evaluation of the varying privacy protection schemes in this report highlighted a few instances where the statutory schemes might be insufficient or where important points should be emphasised.

New Zealand

- Include the Privacy Commissioner's recommendation deleting "directly" from Principle 3 as part of the Government's proposals to reform the Privacy Act in order to remove uncertainty as to whether gathering information using RFID technology (or, potentially, other technologies such as surveillance cameras or facial recognition technology) is within the scope of the Act.

- If there is any doubt as to whether RFID technology is covered by the Privacy Act (for purposes of the collection principles), in light of the Court of Appeal's decision in *Harder v Proceedings Commissioner*, consider clarifying the issue as part of the Government's proposals to reform the Act.

- Maintain the Privacy Act's broad definition of personal information. While it may seem overly broad to some, there are other limitations in the Act which constrain it. Consider addressing the issue should the Court of Appeal's comments in obiter dicta in *Harder v Proceedings Commissioner* result in a narrowing of the scope of personal information.

- Monitor other enactments which have the potential to undercut many of the protections of the information privacy principles under Section 7 of the Privacy Act.

- Ensure that the lack of choice in the Privacy Act does not become problematic, particularly with respect to new uses of technologies like RFID.

California

- Consider adopting a comprehensive approach to privacy protection providing consumers with a baseline level of protection that includes notice, choice and access and correction rights.

- Enhance the Office of Privacy Protection by making it independent and permitting individuals to make complaints to the office. The New Zealand Privacy Commissioner's ability to mediate disputes and help achieve settlements through a low-cost complaints mechanism that emphasises investigation and conciliation is commendable.

- With respect to sectoral legislation, apply the analysis framework put forward in this report to evaluate how the proposal helps to achieve the goals of trust, openness, choice, control, balance, flexibility and certainty.

Recommendations for Public and Private Sector Agencies Using RFID

The following list of recommendations is not necessarily exhaustive, nor are the recommendations themselves novel; others have also suggested them as best practices. They are important enough, however, to bear repeating:

- Think about privacy from the start. Privacy Impact Assessments are an excellent way to do this.[558]
- Consider using less intrusive means to collect personal information.
- Seek individuals' permission before collecting personal information using RFID.
- Be open and transparent about RFID use; do not covertly collect personal information.
- Clear signage is important; identify RFID readers.
- Minimise linkages to personal information.
- Tell individuals what information is being collected in addition to the notification requirements under Principle 3.
- In California, do not simply rely on a blanket consent by the individual to use or disclose collected information for another purpose. This does not build trust.

[558] See, e.g., http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

- Secure systems including databases and RFID tags themselves.
- Give people a choice as to whether or not to disable an RFID tag, without penalty.
- Do not collect information from other business' tags without the individual's permission.
- Resist the temptation to define your purpose broadly under Principle 1.
- In California, provide access to collected information and the ability to request correction

Key Conclusions and Looking Ahead

- A comprehensive approach to privacy can provide a baseline floor of protection. New Zealand's Privacy Act 1993, although not perfect, can offer such a floor with sectoral legislation, in particular codes of practice, and self-regulation helping to fill in the details.

- Trust is a measure of the success of a privacy protection regime and is critically important to the uptake of new technologies like RFID. While important in their own right, the other criteria – openness, choice, control, balance, flexibility and certainty – all underpin trust. For example people are more likely to trust an agency that has been open and transparent about its data collection efforts. Similarly, if individuals have control over their information once it has been collected, they are more likely to trust those who hold it. Each of the criteria can thus be used as a tool to evaluate whether the privacy regime has achieved trust in the system.

- This report analysed three different approaches to privacy protection and evaluated how each might further the goals of trust, openness, choice, control, balance, flexibility and certainty in the context of RFID technology. Although the report analysed only one technology, it provides a model for future analyses of other technologies such as biometrics, global positioning systems (GPS) and electronic databases. For example, at its most basic level, the analysis asks fundamental questions which can be asked of any technology:

    - Why is the criterion particularly important in the context of this technology?
    - What are the privacy issues raised by this technology with respect to the criterion?
    - How does the policy addressing these privacy issues further the goals of the criterion?
    - If the policy is violated, how is the criterion undermined?

Privacy protection regimes are critical and will only become more so as new technological applications develop and consumers worry about their impacts. The importance of legislative schemes that foster the criteria discussed in this report cannot be understated. Trust, especially, is critical to the uptake of new technologies and the other criteria are vital in their own right, as well as being elements of creating trust and confidence.

BIBLIOGRAPHY

AeA (American Electronics Association) (20 May 2006), 'Comments of AeA to the Department of Homeland Security Regarding the Draft Report "The Use of RFID for Human Identification"'. Retrieved from: http://www.aeanet.org

Article 29 Data Protection Working Party (19 January 2005), 'Working document on data protection issues related to RFID technology'

Balkovich, Edward, Tora Bikson and Gordon Bitko (2005), '9 to 5: Do You Know if Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace', Santa Monica, California: RAND Corporation

Belopotosky, Danielle, 'State Department Unveils Trial of Electronic Passports', *National Journal's Technology Daily*, 21 February 2006. Retrieved 23 February 2006 from: http://www.govexec.com/dailyfed/0206/022106tdpm1.htm

Bennett, C. and C. Raab (2003), *The Governance of Privacy: Policy Instruments in Global Perspective*, Hampshire: Ashgate Publishing Limited

Bennett, Colin (1992), *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, NY: Cornell University Press

Bergstein, Brian, 'Retailers Plow Ahead with RFID Chips', *Seattle Post-Intelligencer*, 20 May 2006

Binning, Elizabeth, 'Email Scams Hit Bank Customers', *New Zealand Herald*, 12 June 2006

Boucher Ferguson, Renee, 'RFID's High Cost Deters Business', *eWEEK.com*, 6 March 2006. Retrieved 19 May 2006 from: http://www.eweek.com/article2/0,1759, 1934328,00.asp?kc=EWNKT0209KTX1K0100440

Brown, Russell, 'Scanners: Why Supermarket Bar-codes are Already So Last Century', *The Listener*, 8 February 2003, p.39

Center for Democracy and Technology (1 May 2006), 'CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology'. Retrieved 2 May 2006 from: http://www.cdt.org/privacy/20060501rfid-best-practices.php

Chalmers, Anna, 'Plan to give ID numbers to kids', *The Dominion Post*, 20 March 2006

Christensen, Bill (1 June 2005), 'Proposal to implant tracking chips in immigrants', Technovelgy.com. Retrieved 18 June 2006 from: http://news.yahoo.com/s/space/ 20060601/sc_space/proposaltoimplanttrackingchipsinimmigrants

Clarke, Roger (2005), 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms'. Retrieved 2 March 2006 from: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Clarke, Steve (August 2001), 'The Case for Self-Regulation', *DLB Magazine*. Retrieved from: http://www.marketing.org.nz/cms/Resources/474

Collins, Jonathan, 'Bookstore RFID-enables its Operations', *RFID Journal*, 18 April 2006. Retrieved 24 April 2006 from: http://www.rfidjournal.com/article/articleprint/2273/-1/1

Collins, Jonathan, 'Lost and Found in Legoland', *RFID Journal*, 28 April 2004. Retrieved 18 May 2006 from: http://www.rfidjournal.com/article/articleprint/921/-1/1

Consumer Reports WebWatch (26 October 2005), 'Leap of Faith: Using the Internet Despite the Dangers, Results of a National Survey of Internet Users for Consumer Reports WebWatch'. Retrieved 13 June 2006 from: http://www.consumerwebwatch.org/pdfs/princeton.pdf

Cunliffe, Hon David (1 May 2004), 'Legislating Against Spam'. Retrieved from: http://www.med.govt.nz/upload/1874/discussion.pdf

Cunliffe, Hon David (28 July 2005), 'Anti-Spam Bill Introduced'. Retrieved from: http://www.beehive.govt.nz/ViewDocument.aspx?DocumentID=23810

Curtis, Karen (30 March 2006), 'Good privacy is good business', Keynote address, Privacy Issues Forum, Wellington. Retrieved 12 June 2006 from: http://www.privacy.org.nz/filestore/docfiles/64891293.doc

Electronic Privacy Information Center (2001), *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, Washington, D.C.

DeCew, Judith Wagner (1997), *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press

'E-passport Trial "A Success", but Read Times Worry Some', *The Dominion Post*, 24 April 2006

EPCglobal Frequently Asked Questions (n.d.), EPCglobal. Retrieved 19 May 2006 from: http://www.epcglobalinc.org/about/faqs.html#9

EPC/RFID Consumer Protection Code of Practice (March 2005) GS1 New Zealand. Retrieved 8 May 2006 from: http://www.gs1nz.org/EPCglobal/DownloadEPCRFIDCodeofPractice.aspx

European Commission (6 July 2006), 'RFID Consultation Website: Towards an RFID Policy for Europe'. Retrieved 7 July 2006 from: http://www.rfidconsultation.eu/

European Commission (n.d.), 'Your voice on RFID: Background document for public consultation on Radio Frequency Identification (RFID), Summary of five workshops'. Retrieved 7 July 2006 from: http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf

Evans, Katrine (2005), 'Show Me the Money: Remedies under the Privacy Act', 36 *Victoria University of Wellington Law Review* 475

Evans, Katrine (July 2001), 'Surreptitious Tape-recording: *Harder v The Proceedings Commissioner*', *Human Rights Law and Practice*, pp.32-42

'FDA Approves Use of Implantable Medical Data Chip', *SiliconValley.com*, 13 October 2004

'Five countries review privacy, technology' (17 May 2006). Retrieved 18 May 2006 from: http://www.angus-reid.com/polls/index.cfm/fuseaction/viewItem/itemID/11915

Gellman, Robert (2000), 'Privacy and Harmonization'. Retrieved from: http://www.coll.mpg.de/pdf_dat/gellmann.pdf

Gindin, Susan (1997), 'Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet', 34 *San Diego Law Review* 1153

'GlaxoSmithKline Tags HIV Drug', *RFID Update*, 24 March 2006

Government Administration Committee (1 August 2005), 'Crimes (Intimate Covert Filming) Amendment Bill'. Retrieved from: http://www.clerk.parliament.govt.nz/Content/SelectCommitteeReports/257bar2.pdf

Heisenberg, Dorothee (2005), *Negotiating Privacy: The European Union, the United States and Data Protection*, Boulder, CO: Lynne Rienner Publishers, Inc.

Human Rights Commission Case notes (April 2000), *Proceedings Commissioner v Commissioner of Police* CRT 23/99, Decision No 37/99. Case note 18 retrieved 9 June 2006 from: http://www.hrc.co.nz/hrc_new/hrc/cms/files/documents/19-Jun-2005_17-30-33_TeRito-apr00.pdf

IBM Multi-National Consumer Privacy Survey (October 1999), A comprehensive and comparative look at consumers in the United States, Germany, and United Kingdom and their attitudes toward privacy in everyday business transactions, prepared by Louis Harris & Associates Inc. Retrieved 13 June 2006 from: http://www.asc.upenn.edu/usr/ogandy/ibm_privacy_survey_oct991.pdf

Information and Privacy Commissioner/Ontario (June 2006), 'Privacy Guidelines for RFID Information Systems'. Retrieved 20 June 2006 from: http://www.ipc.on.ca/docs/rfidgdlines.pdf

Information and Privacy Commissioner/Ontario (February 2004), 'Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology'

International Conference of Data Protection and Privacy Commissioners (20 November 2003), 'Resolution on Radio-Frequency Identification'. Retrieved from: http://www.privacyconference2003.org/resolutions/res5.DOC

International Covenant on Civil and Political Rights (1966). Retrieved from: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

International Telecommunication Union (November 2005), *ITU Internet Reports 2005: The Internet of Things*, Geneva. Retrieved 19 May 2006 from: www.itu.int/internetofthings

Johnson, John, 'Wal-Mart: RFID Reduces Out-of-Stocks by up to 62 Percent', *RFID Watch Weekly*, 17 May 2006. Retrieved 18 May 2006 from: http://www.dcvelocity.com/articles/rfidww/rfidww20060517/walmart_rfid.cfm

Klosek, Jacqueline (2000), *Data Privacy in the Information Age*, Westport, CT: Quorum Books

Koppe, Katharina (2002), 'Data Protection and the Internet: A comparison of the approaches towards data protection in the European Union, the United States and New Zealand", LLM research paper, Law Faculty, Victoria University of Wellington

Law Commission (June 2004), 'Study Paper 15: Intimate Covert Filming', Wellington, New Zealand

Leyden, John, 'Consumers punish firms over data security breaches', *The Register*, 15 November 2005. Retrieved 16 June 2006 from: http://www.theregister.co.uk/2005 /11/15/data_security_breach_survey/

Libbenga, Jan, 'Belgians Implant RFID Chip in Tooth', *The Register*, 20 March 2006. Retrieved 19 May 2006 from: http://www.theregister.co.uk/2006/03/20/rfid_in_tooth/ print.html

Longworth, E. and T. McBride (1994), *The Privacy Act: A Guide*, Wellington: GP Publications

Lucas, Greg, 'Students Kept Under Surveillance at School: Some Parents Angry over Radio Device', *The San Francisco Chronicle*, 10 February 2005.

Marketing Association of New Zealand (n.d.). Retrieved from: http://www.marketing.org.nz/

Marks & Spencer (18 February 2005), 'Background to Marks & Spencer's Business Trial of RFID in its Clothing Supply Chain'. Retrieved 19 May 2006 from: http://www2.marksandspencer.com/thecompany/mediacentre/pressreleases/2005/com 2005-02-18-00.shtml

'Metro Opens Store of the Future', *RFID Journal*, 28 April 2003. Retrieved 18 May 2006 from: http://www.rfidjournal.com/article/articleprint/399/-1/1

Ministry of Economic Development (August 2004), 'Summary of submissions for legislating against spam in New Zealand'. Retrieved from: http://www.med.govt.nz/upload/1966/submissions-summary.pdf

Mulrooney, Paul, '$23,000 Skimmed from ATM', *The Dominion Post*, 30 March 2006

Neff, Jack, 'Privacy Group Slams Levi's for RFID-Chip Clothing Tags', *Advertising Age*, 28 April 2006

O'Brien, Kevin, 'Wireless: Useful tiny tracking tags provoke privacy concerns', *International Herald Tribune*, 15 May 2006

Office of the Privacy Commissioner of Canada (May 2006), 'Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act'. Retrieved from: http://www.privcom.gc.ca/information/ar/200506/2005_pipeda_e.asp#top

Organisation for Economic Co-operation and Development (27 February 2006), 'Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations', Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy. Retrieved 17 June 2006 from: http://www.oecd.org/dataoecd/57/43/36323191.pdf

Palmer, G. and M. Palmer (1997), *Bridled Power: New Zealand Government under MMP*, Auckland: Oxford University Press

Papakonstantinou, Vagelis (2002), *Self-Regulation and the Protection of Privacy*, Baden-Baden: Nomos Verlagsgesellschaft

'Pfizer Shipping RFID-tagged Viagra', *RFID Update*, 9 January 2006

Privacy Commissioner (February 2006), 'A Summary Report', conducted by UMR Research Limited. Retrieved 16 June 2006 from: http://www.privacy.org.nz/filestore/docfiles/24153322.pdf

Privacy Commissioner (November 2005), 'Annual Report of the Privacy Commissioner for the Year Ended 30 June 2005'. Retrieved from: http://www.privacy.org.nz/filestore/docfiles/annualreport2005.pdf

Privacy Commissioner (6 December 2004), 'Credit Reporting Privacy Code 2004'. Retrieved from: http://www.privacy.org.nz/filestore/docfiles/26242772.pdf

Privacy Commissioner (n.d.), 'General Information Paper'. Retrieved from: http://www.privacy.org.nz/privacy-act/general-information-paper

Privacy Commissioner (18 December 2003), 'Third Supplement to the First Periodic Review of the Operation of the Privacy Act 1993'

Privacy Commissioner (November 1998), 'Necessary and Desirable: Privacy Act 1993 Review, Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act'

Privacy Commissioner (28 June 1994), 'Health Information Privacy Code 1994', Reprinted and updated January 2003

Privacy Rights Clearinghouse (n.d.), 'A chronology of data breaches reported since the ChoicePoint incident'. Retrieved 5 July from: http://www.privacyrights.org/ar/ChronDataBreaches.htm

Pullar-Strecker, Tom, 'Firms Join Up for RFID Trial', *The Dominion Post*, 17 April 2006

Pullar-Strecker, Tom, 'Warehouse Study Paves Way for RFID Trial', *The Dominion Post*, 27 February 2006

Reding, Viviane (9 March 2006), 'The RFID Revolution: Challenges and Options for Action', International CeBIT Summit, Hannover. Retrieved 16 May 2006 from: http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/06/162&format=HTML&aged=0&language=EN&guiLanguage=en

Reilly, P. and R. Cullen (January 2006), 'Information Privacy and Trust in Government: A citizen-based perspective'. Retrieved from: http://www.e.govt.nz/resources/research/trust-and-privacy

'RFID Chip Hides in Tooth', 3 March 2006. Retrieved 6 March 2006 from: http://www.contractoruk.com/news/002543.html

RFID Journal (n.d.), 'RFID Journal Frequently Asked Questions'. Retrieved 5 May 2006 from: http://www.rfidjournal.com/faq/16

'RFID Position Statement of Consumer Privacy and Civil Liberties Organizations' (20 November 2003). Retrieved from: http://www.privacyrights.org/ar/RFIDposition.htm

Richtel, Matt, 'In Texas, 28,000 Students Test an Electronic Eye', *The New York Times*, 17 November 2004

Roberts, C.M. (2006), 'Radio frequency identification (RFID)', *Computers & Security*, pp.18-26

Roth, Paul (2006), 'The workplace implications of RFID technology', *Employment Law Bulletin*, February, pp.10-14

Roth, Paul, *Privacy Law and Practice* (looseleaf, Butterworths, Wellington), last updated March 2006

Roth, Paul (30 March 2006), 'Workplace Privacy Issues Raised by RFID Technology', Privacy Issues Forum, Wellington

Roth, Paul (November 1997), 'The Privacy Act 1993: Workplace Testing, Monitoring, and Surveillance', *Human Rights Law and Practice*, pp.113-127

Roussos, George (March 2006), 'Enabling RFID in Retail', *IEEE Computer Society*, pp.25-30

Sayer, P. and J. Niccolai, 'European Commission launches inquiry into RFID', *Computerworld*, 20 March 2006

Senate Republican High Tech Task Force (109th Congress), 'Policy Agenda'. Retrieved from: http://republican.senate.gov/httf/index.cfm?FuseAction=Policy Agenda.Home

Shroff, Marie (11 August 2004), 'A Public Advocate for Private Matters: The role of the Privacy Commissioner', Address by Privacy Commissioner Marie Shroff, Victoria University of Wellington, Centre for Public Law, Public Office Holders Address. Retrieved from: http://www.privacy.org.nz/library/a-public-advocate-for-private-matters-the-role-of-the-privacy-commissioner

Slane, Bruce (9 April 1999), 'Privacy Protection: A Key to Electronic Commerce', Address by Privacy Commissioner Bruce Slane, New Zealand Law Conference Rotorua. Retrieved 13 June 2006 from: http://www.privacy.org.nz/library/privacy-protection-a-key-to-electronic-commerce

Songini, Marc, 'Wisconsin law bars forced RFID implants', *Computerworld*, 12 June 2006. Retrieved 14 June 2006 from: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111542&source=NLT_AM&nlid=1

Stein, Rob, 'Use of Implanted Patient-Data Chips Stirs Debate on Medicine vs. Privacy', *The Washington Post*, 15 March 2006, p.A1

Stein, Rob, 'Implantable Medical ID Approved by FDA', *The Washington Post*, 14 October 2004, p.A1

Stevens, Robert (September 1998), 'Move Openly to Jail: Do Not Pass Go? – Questioning Dr. Roth's Interpretation of "Directly" in the Privacy Act 1993', *Human Rights Law and Practice*, pp.116-119

Stewart, Blair (24 November 2005), 'Seeking Solutions to the Privacy Challenges of Emerging Technologies', Presentation to New Zealand Computer Society, Wellington. Retrieved 20 June 2006 from: http://www.privacy.org.nz/filestore/docfiles/65571469.ppt

Stewart, Blair (9 February 2005), 'EPC/RFID: The Way of the Future? A Privacy Perspective', Notes for a contribution by Blair Stewart, Assistant Privacy Commissioner, to a panel session at GS1 New Zealand/EPCglobal New Zealand

Stewart, Blair (31 May 1999), 'Privacy Law and the Private Sector: A New Zealand Perspective', Speech by Blair Stewart, Assistant Privacy Commissioner, at the IIR Minimising Risks and Costs of Privacy Requirements Conference Melbourne

"EPC/RFID-The Way of the Future" Conference, Auckland. Retrieved 26 May 2006 from: http://www.privacy.org.nz/filestore/docfiles/6806566.pdf

Swedberg, Claire, 'RFID Watches Over School Kids in Japan', *RFID Journal*, 16 December 2005. Retrieved 19 December 2006 from: http://www.rfidjournal.com/article/articleprint/2050/-1/1

'The End of Privacy?', *Consumer Reports*, June 2006, pp.33-39

'The Future is Here: A Beginner's Guide to RFID', *RFID Gazette*, 28 June 2004. Retrieved 18 May 2006 from: http://www.rfidgazette.org/2004/06/rfid_101.html

Tunnah, Helen, 'E-passports by End of Year', *New Zealand Herald*, 29 October 2005

Universal Declaration of Human Rights (1948). Retrieved from: http://www.un.org/Overview/rights.html

U.S. Department of Commerce (April 2005), 'Radio Frequency Identification: Opportunities and Challenges in Implementation'. Retrieved from: http://www.technology.gov/reports/2005/RFID_April.pdf

U.S. Department of Homeland Security (May 2006), 'The Use of RFID for Human Identification', a draft report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee. Retrieved from: http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_rpt_rfid_draft.pdf

U.S. Federal Trade Commission (26 January 2006), 'ChoicePoint Settles Data Security Charges'. Retrieved from: http://www.ftc.gov/opa/2006/01/choicepoint.htm

U.S. Federal Trade Commission (March 2005), 'Radio Frequency IDentification: Applications and Implications for Consumers'. Retrieved from: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

U.S. Food and Drug Administration (9 June 2006), 'FDA Announces New Measures to Protect Americans from Counterfeit Drugs'. Retrieved 12 June 2006 from: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01386.html

U.S. Food and Drug Administration (March-April 2005), 'Radiofrequency Identification Technology: Protecting the Drug Supply', *FDA Consumer Magazine*. Retrieved 19 May 2006 from: http://www.fda.gov/fdac/features/2005/205_rfid.html

U.S. Government Accountability Office (May 2005), 'Information Security: Radio Frequency Identification Technology in the Federal Government'. Retrieved 16 May 2006 from: http://www.gao.gov/new.items/d05551.pdf

U.S. Office of Management and Budget (May 2004), 'Overview of the Privacy Act of 1974', prepared by the Office of Information and Privacy. Retrieved from: http://www.usdoj.gov/04foia/04_7_1.html

U.S. State Department, 'The U.S. Electronic Passport Frequently Asked Questions'. Retrieved 24 May 2006 from: http://travel.state.gov/passport/eppt/eppt_2788.html

'Vendors Target Amusement Parks', *RFID Journal*, 27 November 2002. Retrieved 18 May 2006 from: http://www.rfidjournal.com/article/articleprint/123/-1/1

VeriChip Corporation (n.d.), "Solutions: Access Control". Retrieved 6 June 2006 from: http://www.verichipcorp.com/content/solutions/1117391741

Vierria, Dan, 'Tag – You're It', *The Sacramento Bee*, 12 May 2006

Warren, S. and L. Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 193

Waters, Richard, 'US Group Implants Electronic Tags in Workers', *Financial Times*, 12 February 2006

Westin, Alan (1967), *Privacy and Freedom,* New York: Atheneum

APPENDIX – PRIVACY ACT 1993: INFORMATION PRIVACY PRINCIPLES

Privacy Act 1993[559]

Part 2
Information privacy principles

6 Information privacy principles

The information privacy principles are as follows:

Information privacy principles

Principle 1

Purpose of collection of personal information

Personal information shall not be collected by any agency unless---

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

Principle 2

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds, –

(a) that the information is publicly available information; or

(b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or

(d) that non-compliance is necessary---

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) that compliance would prejudice the purposes of the collection; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

[559] Reprinted as at 1 October 2003. For complete text of the Privacy Act 1993, please see: http://www.legislation.govt.nz

(g) that the information---

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) that the collection of the information is in accordance with an authority granted under section 54.

Principle 3

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of--

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of---

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) if the collection of the information is authorised or required by or under law,---

(i) the particular law by or under which the collection of the information is so authorised or required; and

(ii) whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,---

(a) that non-compliance is authorised by the individual concerned; or

(b) that non-compliance would not prejudice the interests of the individual concerned; or

(c) that non-compliance is necessary---

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that compliance would prejudice the purposes of the collection; or

(e) that compliance is not reasonably practicable in the circumstances of the particular case; or

(f) that the information---

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4

Manner of collection of personal information

Personal information shall not be collected by an agency---

(a) by unlawful means; or

(b) by means that, in the circumstances of the case,---

(i) are unfair; or

(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure---

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against---

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled---

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b), an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5.

Principle 7

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled---

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1), the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8

Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,---

(a) that the source of the information is a publicly available publication; or

(b) that the use of the information for that other purpose is authorised by the individual concerned; or

(c) that non-compliance is necessary---

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to---

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information---

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) that the use of the information is in accordance with an authority granted under section 54.

Principle 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,---

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary---

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to---

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information---

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.

Principle 12

Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any 1 or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of section OD 7 of the Income Tax Act 1994.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

ISBN 0-473-11336-8