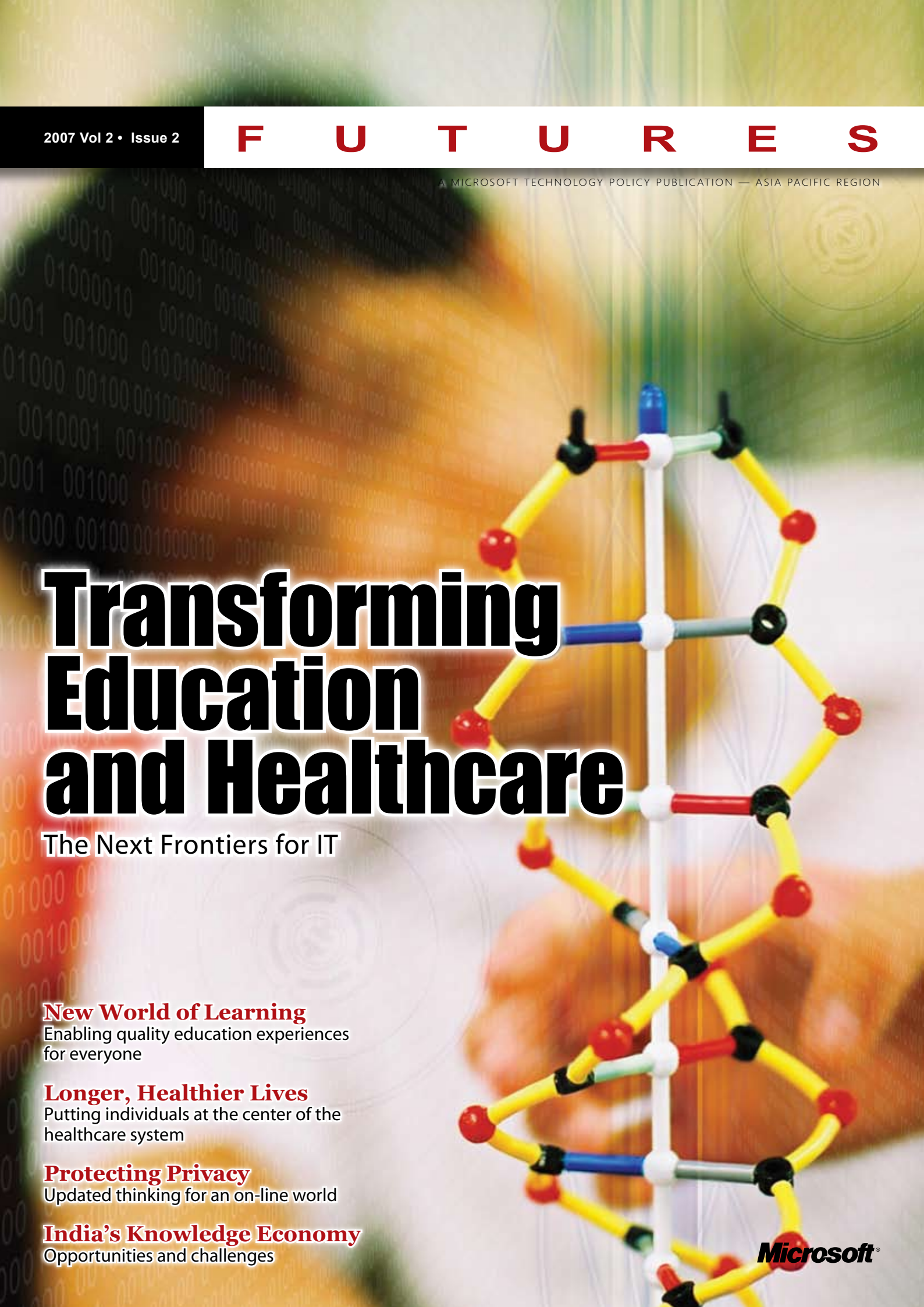
2007 Vol 2 • Issue 2

F U T U R E S

A MICROSOFT TECHNOLOGY POLICY PUBLICATION — ASIA PACIFIC REGION



Transforming Education and Healthcare

The Next Frontiers for IT

New World of Learning
Enabling quality education experiences for everyone

Longer, Healthier Lives
Putting individuals at the center of the healthcare system

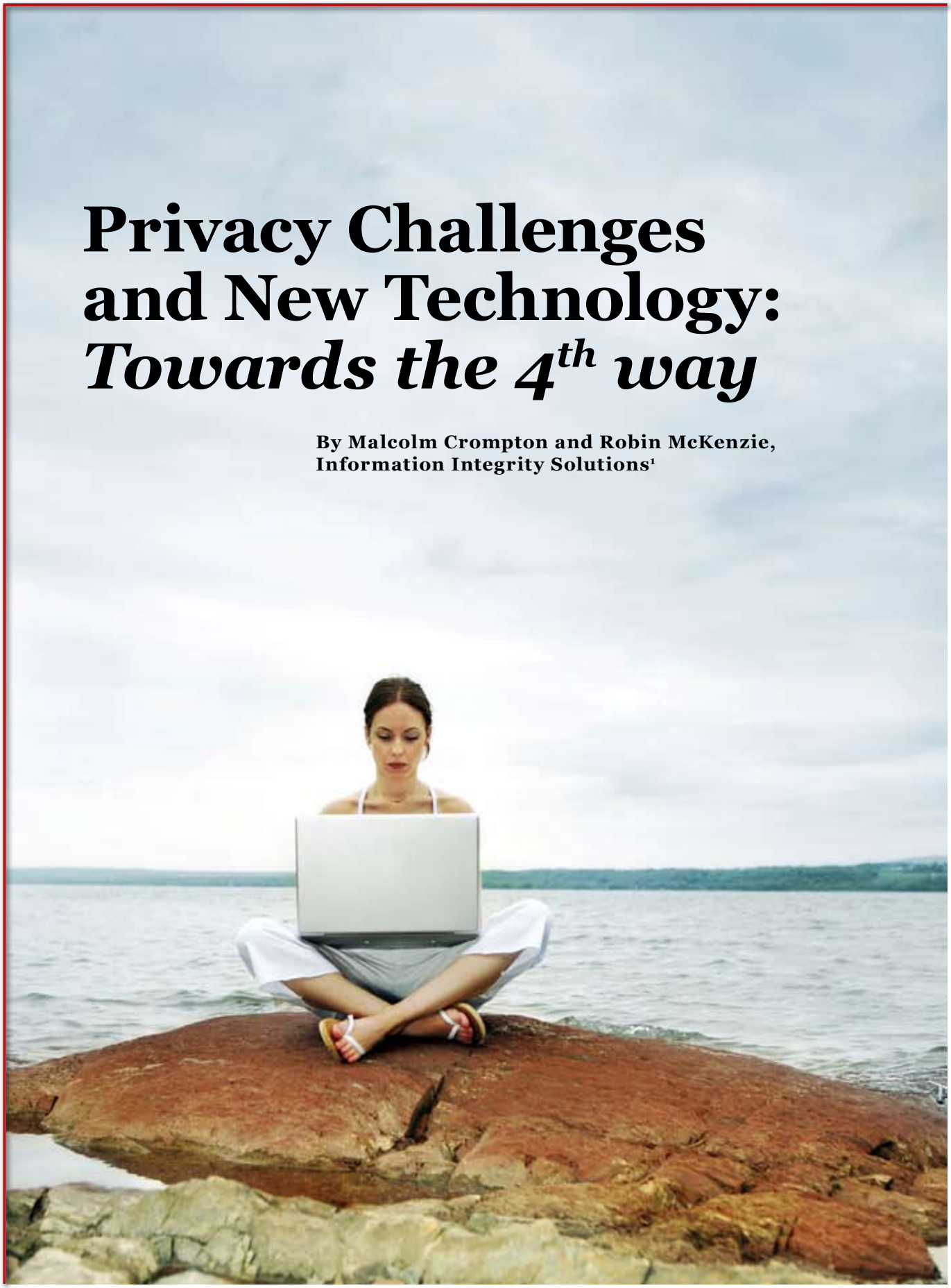
Protecting Privacy
Updated thinking for an on-line world

India's Knowledge Economy
Opportunities and challenges

Microsoft®

Privacy Challenges and New Technology: *Towards the 4th way*

By Malcolm Crompton and Robin McKenzie, Information Integrity Solutions[1]



Introduction

The use of new technology has dramatically transformed the information landscape. While many economies have frameworks for the protection of personal information, including privacy laws, a general feeling of unease is emerging; a feeling that these frameworks, largely developed in an environment of paper-based information systems and analogue communications systems, are either breaking down or broken.

Traditional privacy protection is based on the notion of giving individuals fine-grained control and expecting them to want and be able to exercise it. Arguably the current laws do not deliver well on this objective; nor do they necessarily give individuals confidence or trust in the information handlers.

This is a global issue which requires a global response. The importance of getting the privacy framework right is well recognized in many economies and in forums such as the European Union (EU), the Organisation for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation forum (APEC). Unfortunately, there is real potential for the efforts on all these fronts to turn into a process nightmare of questionable efficacy, especially if legislative change is an emergency response to a new development in technology, a new business practice, major privacy breach or otherwise.

There is a need for new thinking that delivers both better privacy and more efficient business practices, not with more rules and restrictions but with a greater understanding of what is needed for real trust to exist between individuals and business so that when personal information is revealed there will be no surprises as to how it is handled — and if things go wrong — there will be swift and efficient restitution. At best, innovation by business, perhaps in the form of new business processes, or by individuals, as we see emerging in the world of 'Web 2.0', should be able to develop safely with minimal hindrance.

"Traditional privacy protection is based on the notion of giving individuals fine-grained control and expecting them to want and be able to exercise it."

What is Happening to Our Personal Information?

The amount of personal information being collected is growing explosively. According to IDC, the amount of information created and copied in 2010 will surge more than six-fold to 988 exabytes, representing a compound annual growth rate of 57 per cent. The last time research of this type was attempted was in 2003 by researchers at the University of California, Berkeley, who came up with an information total of around five exabytes. [2]

Much of the information collected is about each of us as individuals. It also includes very significant and potentially sensitive information, from our financial records to our health records with an increasing proportion of it subject to analysis in ways which many of us barely know about, ranging from credit histories to customer relationship management or population health studies.

An increasing proportion of the information about us is information about our movements and actions. The sources range from the 'black boxes' recording incidents in our motor cars to the recording of our toll way payments, video images of us going in and out of buildings, moving through public places and the continued surveillance of our internet activity and SMS messages.

The further potential for sources of data to fuel this growth is enormous. More and more of the devices around us will be actively networked to the wider world and contain significant processing power — phones, fridges, doorways, internally worn prosthetic devices, as well as all financial transactions. Collation of data from these

[1] See CNET: "Dell embraces Google" - http://news.com.com/Dell+embraces+Google/2100-1032_3-6077051.html

[2] "Humans created 161 exabytes of data in 2006", www.iTnews.com.au, 7 Mar 2007, www.itnews.com.au/print.aspx?CIID=74870&SIID=35

CONVERGENCE: Security and privacy are no longer to be seen as mutually exclusive but as merging in the current rapidly evolving IT environment, said Peter Cullen, Microsoft's Chief Privacy Strategist, at a recent Privacy Commissioner hosted event in Australia.

sources adds another dimension — potential tracking of where we are, what we are doing and with whom or what, moment by moment.

Identity Management of Increasing Significance

For this reason, our 'identity' is one of the most important points of control over personal information. Each of us as individuals is keenly aware that our 'identity' is the 'glue' that holds all this personal information together. For the same reason, organizations both public and private seek information that is connected to an 'identity' because that is often how they add value.

Our 'identity' is a very subtle concept. [3] Often, it is not necessarily the 'identity' we would assign to ourselves in any of the myriad roles we occupy, be it parent, employee, student, seeker of credit or anything else. At other times, they are identities with characteristics assigned to us by a person or organization that has been gathering and analyzing personal information believed to be related to that identity.

Indeed, it is important to distinguish between an 'identity' that has been assigned to us and the 'profile' developed about that identity using the information linked (rightly or wrongly) to the identity. 'Identity' seeks to define the physical you and me. That identity then is used to seek links between the various elements of our personal histories that have been recorded in order to build a profile. The history includes our behaviors and events in which we have participated.

Moreover, either because of the lack of more subtle thinking or because organizations

[3] This subtlety is explored further in "Proof of ID required? Getting Identity Management Right", by Malcolm Crompton when Privacy Commissioner, March 2004 – in HTML, PDF or Word – online at: www.privacy.gov.au/publications/index.html#S

are actively seeking more information about us, identity is used to authorize or collate activity when it is not inherently necessary, even when the technologies exist to avoid such surveillance. [4]

Fraudsters have become good at making identities fuzzy. They use those fuzzy identities to participate in events that then link in an inaccurate way to the individual who really is that identity. Data then leads to false information, false knowledge and false wisdom.

As such, identity management is arguably the privacy issue of the moment.

Our Personal Information is Moving Across Borders

As more and more personal information is collected used and disclosed, an increasing

Authors' Biographies

Malcolm Crompton
Managing Director, Information Integrity Solutions Pty Ltd

Malcolm Crompton provides high level advice to private sector and public sector organizations on building trust through excellent data governance, particularly in their collection and use of personal information. He is also the Asia Pacific based Director of the International Association of Privacy Professionals and Director of Bellberry Limited, a private not-for-profit organization that provides health ethics committee services in accordance with the NHMRC Statement on Ethical Conduct in Research Involving Humans.

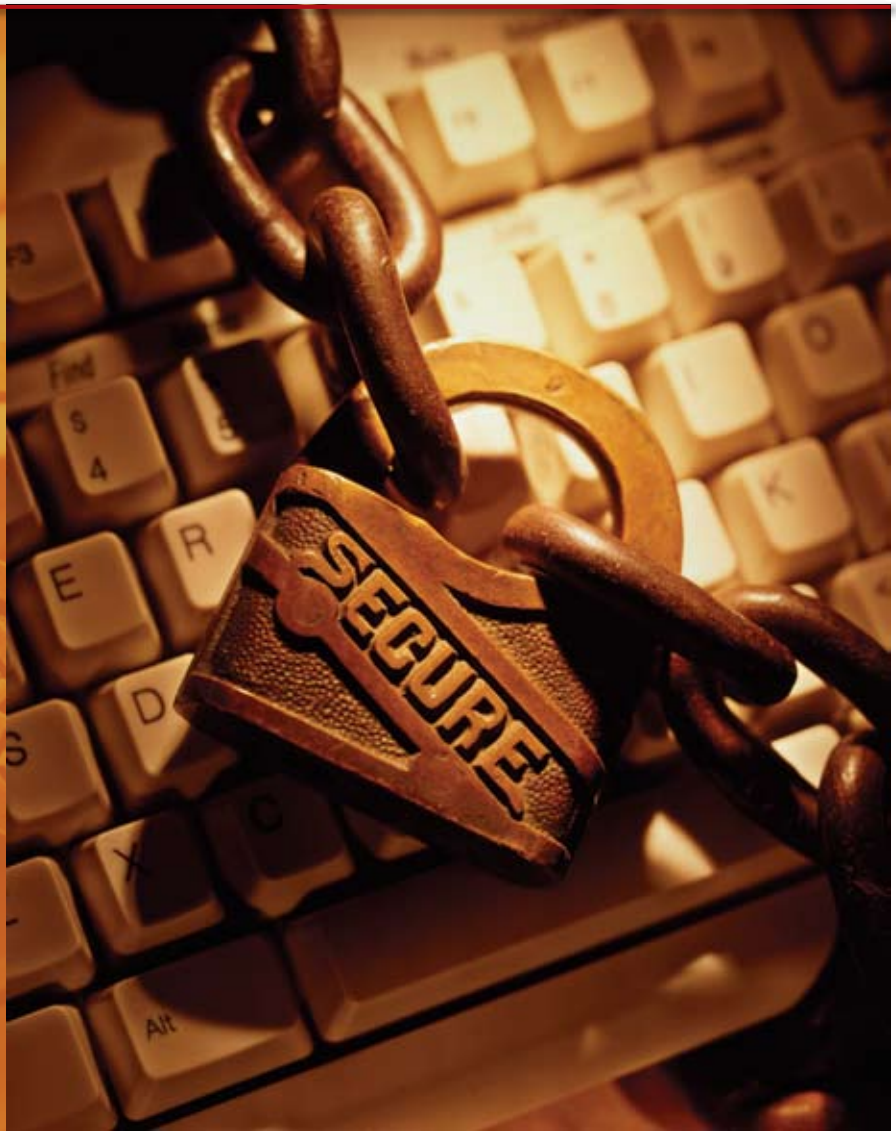
He was Australia's third Federal Privacy Commissioner for five years until April 2004. He led the implementation of private sector privacy law that commenced in 2001. He has established a global reputation for his forward thinking on the handling and governance of personal information. Malcolm has advised APEC regularly on implementation of the APEC privacy framework. He has also consulted to the OECD, leading technology companies, Australian financial institutions and government agencies. He is a member of the Microsoft Trustworthy Computing Academic Advisory Board.

Robin McKenzie
Principal Consultant, Information Integrity Solutions Pty Ltd

Robin McKenzie has most recently held a senior position with the federal Office of the Privacy Commissioner. Over five years in policy and corporate and public affairs she played a key role in projects including: implementing the private sector provisions of the Privacy Act including developing the guidelines and information sheets; overseeing the drafting and passing of the resolution relating to short privacy notices at the 25th International Conference of Data Protection & Privacy Commissioners in 2003; managing the review of the private sector provisions of the Privacy Act; researching and writing major speeches on leading edge areas of privacy including biometrics and regulatory issues. ■

[4] See, for example: "Proof of ID required? Getting Identity Management Right" (ibid); and "ID Cards - UK's high tech scheme is high risk", London School of Economics News Release, 27 June 2005 and from there, link to the LSE Report titled The Identity Project: an assessment of the UK Identity Cards Bill and its implications, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

"... We are seeing a general unease also emerging among policymakers and regulators, sensing that 'there must be a better way'... For example, regulators around the world are acting on the basis that new approaches are needed including the need to find privacy solutions that go beyond simply implementing privacy principles."



proportion is flowing seamlessly across borders through back up servers, for "24x7, follow the sun" service facilities such as call centers, service bureaus, round-the-clock problem solving. Among other things, this creates a growing need by law enforcement and national security officials for greater cooperation between governments and their agencies and with the private sector. The public expects that the protection of their personal information not be compromised by such developments. The level of protection should remain the same whether personal information about individuals stays in the home economy or moves or is accessed somewhere else.

The Pacific Rim is one of the areas of the world where the handling of personal information is increasing and transforming most rapidly. The region's pre-eminent economic grouping, APEC, has recognized that a key to economic growth through eCommerce is the free flow of personal information in a way that respects privacy. However, it has become very clear that the barrier to achieving this goal is the emerging problem of cross border data flows where information collected in one economy is processed in another. In the context of privacy regulation, the challenge is made more difficult because privacy and data protection regulation is usually bound to a local jurisdiction and can only 'see' and regulate the information flows in that jurisdiction.

Privacy Laws Under Stress

Privacy laws do not currently map well onto this exponential growth in e-information

and related business models because privacy laws tend to assume binary relationships between individuals and organizations rather than in terms of the networking of information and extended value-chains.

If we are going to use personal information in innovative ways, there is the question of who bears the risk when things go wrong. Concern about this issue contributes to people's sense of being out of control, a sense of distrust and the feeling that things need to be fixed.

This angst is particularly impacting on public data sets derived from various government activities, including land sales, motor vehicle registration, and the electoral system. As processing capacity and innovative uses increase there is a related tendency to respond to individual concerns by limiting access to specific authorized circumstances. In Australia, this has been the case for credit reporting databases, the electoral roll and the integrated public telephone number database.

The 'Rules of The Game' As They Are Today

Unfortunately, these circumstances have been met with a global patchwork response. In the face of the many challenges that technology has posed for privacy, governments have often adopted a BAND-AID and technology specific response. There is spam legislation, data breach legislation, spyware legislation and other laws running parallel with privacy principles. In addition, each economy has its own response. This patchwork of regulation is causing major compliance difficulties for companies particularly those operating across borders.

Most laws aimed at the protection of personal information are based on regulating various stages of an 'information life cycle'. The conventions that form the basis of data protection law have been designed to deal with discrete collections of data and discrete histories. They were based on the concept of transparency and individual control (albeit with increasing numbers of exceptions). Thus they usually provide for notice, collection minimization, use and disclosure limitations, security and accuracy, rights of access and correction and destruction.

"If we are going to use personal information in innovative ways, there is the question of who bears the risk when things go wrong."

Economies in the APEC region played a key role in the early development of privacy frameworks and laws. One of the earliest frameworks promulgated by a multilateral organization was developed by the OECD in 1980 through a working group chaired by eminent Australian Justice, Michael Kirby. Australia and New Zealand were amog the first economies to adopt a law based on the OECD principles. But the OECD framework was created in advance of the information technology revolution that has swept across the globe since that time. As outlined more fully below, APEC more recently established a leadership role in developing a new privacy framework — adopted in November 2005 — that takes into account the dramatic changes we've seen in how personal information is generated, shared, and stored in a digital environment.

Privacy is also protected by a myriad of other laws, including anti-spam law, broader consumer protection law, telecommunications and postal legislation, administrative law such as Freedom of Information and Ombudsmen. Despite requirements in privacy laws to keep information secure, privacy and security in a broader sense have often been seen as incompatible. However, at a recent Privacy Commissioner hosted event in Australia, Peter Cullen, the Chief Privacy Strategist of Microsoft, confirmed that security and privacy are no longer to be seen as mutually exclusive but as merging in the current rapidly evolving IT environment.

General Public Policy Response

Notwithstanding the continued, often patchwork response just described, we are seeing a general unease also emerging among policymakers and regulators, sensing that 'there must be a better way'.

A NEW WAY: In Australia, a consortium of businesses has formed to develop innovative approaches aimed at meeting the new privacy challenges. They are developing new thinking on how the benefits of new technology including new data analytics capacity can be achieved in a way that also generates consumer trust.

For example, regulators around the world are acting on the basis that new approaches are needed including the need to find privacy solutions that go beyond simply implementing privacy principles. For example, the final communiqué from the 2006 Data Protection Commissioners' conference, which had as its focus the "surveillance society", noted that:

- surveillance activities can be well-intentioned and bring benefits;
- unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy;
- privacy and data protection regulation is an important safeguard but not the sole answer;
- public trust and confidence is paramount.

Often, the "sectoral approach" to privacy currently embodied in US law is juxtaposed against the more prescriptive and expansive European Data Directive approach but there are other legislative approaches emerging. Specifically, there are reviews of laws and moves to introduce new and different laws or non-legislative approaches in a number of economies, seeking to find a 'third way'. For example:

- A UK review of privacy law is calling for penalties for breach of privacy laws;
- In the US there are many initiatives at all levels of government, including data breach laws and a call for uniform federal omnibus privacy legislation;
- In Australia there are reviews of privacy law at both federal and state levels, including taking into account developments in technology and the information economy;
- New Zealand is reviewing its privacy law and is exploring privacy on a first principles basis;
- Canada and Japan are also reviewing their privacy laws;
- Singapore has recently been conducting an interagency privacy review to determine whether legislation is required;
- New privacy laws are being considered in Malaysia while deliberations are

beginning in China around what privacy rules might look like in the future, and;
- In India, there has been some support for developing a "self regulatory organization (SRO)" and data privacy watchdog through industry consultation rather than through legislative mandate.

A theme of note in the submissions of Privacy Commissioners to the various reviews and inquiries has been the call for additional enforcement powers. Another theme has been the need for greater consistency in privacy law including the need to protect personal information as it travels across borders. For economies without specific privacy laws, the APEC privacy principles are providing a good basis, with a "harms-based" approach, for developing a response to privacy challenges.

In the light of the major challenges described here, however, the policy debates highlighted above will not end the process for driving new thinking and creating new approaches. We almost certainly need to find an even braver 'fourth way' — an approach that takes account of existing regulatory regimes but in a way that clearly acknowledges the need in today's digital age for greater global harmonization and stronger collaboration between the public and private sectors.

Trends Towards A Possible Fourth Way — The Basic Principles

There are a number of significant initiatives around the Asia Pacific region aimed at finding a new way. These include on the one hand significant work that a number of global organizations including the Hunton & Williams Centre for Information Policy and Leadership, Proctor and Gamble, Kodak, Microsoft as well as the US Federal Trade Commission are undertaking to develop more consumer friendly, or multilayered

Quarantining only Marginally Effective

The implementation model that businesses and governments have been developing for the APEC Privacy Framework breaks new ground by moving away from the model dominant elsewhere that relies on the quarantining of personal data within a nation or region in order to protect individual rights. The fact that the APEC model recognizes that such quarantining can only be marginally effective in a highly globalized and networked age is of great significance for both international business and consumers. By shifting the emphasis from quarantine to enforcement at all points in the "data chain", the Framework has the potential to both ease the burden of regulatory compliance for businesses and to enhance real-world consumer data protection. ■

APEC Information Privacy Principles

As Set Out in The APEC Privacy Framework [1]

I – Preventing Harm

Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

II – Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

a) the fact that personal information is being collected;
b) the purposes for which personal information is collected;
c) the types of persons or organizations to whom personal information might be disclosed;
d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;
e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

III – Collection Limitation

The collection of personal information should be limited to information that is relevant to the purposes of collection and

[1] Online at www.apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.html

any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

IV – Uses of Personal Information

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

a) with the consent of the individual whose personal information is collected;
b) when necessary to provide a service or product requested by the individual; or,
c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

V – Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

VI – Integrity of Personal Information

Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

VII – Security Safeguards

Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

VIII – Access and Correction

Individuals should be able to:

a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;
b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;
    i. within a reasonable time;
    ii. at a charge, if any, that is not excessive;
    iii. in a reasonable manner;
    iv. in a form that is generally understandable; and,
c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

Such access and opportunity for correction should be provided except where:

i. the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;
ii. the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or
iii. the information privacy of persons other than the individual would be violated.

If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

IX – Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. ■

ATMOSPHERE OF TRUST: The key moving forward will be securing a commitment by APEC Member Economies to implement pilot projects within the APEC Pathfinder Framework until a complete, effective and adaptable compliance framework is in place. The ultimate goal must be an atmosphere of trust by citizens and consumers without stifling innovation and efficiencies created by emerging technologies.

privacy notices. Data breach law is also increasingly being enacted in the US.

These initiatives are nevertheless only partial responses. At a more holistic level, in Australia, a consortium of businesses has formed to develop innovative approaches aimed at meeting the new privacy challenges. They are developing new thinking on how the benefits of new technology including new data analytics capacity can be achieved in a way that also generates consumer trust. This includes looking at such options as an even stronger focus on allocating and mitigating the risks arising from the handling of personal information combined with stronger transparency and accountability measures instead of excessive reliance on consumers responding to 'notice and consent' except where it really matters. In New Zealand, the government is one of the leaders in implementing e-Government initiatives which include developing a consumer centric and privacy enhancing approach to identity management in the online environment.

Compliance and Enforcement In A Fourth Way World

One of the most significant implications of the developments described here is that for the foreseeable future, we will be in a world where "privacy is local but processing

is global".[5] In other words, cultures and legal systems will be different between the economies in our region and across the world: acceptable use of personal information in one economy may not be acceptable in another, for example. On the other hand, the processing of personal information will be globalized. The "fourth way" will ensure that the original expectations that an individual has in a particular economy are respected and enforced no matter where the personal information is processed. No more (as happens in some parts of the world) and no less (as happens in many other places). These 'original expectations' have three important components: the protections in law in the individual's economy, the promises from the collecting organization, and the choices exercised by the individual.

APEC is uniquely focused on developing a framework that meets these expectations.

In their 2006 Annual Statement, APEC Ministers set out their vision for moving beyond simply drawing up the APEC Privacy Framework that they had endorsed the previous year, in order to see it implemented. In that Statement, they emphasized the need to ensure "responsible and accountable Cross Border information flows and effective privacy protection without creating unnecessary barriers". Ministers also "encouraged Officials to facilitate this goal by developing and disseminating implementation frameworks such as best practices for Cross Border rules".

In 2007, business and governments have cooperated to make very rapid progress in developing a "Choice of Approach" implementation model based on Cross Border Privacy Rules (CBPRs). They have also sought increasing consumer involvement. The implementation model that they have been developing for the Framework breaks new ground by moving away from the model dominant elsewhere that relies on the quarantining of personal data within a nation or region in order to protect individual rights. The fact that the APEC model recognizes that such quarantining can only be marginally effective in a highly globalized and networked age is of great significance for both international business and consumers. By shifting the emphasis from quarantine to enforcement at all points in the "data chain", the Framework has the potential to both ease the burden of regulatory compliance for businesses and to enhance real-world consumer data protection.

In this model, participating economies choose the entities and procedures that will be used within the economy to assess and enforce the compliance of an organization's (CBPRs) with the APEC Privacy Framework. The model will ensure the cross recognition of the chosen compliance entities and cross border enforcement of compliance with CBPRs, including investigation and resolution of consumer complaints. It is expected that implementation will commence in an APEC Pathfinder framework in 2008.

Conclusion

The privacy paradigms that took hold in the analogue world will need to evolve to take into account 'fourth way' thinking. Just as technology continues to change and information proliferates exponentially, laws and regulations and means of ensuring compliance will all need to be flexible enough to accommodate these trends. Policymakers will need to be mindful that laws promulgated in this area must be dynamic, and that technology will always outpace policy. The ultimate goal must be an atmosphere of trust by citizens and consumers without stifling innovation and efficiencies created by emerging technologies. This is indeed a tall order, but the creative thinking we've seen through the implementation of the APEC Privacy Framework is a very positive sign that dramatic progress is possible. The key moving forward will be securing a commitment by APEC Member Economies to implement pilot projects within the APEC Pathfinder Framework until a complete, effective and adaptable compliance framework is in place. ■

"Just as technology continues to change and information proliferates exponentially, laws and regulations and means of ensuring compliance will all need to be flexible enough to accommodate these trends."

[5] A phrase popularized by Marty Abrams, the Executive Director of the Center for Information Policy Leadership.