IDENTITY & ACCESS

Virtual Opportunity Congress IV Report

Queensland Parliament House

Brisbane • December 2006

Virtual Opportunity Congress IV

“Identity and Access”

Brisbane, Australia

30 November – 1 December 2006

For further information contact:

Global Access Partners Pty Ltd

53 Balfour St, Chippendale, Sydney NSW Australia 2008

Phone +61 2 8383 2416 Fax +61 2 9319 5754

Website www.globalaccesspartners.org

Table of Contents

Appendices:

Executive Summary

Virtual Opportunity Congress IV on Identity and Access, held at Queensland Parliament House on 1 December 2006, brought together key stakeholders from Government, Industry and Academia in a national debate on identity security.

The Congress, jointly hosted by Sydney-based policy network Global Access Partners (GAP) and the National Consultative Committee on Security and Risk (NCCSR), examined current progress in finding solutions to the fast growing problems of identity theft and data security. Over 100 participants led by keynote speakers including Special Minister of State the Hon. **Gary Nairn MP**, Queensland's new Attorney-General the Hon. **Kerry Shine MP** and Minister for Police and Corrective Services the Hon. **Judy Spence MP**, contributed to the discussion. Symantec's Chief Technology Officer **Mark Bregman** and Microsoft's Worldwide Industry Technology Strategist **Phil Stradling** added their unique industry perspective.

Virtual Opportunity IV focused on cross-sectoral responsibility in developing systems to curb cyber crime and fraud targeting passwords, pin numbers and computerised finances. Ten million Americans have their identity stolen every year[1] and a growing number of Australians are falling prey to fraudulent identity schemes.

The Congress spotlighted notable Government identity management initiatives and emphasised the importance of public-private partnerships in addressing online crime. The need for individuals to control access to their own data took centre-stage in the debate.

Key points of the discussion included the following:

- Emerging information technologies have created exciting opportunities in commerce, education and healthcare, but have also afforded new avenues for crime. Identity theft is an "increasing and insidious crime" costing Australia an estimated $3.5 billion per annum. It tarnishes the reputations of its victims, defrauds financial institutions and undermines public confidence in purchasing goods and sharing personal information online.

- Identity protocols established in the past are no longer applicable as centralised controls are overwhelmed by the viral, unpredictable and anonymous challenges of the internet. Citizens demand individually tailored and user-friendly identity solutions and the 'centre of gravity' will continue to tilt towards the individual user's demands, rather than the provider's convenience. If individuals, rather than banks or organisations, are asked to bear the brunt of the costs of identity theft, people's willingness to transact business online will be greatly reduced.

Javelin Strategy & Research, 2006 Identity Fraud Survey Report - www.privacyrights.org/ar/idtheftsurveys.htm

- Identity management and security projects have tended to be 'proprietary' in the past, with individual organisations developing their own incompatible schemes. ‘Federated Identity Management’ and standards based approaches involving partners working together to produce common standards and protocols, may be the way forward.

- A 'Trust Centre' would offer an opportunity to develop a common, secure and cost effective electronic identity verification system by vouching for someone's identity to a third party without disclosing additional information about them.

- The complex chain of identity protection is as strong as its weakest link and more secure government documents - driver’s licence, passports, birth certificates etc. – are required. Once stolen, digital identities can be forged in vast numbers compared to physical documentation.

- Australia has played a leading role in developing virtual technology, but new methods must be developed and adopted much more quickly today. Such protocols must be simple to use and cost effective to implement. Organised crime is not hampered by the need to outline new policy proposals or conduct post-operational assessments and so is continually a step ahead of bureaucratic enforcement agencies.

- The Department of Health and Human Services’ Access Card is a smart card designed to operate in a framework agreed by state and federal governments to assure compatibility with other systems and maintain high standards of privacy and usability. The Card embodies the difference between an identity card and an access card. It establishes the cardholder’s right to benefits, but is intended not to offer unnecessary information. Data held on people can be limited to the 'roles' they play in specific situations.

- Individuals should be able to lodge and control a variety of identity credentials with government and choose which they wish to use to access particular services. Citizens want to claim ownership of their own information, rather than such data being seen to be the property of the state.

- The opaque nature of identity technology invites public suspicion as to its efficacy and intention. IT allows a wide range of people to access data from diverse locations but also facilitates the tracking of exactly who accessed what information and when.

- The public's unwillingness to give organisations information is based on their fatigue with unnecessary intrusion as much as the fear of criminal exploitation. Consumers are being asked to provide time consuming identity checks, which they will soon reject if they fail to benefit from them. People cannot provide physical proof of identity such as driver’s licenses online, therefore the 'cyber world' requires new solutions, perhaps in the manner of the credit industry which relies on 'credit scores' compiled without specific interaction with the consumer.

- Consumers demand security usability, certainty of website identity, the provision of sufficient information to allow swift decision making and a reasonable number of steps to navigate any particular transaction. People learn to use computers and the internet by 'playing' with them, rather than reading books or taking courses, and ID management requires a similar approach with safeguards reducing the risks of failure and offering user friendly restitution.

- Co-operation between the public and private sectors, citizens and consumer protection bodies can create safe, reliable and trusted channels of communication. Clear contractual rules about who bears the risk when identities are misappropriated must be created. Governments must balance the competing needs of speed and efficiency with privacy and security, and victims of identity theft require better systems to re-establish their bone fides.

DISCLAIMER: This Report represents a wide range of views and interests of the participating individuals and organisations. Statements made during discussions are the personal opinions of the speakers and do not necessarily reflect those of the organisers and sponsors of the Congress.

(for the full Report of the Congress' proceedings, see pages 18-35)

The Steering Committee

The Steering Committee of Government and business executives worked over a few months on the Congress' objectives, topics for discussion and a continuity strategy, to ensure outcomes are achieved beyond the event.

The members of the Steering committee for Virtual Opportunity Congress IV on Identity and Access were (in alphabetical order):

Mr Keith Besgrove
Chief General Manager
Access & Consumer Division
Department of Communications,
Information Technology and the Arts,
Australian Government

Mr Patrick Callioni
Division Manager
Australian Government Information
Management Office, Department of
Finance and Administration, Australian
Government

Mr Malcolm Crompton
Managing Director
Information Integrity Solutions

Mr Michael Dupe
Branch Manager, Investments and Enabling
Projects, Australian Government Information
Management Office, Department of Finance
and Administration, Australian Government

Mr Peter Fritz AM
Managing Director
Global Access Partners (GAP)

Mr Peter Ford
Chairman, National Consultative
Committee on Security and Risk

Mr Chris Gration
Head of External Relations and
Compliance, Baycorp Advantage

Ms Erica Hughes
General Manager, Baycorp Advantage

Mr Martin Kaldor
Vice Chair, Australian Information
Security Association

Ms Catherine Martsch
Chief Executive Officer, Trust Centre

Mr Matthew Osborne
Principal Policy Officer, Law and Justice
Policy, Department of the Premier and
Cabinet, Queensland Government

Mr Greg Stone
Regional Chief Technology Officer
Microsoft Australia and New Zealand

Mr David Sykes
Vice President & General Manager,
Pacific Region, Symantec Australia

Mr Patrick Vidgen
Acting Deputy Director- General
Governance, Department of the Premier
and Cabinet, Queensland Government

Partners & Sponsors

Virtual Opportunity Congress IV on Identity and Access was coordinated by **Global Access Partners (GAP) Pty Ltd** – an influential network that initiates high level discussions on global issues, encouraging the sharing of knowledge, progress and policy change (*see App. 2, page 40*). GAP structures each initiative around the desired business outcomes of its partners and sponsors.

The Congress was co-sponsored by GAP's partners whose role extends beyond the event through membership in the **National Consultative Committee on Security and Risk (NCCSR)** - a powerful group of senior Government and business executives. The NCCSR was established following Virtual Opportunity Congress III on Security and Risk in 2003. Operating as a forum for high-level discussion and a platform for public and private partnerships, the Committee focuses on emerging issues in IT security, innovative policy options and industry projects with concrete economic outcomes.

Our thanks go to the following organisations (listed in alphabetical order) for their contribution and foresight:

- **Australian Government Information Management Office (AGIMO), Department of Finance and Administration**
- **Baycorp Advantage**
- **Microsoft Australia**
- **Queensland Government**
- **Symantec Australia**

(for more information on the sponsors of Virtual Opportunity Congress IV on Identity and Access, see App. 2, pages 38-43)

Keynote Speakers

The Congress took place over two days. Day One included the opening dinner (30 November 2006, River Room, Stamford Plaza Hotel), while Day Two consisted of two morning and two afternoon plenary sessions (1 December 2006, Legislative Assembly Chamber, Queensland Parliament House) under the following headings: **"Identity and Access: A Global Perspective"**, **"National and Government Initiated Identity Management: Opportunities and Directions for Further Development"** , **"Consumer Centric Identity Management: Opportunities and Directions for Further Development"** and **"The Way Forward for Australia"** (*for a full programme, see App. 1, pages 36-37*). Each session began with thought provoking addresses from the keynote speakers and continued as a dialogue between delegates in a 'think tank' mode.

The keynote speakers and session chairs of Virtual Opportunity Congress IV on Identity and Access were (in alphabetical order):

Mr Philip Argy
Senior Partner, Intellectual Property & Technology Group, Mallesons Stephen Jaques, President, Australian Computer Society

Mr Keith Besgrove
Chief General Manager, Access & Consumer Division, DCITA

Mr Mark Bregman
Executive Vice President & Chief Technology Officer, Symantec

Mr Patrick Callioni
Division Manager, AGIMO

Mr Michael Coomer
Group Executive, Business & Technology Solutions & Services, Westpac

Mr Malcolm Crompton
Managing Director
Information Integrity Solutions

Mr Peter Ford
Chairman, NCCSR

Mr Peter Fritz AM
Managing Director, GAP

Ms Erica Hughes
General Manager, Baycorp Advantage

Mr Chris Jordan AO
New South Wales Chairman, KPMG

Dr Audun Josang
Associate Professor, School of Software Engineering & Data Communication

The Hon. Gary NairnMP
Special Minister of State, Federal Minister responsible for e-Government

Mr John Rimmer
Partner, Joint Technology Partners, Co-chair NCCSR

The Hon. Kerry Shine MP
QLD Attorney-General and Minister for Justice

The Hon. Judy Spence MP
QLD Minister for Police & Corrective Services

Mr Phil Stradling
Global Industry Technology Strategist, Public Services and e-Government, Microsoft USA

Mr Paul Summergreene
Executive Director, Information Management Division, Queensland Transport

Mr David Sykes
Vice President & General Manager, Pacific Region, Symantec Australia

Ms Louise Sylvan
Deputy Chair, Australian Competition Consumer Commission

Mr Philip Argy

Philip Argy has been a partner of Mallesons Stephen Jaques for over 22 years. He qualified at the University of New South Wales for a Commerce (Information Systems) degree in 1975 and a Bachelor of Laws the following year. He is a barrister and solicitor of the Supreme Courts of New South Wales, the Australian Capital Territory, Victoria and Western Australia. Philip specialises in intellectual property, science, technology and competition law. He is a renowned strategist in both commercial negotiations and commercial litigation in areas as diverse as food and drug regulation; patent, copyright and trade mark litigation; outsourcing; electronic commerce and digital signatures. Philip is on the World Intellectual Property Organisation (WIPO) panel of arbitrators for the resolution of intellectual property disputes, especially those involving domain names. Philip was a member of the Federal Attorney-General's *Electronic Commerce Expert Group* and a member of the auDA Names Panel that prepared the domain name eligibility and allocation policy for the .au space. He was also a member of the auDA Competition Panel and chaired the Working Group that drafted the auDRP - Australia's domain name dispute resolution policy. Philip is National President of the Australian Computer Society and lectures extensively on subjects such as professionalism, risk management, electronic evidence and record retention and on intellectual property issues. He has appeared as an expert witness before Parliamentary hearings in relation to On-line Content Regulation, Cybercrime and Spam.

In 1996 Information Age nominated Philip as one of the 50 most influential people in Australia in the IT field, and he was awarded a ComputerWorld Fellow in 1997 for services to the IT industry. He is national Chairman of the eCommerce Committee of the Law Council of Australia, a Past President and founding member of the NSW Society for Computers and the Law, and a long standing member of the Australian Corporate Lawyers' Association. Philip is also a member of the NSW Law Society's Legal Technology Committee and he chairs the Webcast Committee of the International Technology Law Association.

Mr Keith Besgrove

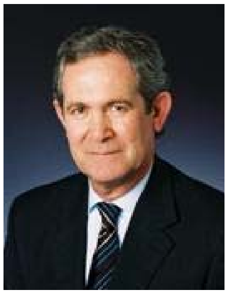
Keith Besgrove is the Chief General Manager of the Access & Consumer Division in the Department of Communications, Information Technology, and the Arts in Canberra. Keith provides advice to the Australian Government on strategic, legal and regulatory issues relating to communications and the information economy. His responsibilities include domain names, spam, consumer issues and broadband. He has been involved in various international groups including the OECD, APEC and ITU, and is the current chair of the OECD Working Party on Information Security and Privacy (WPISP). In recent years, he has also been responsible for research into the impact of ICT in improving productivity in Australia. Keith is fifty five years old, holds a Bachelor of Arts in Political Science from the University of Sydney and has two adult children. He is also a graduate of the Wharton School's Advanced Management program, and has completed an Australian Government Research Fellowship into innovation programs in Israel and Singapore.

Mr Mark Bregman

Mark Bregman is the executive vice president, chief technology officer of Symantec, responsible for the Symantec Research Labs, emerging technologies, architecture and standards, and developing the technology strategy for the company. He also guides Symantec's investments in advanced research and is responsible for the development centres in India and China. In addition, Mark leads the field technical enablement team, which works closely with the technical sales team to ensure they are prepared to assist customers in managing the impact of changing and emerging technical requirements. Mark Bregman joined Symantec through the company's merger with VERITAS Software. At VERITAS, he served as chief technology officer, responsible for cross-product integration, advanced product development, merger and acquisition strategy, and the company's engineering development centres in Pune, India and Beijing, China. He also served as VERITAS' executive vice president in charge of product operations since joining the company in 2002. Prior to joining VERITAS, Mark was CEO of Airmedia, a wireless Internet firm. Previously, Mark spent 16 years at IBM where he led the RS/6000 and Pervasive Computing divisions and held senior management positions in IBM Research and IBM Japan. He was also technical assistant to IBM CEO Lou Gerstner. Mark Bregman holds a bachelor's degree in physics from Harvard College and a master's degree and doctorate in physics from Columbia University. He also serves on the Board of Overseers of Fermi National Accelerator Lab. He is a member of the Visiting Committee to the Harvard University Libraries, a member of the American Physical Society, and a senior member of IEEE.

Mr Patrick Callioni

Patrick has degrees in Arts and in Law, he is a Barrister and a Fellow of the Australian Institute of Management, a Director of the Society for Knowledge Economics, and a Member of the Australian Institute of Company Directors and of the Chartered Institute of Purchasing and Supply (Australia). Patrick has presented and published papers on a variety of topics in recent years, including strategic management, value creation, performance indicators, and the information economy and knowledge management. Patrick has experience as a senior manager in program management, policy development, service delivery and corporate management - in health care, employment and training, income support and compensation, and information management. In Finance, Patrick's role is to oversee the management and strategic development of whole of government ICT infrastructure.



Mr Michael Coomer

Michael has over 30 years of experience at the forefront of information technology, having had associations in the telecommunications, financial services, aerospace and defence industries. Michael spent over 10 years with Rockwell International, working in numerous overseas roles, on large scale defence, aerospace and telecommunications projects. In 1987, he joined the Ansett Transport Industries Group and was appointed its Chief Information Officer in 1989. In this capacity, Michael had overall responsibility for the replacement of all of the Group's systems, including reservations, scheduling, telephone and many other operations systems, in anticipation of de-regulation in 1990. As IBM Australia's Head of Systems Integration, Michael helped create the very successful Lend Lease-IBM Joint Venture, ISSC Australia in 1993. From January 1995 until March 2000, Michael was the Chief Information Officer of the National Australia Bank, Australia's largest bank. In this role, he was responsible for the Group's IT activities in Australia, New Zealand, Europe, the US and Asia and oversaw the bank's transition into the Internet age. In January 2002, Michael joined Westpac Banking Corporation. He is the Group Executive for Business & Technology Solutions & Services with responsibility for information technology, outsourcing governance, all back-office operations and support, and corporate services. Michael also has group-wide executive responsibility for ensuring that Westpac's control frameworks against fraud, money laundering and the financing of terrorism are developed and monitored. Within his portfolio Michael also has group-wide responsibility for the provision of specialist business continuity services and physical security requirements. Michael is a Fellow of the Australian Institute of Management, the Australasian Institute of Banking & Finance, the Telecommunications Institute and the Australian Company Directors Institute. He is a non-Executive Director of Adev Advantage Limited. He is also a member of the J B Were Private Equity Fund.

Mr Malcolm Crompton

Malcolm Crompton is Managing Director of Information Integrity Solutions, providing high level advice to private sector and public sector organisations on building trust through excellent data governance, particularly in their collection and use of personal information. 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. Malcolm has established a global reputation for his forward thinking on the handling and governance of personal information and has been the invited speaker at many events in North America, Europe and Asia as well as Australia. Malcolm is also a member of the Microsoft Trustworthy Computing Academic Advisory Board, the global External Advisory Board of the IBM Privacy Institute, the Reference Group for the Privacy and Identity Management for Europe (PRIME) project and the Expert Advisory Committee on Information Technology of the Australian Medical Association. He is a member of a number of international privacy award judging panels. Between 1996 and 1999, he was Manager of Government Affairs in Canberra for AMP Ltd. In the previous 20 years, Malcolm held senior executive positions in the Federal Department of Finance, served as both a superannuation scheme trustee and scheme founder and worked in the Transport and Health portfolios. In 2004 he was awarded the inaugural Chancellor's Medal for distinguished contribution to the Australian National University. He has degrees in Chemistry and Economics.

Mr Peter Ford

Peter Ford provides consultancy services in privacy, security and related fields and is a member of the Australian Law Reform Commission's Advisory Group for review of the Privacy Act. Since June, 2006, he has also been a part-time Visiting Fellow at the ANU College of Law with responsibility for coordinating the law internship program. In July 2004, he retired from the position of First Assistant Secretary, Information and Security Law Division of the Australian Attorney-General's Department. The Division was formed in February 1997 and was responsible for policy relating to privacy, freedom of information, intellectual property, legal aspects of electronic commerce and support to the Attorney-General on national security, critical infrastructure protection and electronic surveillance aspects of law enforcement policy. Prior to that, he worked in areas of human rights, court administration, administrative law, freedom of information and constitutional law. As Divisional Head, he served as Agency Coordinator, a statutory position under the *Telecommunications Act 1991*, and also served on the Government Public Key Authority, the National Electronic Authentication Council, the Board of CrimTrac and the Privacy Advisory Committee. Between 2000 and 2003, Peter Ford chaired the OECD Working Party on Information Security and Privacy which, in 2002, produced the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. He also chaired the APEC Privacy Sub-Group, which produced the *APEC Privacy Framework* and was Vice-Chair of the APEC Electronic Commerce Steering Group with responsibilities for confidence and trust building measures until May 2004. He has published articles in the areas of privacy, human rights, telecommunications interception and constitutional law. Peter has a BA (Univ. of Qld.), LL.B. (Australian National University) and an M.Phil. (Glasgow).

Mr Peter Fritz AM

Peter Fritz is Managing Director of GAP, and Group Managing Director of TCG Group - a network of private, independent and mutually supportive companies which over the last 34 years has produced many breakthrough discoveries in computer and communication technologies. In 1993, some of the 65 companies in the TCG Group were publicly floated on the Australian Stock Exchange as TechComm Group Limited (now called Utility Computer Services UXC), with great success. Another former TCG company floated on the New York Stock Exchange in November 1997 for US$600m, making it the largest technology company to be established in Australia until that time. Peter's innovative management style and corporate structuring has lead to the creation of a business model which is being copied by many successful entrepreneurs, and has become part of university undergraduate and masters programs in business management in Australia and around the world. Peter Fritz chairs a number of influential government and private enterprise boards and is active in the international arena, including having represented Australia on the OECD Small and Medium Size Enterprise Committee. He is the holder of six degrees and professional qualifications, is a recipient of the Order of Australia, and has received many other honours.

Ms Erica Hughes

Erica joined the Baycorp Advantage Group in August 2005. She has extensive experience in implementing product, pricing and channel strategies to drive growth in market share, and in process re-engineering to support an improved customer focus. Erica and her team are currently developing leading solutions for Identity Verification and Fraud Prevention for Financial Services clients. Previously, Erica held several senior management roles, primarily in a credit risk and product management capacity, in the financial services sector with National Australia Bank and Westpac and as Head of Consumer Banking (Personal Financial Services) at ANZ. Erica has a BA in Applied Finance and Investment.

Mr Chris Jordan AO

Chris has a BCom, LLB from the University of New South Wales and a Master of Law from Sydney University. He is a Fellow of the Institute of Chartered Accountants in Australia, a Fellow of the Taxation Institute in Australia and a Fellow of the Australian Institute of Company Directors. Chris was awarded the honour of Officer of the Order of Australia in the 2005 Queens Birthday Honours list and was awarded a Centenary Medal in 2001. Chris is the Deputy Chairman of the Board of Taxation which is an advisory body to the Federal Treasurer, Peter Costello. He is a member of the Sydney Children's Hospital Foundation Board which supports the operation of the Sydney Children's Hospital at Randwick in Sydney. Chris has also been appointed by the NSW Minister for Tourism and Sport and Recreation, Sandra Nori, to the Games Advisory Committee of the Sydney 2009 World Masters Games. He is a member of the Board of the Bell Shakespeare Company. Chris Jordan led the KPMG team which prepared the business case for the Department of Human Services on the health and social services access card.

Dr Audun Josang

Dr Audun Jøsang is Associate Professor at the Faculty of IT at QUT in Brisbane. His research focuses on ID management and online trust management. It is becoming evident that poor usability of current identity management systems causes serious security vulnerabilities despite strong cryptography and two-factor authentication being used. Prof Jøsang is therefore working on user-centric identity management models that provide excellent usability and privacy in addition to strong security. Deciding who can be trusted in the online world is becoming more and more difficult. Prof Jøsang is also working on online trust management solutions in the form of reputation systems and trust engines. In particular Prof Jøsang is well known worldwide for the development of belief reasoning with subjective logic that is ideally suited for analysing transitive trust networks. Before joining QUT in 2005, Prof Jøsang was the Research Leader of the Security Unit at DSTC in Brisbane. He has also been Associate Professor at the Norwegian University of Science and Technology (NTNU), Senior Research Scientist in Telenor R&D in Norway, and telecommunications System Architect in Alcatel Bell in Belgium. Prof Jøsang has a BSc in Telecommunications from the Norwegian Institute of Technology, a MSc in Information Security from Royal Holloway College in London, and a PhD from the Norwegian University of Science and Technology.

The Hon. Gary Nairn MP

The Hon Gary Nairn MP, the Special Minister of State and Federal Member for Eden-Monaro, has portfolio responsibility for the implementation of e-Government in Australia. As a Minister within the Finance portfolio, Mr Nairn's responsibilities also include Ministerial and Parliamentary Services, the Australian Electoral Commission, government advertising and a number of Government Business Enterprises including Film Australia, Film Finance Corporation and the Defence Housing Authority. Mr Nairn was elected to the House of Representatives in 1996, winning the New South Wales seat of Eden-Monaro which he has held since. Prior to this, Mr Nairn was Parliamentary Secretary to the Prime Minister with key responsibility for the implementation of the National Water Initiative and the administration of the National Security Science and Technology Unit within the Department of Prime Minister and Cabinet. Prior to entering politics Mr Nairn was Managing Director of his own survey and mapping business that, between 1983 and 1996 operated in the Northern Territory and later in Queanbeyan, New South Wales.

Mr John Rimmer

John Rimmer is a senior strategist with a long history of policy innovation, corporate governance and senior executive roles. He now serves as a Board member on public sector and private companies. John was until February 2004 the Chief Executive Officer of the Australian Government's National Office for the Information Economy. Between 1997 and 2000 he undertook a range of consulting and non-executive Board appointments. Until 1997 he held leadership positions in Victorian Government Health, Premier's and State Development portfolios. John has particular strengths in identifying and analysing corporate strategies. His judgment and corporate governance skills make him an excellent board member and advisor to boards in both the public and private sectors. He has a well developed understanding of government and health services, intergovernmental relations, community development and the strategic impact of information and communications technologies. Most recently the focus of his attention has been on the drivers of innovation in Australian firms and the alignment of business strategy and information technology investments in complex organisations. In a voluntary capacity John is actively involved in swimming sports, until recently as President of a successful swimming club and now as a technical official in Swimming Victoria.

The Hon. Kerry Shine MP

Queensland's new Attorney-General and Minister for Justice Kerry Shine was sworn in on 1 November 2006. Mr Shine had served as the Minister for Natural Resources and Water since the re-election of the Beattie Government in September. Mr Shine also has the responsibility as the Minister Assisting the Premier in Western Queensland. Prior to the September 2006 State election, Mr Shine had served as Parliamentary Secretary to the Minister for Communities, Disability Services and Seniors and Premier's Advisor on Western Queensland from 28 July 2005. Mr Shine was elected to State Parliament in February 2001 as the Member for Toowoomba North. Prior to entering Parliament, Mr Shine was a solicitor. He commenced a firm in his home town of Toowoomba in 1976.

The Hon. Judy Spence MP

Judy Spence entered politics in 1989 as the Labor Member for Mt Gravatt and is now Queensland's longest serving female MP, as well as the State's first female Police and Corrective Services Minister (2004 to date).. Before entering politics Judy was a high school teacher, first posted to Calen, before returning to South-East Queensland to marry. She then taught at Woodridge, Beenleigh and Browns Plains. In 1996 Judy was appointed Shadow Minister for Consumer Affairs and Women and Adviser to the Leader of the Opposition on Federal/State Relations. From December 1996 to June 1998 Judy was the Shadow Minister for Women, Aboriginal and Torres Strait Islander Affairs and Consumer Affairs. When Labor won Government in July 1998, Judy was sworn in as the Minister for Aboriginal and Torres Strait Islander Policy, Women's Policy and Fair Trading. As the Minister for Fair Trading, Judy oversaw legislation to crackdown on scams, as well as strategies to raise community awareness. She also had responsibility for the Building Services Authority and the Residential Tenancies Authority. In the Beattie Government's second term, Judy was the Minister for Families, Disability Services, Seniors and Aboriginal and Torres Strait Islander Policy. During that time she gained further insight into police work while exposing the failings of the State's child protection system, expanding domestic violence protection to more Queenslanders, oversaw the operation of the State's two youth detention centres - in Brisbane and Townsville - and administered the Juvenile Justice Act. Judy also brings her understanding of Indigenous issues and the complex needs of people with disabilities to the Police and Corrective Services portfolios.

Mr Phil Stradling

Phil is responsible for shaping strategy and solutions that address the goals of government agencies around the worldwide. Prior to this role, Phil spent 10 years as a senior strategy consultant in the UK working with a variety of government agencies and driving initiatives focused on e-government infrastructure and e-government services. Among his more noteworthy achievements Phil was a major contributor to the conception and development of the UK Government Gateway, initiating the use of XML and a cross-government interoperability framework, and championing new ways of delivering e-services through partners. Most recently Phil established and led an identity management Team across the various product groups of Microsoft which spearheaded the adoption of Next Generation Identity & Access across Public Sector.

Mr Paul Summergreene

Paul Summergreene is currently the Executive Director of Queensland Transport's newly formed Information Management (IM) division where he directs a team of 400 staff and manages an annual budget in excess of $1.9b. Queensland Transport's IM Division is responsible for delivering Information and Communication Technology (ICT) services to over 8,300 internal customers throughout Queensland. Paul is also accountable for the provision of Corporate Financial services and Information Management across the department. Paul and his team are acknowledged ICT leaders within Queensland Government and in the delivery of information management solutions. Some of their achievements include: Service Orientated Architecture (SOA) – QT was the first in the world to implement an SOA (1997) and has been recognised by IBM for its advanced planning and architecture management practices; Generic Payment Service (GPS) – The first online payment system in Queensland Government was implemented by QT in 2001. Since then it has been used to deliver all of QT's online payment services and has processed over $100m in transactions; Consultancy to Fijian Government – QT is providing ongoing assistance to the Fiji Land Transport Authority in their implementation of an Integrated Network Data Access system. Paul's 29 years of Queensland Government experience has recently broadened to encompass the role of Project Director for implementing the New Queensland Driver License (NQDL). The NQDL will place Queensland at the international forefront in delivering a secure licensing system using innovative technology that will improve licensing security, service delivery and reduce fraudulent activity. Rollout of the 2.8 million smart card driver licenses will begin with a pilot in late 2008 and scheduled to be completed by 2011.

Mr David Sykes

David Sykes is Managing Director and Vice President of Symantec's Pacific region encompassing Australia, New Zealand and the Pacific Islands. He is responsible for driving Symantec's sales and business development in the region and serves as senior leader for the overall Symantec business in the Asia Pacific & Japan. Prior to this role David served as Senior Director of Enterprise sales for Asia Pacific. Based in Hong Kong, he was responsible for the sale and delivery of Symantec's high-end integrated security solutions to Symantec's largest customers across all segments of government, industry and commerce. David has been with Symantec since 2000, when he was appointed sales director for Australia. David later assumed the role of director for North Asia, guiding and contributing to Symantec's success in the enterprise and consumer markets of Korea, China, Taiwan and Hong Kong. David joined Symantec from Computer Associates, where he held a number of senior positions, including Australian general manager and New Zealand managing director. Prior to Computer Associates, David spent 8 years in a variety of sales and finance roles with companies such as Digital Equipment and BHP. He participates in several industry associations and provides pro-bono advice to charities and non-profit organisations. David is a member of the Australian Institute of Company Directors and has a Bachelor of Commerce with Accounting and Law from the University of Newcastle.

Ms Louise Sylvan

Louise Sylvan is Deputy Chair of the Australian Competition and Consumer Commission, appointed as the member with expertise in consumer affairs. She was formerly the CEO of the Australian Consumers' Association, and served on the Executive of Consumers International for three years as President. Louise is well known nationally and internationally for her work in enhancing consumer empowerment and protection in a range of areas such as health, food safety issues, financial services, as well as in competition and consumer policy. Her strong impact on the issues of the day was recognised in her inclusion as one of Australia's 20 True Leaders in 2002 by the Australian Financial Review's BOSS magazine. Currently, Louise is part of Australia's delegation for the OECD's Consumer Policy Committee and the International Consumer Protection and Enforcement Network (ICPEN), serves on the Australian Statistics Advisory Council to the ABS and was a member of the global Steering Group which is formulated the Intellectual Property Charter. Prior memberships included six years on the Australian Prime Minister's Economic Planning Advisory Council and the Self-Regulation Task Force in 1999-2000. Louise has a BA and MPA from universities in her original homeland of Canada and immigrated to Australia in 1983.

Participating Organisations

Participation in each GAP Congress is by invitation only. The Congress is attended by the top echelon of government and industry. Delegates from the following 58 organisations participated in Virtual Opportunity Congress IV on Identity and Access (*for the full list of delegates, see App. 3, pages 44-48*):

- Advisory Group for the ALRC review of the Privacy Act
- Attorney-General's Department, Australian Government
- AusCERT (Australian Computer Emergency Response Team)
- Australian Centre for Health Research
- Australian Competition and Consumer Commission
- Australian Computer Society
- Australian Crime Commission
- Australian Federal Police
- Australian Government Information Management Office, Department of Finance and Administration
- Australian Information Security Association (AISA)
- Australian Medical Association
- Australian Postal Corporation
- Australian Taxation Office
- BankID, Sweden
- Baycorp Advantage
- Business Review Weekly
- Cisco
- Deloitte Touche Tohmatsu
- Department of Justice and Attorney-General, Queensland Government
- Department of Communications, Information Technology & the Arts, Australian Government
- Department of the Premier and Cabinet, Queensland Government
- Dragonfly Technologies Pty Ltd
- Fairfax Business Media
- Queensland Police Service
- GE Money Australia & New Zealand
- Hannover Fairs Australia
- HSBC Bank Australia Limited
- IBM Software Group
- IdentityPoint Pty Ltd
- Information Integrity Solutions
- KPMG
- Lenovo (Australia & New Zealand)
- Lockstep Consulting Pty Ltd
- Macquarie University
- Microsoft ANZ
- Microsoft Corporation, USA
- National Australia Bank Ltd
- National Consultative Committee on Security & Risk
- Neoteck Business Solutions
- NSW Department of Lands
- Office of the Chief Information Officer, Government of Victoria
- Office of the Hon. Gary Nairn MP, Special Minister of State
- Office of the Hon. Judy Spence MP, Queensland Minister for Police & Corrective Services
- Office of the Hon. Kerry Shine MP, Queensland Attorney-General and Minister for Justice
- Privacy NSW
- Queensland Government Chief Information Office
- Queensland Transport
- Queensland University of Technology
- Smart Internet Technology CRC
- St George Bank
- Symantec Australia
- Symantec USA
- TCG Group
- Telstra Corporation
- Trust Centre
- University of Ballarat
- Westpac Banking Corporation

Report of the Congress Proceedings

The key points made by each speaker are outlined below. Full transcriptions of the speeches are available on request from GAP.

Ms Erica Hughes

General Manager, Information Services and Solutions, Baycorp Advantage

In her introductory address, Ms Hughes discussed the need to balance processing efficiency and information privacy, as laid out in the OECD principles, in the light of the exponential growth of data stored in electronic media.

> "In 2003 Australia had 36,000 terabytes of digitally stored data, a figure expected to grow to 176,000 terabytes in 2007. One terabyte is the equivalent of 500 million pages of typed A4 paper. 800 megabytes of information is produced every year for each person on the planet and modern technology allows this information to be networked globally and instantaneously. Establishing identity is the key to managing and protecting that information."
>
> **Erica Hughes**

Though consumers, business and government demand better control of data access, and government and business share an interest in stronger identity management, consumers may not yet see the case for adopting identity management technology. Innovation has been beleaguered by false starts and consumer uptake of optional enhancements that only a has been slow, despite the heavy investment of banks in better security protocols.

Ms Hughes highlighted the difficulty of regulating networks which offer public benefits but which incur private costs. She pointed out the high start-up costs of such networks, but also their potential for rapid growth after the attainment of 'critical mass', and stressed synergy of government regulation and business investment can bring new networks to this crucial take off point.

She envisaged a future market characterised by consumer, business and government confidence in which the control of risk is shared between identity issuers, consumers and identity users. She stressed the role of private firms such as Baycorp in making this vision a reality.

The Hon. Kerry Shine MP

Attorney-General and Minister for Justice, Minister Assisting the Premier in Western Queensland, Member for Toowoomba North Queensland Government

Mr Kerry Shine outlined the intention of the Queensland Government to create a new offence of 'identity theft' to allow law enforcement agencies to counter this "increasing and insidious crime". The new offence will allow agencies to act against credit card skimming before financial fraud is committed, with a maximum penalty of three years imprisonment.

He traced the impact of such crimes, from a Brisbane woman driven into bankruptcy after a fraudster ran up bills of $10,000 using her lost driving license, to a 2003 study which estimated the worldwide cost of such fraud to be a "staggering $2 trillion."

New information technologies have opened up opportunities in commerce, education and healthcare and greatly enhanced the ability of government to deliver services in decentralised states, but have also afforded criminals new opportunities to commit crime. In this new environment governments must balance the competing needs of speed and efficiency with privacy and security.

Mr Shine believed that service delivery and privacy protection need not be mutually exclusive, and praised the cooperation of Commonwealth, state and territory agencies in developing the National Identity Security Strategy and the proposed Commonwealth Government Access Card.

He recognised the frontline role of the Registries of Births, Deaths and Marriages and said the Queensland Registry will soon join the certificate validation service to provide online verification of births and changes of name. Introducing a new 'Smart' driver's licence to replace the current laminated card will increase security and allow licence holders to access government services and view their details via a personal identification number.

Session 1 - "Identity and Access: A Global Perspective"

Mr Michael Coomer

Group Executive, Business and Technology Solutions and Services
Westpac Banking Corporation

Mr Coomer estimated the annual cost of identity theft in Australia at $3.5 billion a year, one fifth of the sum spent on commercial information technology.

He pointed out the insidious and vicious nature of such crimes in tarnishing the reputations of their innocent victims and defrauding financial institutions. Victims of identity theft are often required to go through an expensive and frustrating "extraordinary process" to prove their innocence and this erodes trust in the whole system.

Although Banks have been working to increase customer awareness of computer, credit card, document and internet security issues, the biggest challenge facing Westpac was 'social engineering' - the collection of techniques fraudsters use to manipulate well meaning people into providing confidential information. Unisys' quarterly security index records identity theft as the chief concern of Australians, ahead of war and terrorism. Identity fraud damages corporate reputations and may lead to a loss of consumer confidence in new technologies, undoing a decade of work by government and business to encourage electronic data transfer.

> "Identity theft is one of the fastest growing crimes in Australia and it's costing the country an estimated $3.5 billion a year. That's about 20 per cent of what Australian companies spend on information technology on a yearly basis."
>
> **Michael Coomer**

Trust and security are the foundation of financial services, security being the means by which the goal of trust is achieved. Customers willingly provide banks with confidential information to preserve their vital assets and it is vital that this information is protected, using techniques such as dual factor authentication and, in the future, biometric data and perhaps voice recognition.

Mr Coomer highlighted Westpac's role in convincing the government not to risk identification standards and trust in the financial sector in drafting new anti-money laundering legislation, but praised the government's role in promoting co-operation to 'close the loop' on identity fraud. He said the industry needed to 'raise its game' and develop a similarly coordinated industry-wide approach to ensure the best outcome for customers.

"The percentage of Australians concerned about misuse of personal information stands at 59 per cent, with war and terrorism trailing by 7 per cent."
Michael Coomer

A collaborative response to criminals combining to commit fraud is vital and an international template for action might be the Swedish bank trust network which allows digital certificates issued by one bank to be used by that bank's customers to access government services.

A number of Australian banks are discussing such a scheme, but Mr Coomer advocated defining the nature of the problem before 'throwing technology' at its solution. ATM and EFTPOS networks were constructed individually, but a shortage of time and capital means a joint solution must be developed now.

A 'Trust Centre' would offer an opportunity to develop a common, secure and cost effective electronic identity verification system. This would offer both security and efficiency, though plans for such a centre are still at the conceptual stage in terms of common infrastructure and standards and its role in acting as a clearing house for access to federal data bases.

The challengers of cheque and credit card fraud have largely been overcome by the banking industry, and identity theft can be defeated by a similar process of collaboration and the sharing of best practice. Identity protection is as strong as its weakest link and more secure government documents - driver's licence, passports, birth certificates etc – are required.

A trust centre would increase individual security and alleviate community concerns while reducing the need to carry a host of ID and would act as a central point for the reporting of fraud and identity theft.

The trust centre would minimise duplication of identification processes leading to reduced costs for the banking sector and close loopholes which criminals currently exploit. This in turn would bolster Australia's reputation as a safe place to bank and transact, providing more economic benefits for the country.

He stressed that it would not be a version of the national ID card, an idea rejected by the Australian public.

Mr Coomer stated his support for Joe Hockey's Access Card initiative and praised its focus on providing efficient access to government benefits while ensuring that only those entitled to those benefits obtain them. He believed this initiative could form an important plank in the development of electronic identification aspired to in the AML legislation.

The trust centre could provide an independent way of verifying primary documentation to allow both parties to transact online with greater confidence and provide an opportunity for the government and the banking industry to work together on online verification and authentication.

Mr Keith Besgrove

Chief General Manager, Access & Consumer Division, Department of Communications, Information Technology and the Arts
Australian Government
Chair, OECD Working Party on Identity Management

In discussing a number of identity management projects undertaken worldwide, Keith Besgrove noted that governments have a strong historical involvement in traditional identity management through issuing birth certificates, passports and providing border control and are increasingly concerned with digital identities. He remarked that the most successful schemes are coordinated across tiers of government in collaboration with the private sector.

He focused on Scandinavia, praising Denmark's 13 year old e-Health portal for administering electronic patient files for over 1.2 million Danish citizens. Danes can now access their medical records through their personal page on the portal and see their diagnoses, operations and examinations under the heading 'My Treatments in Hospital'.

For over a year Danish Police have had a virtual police station, a place where citizens can report crimes and help the police follow up on matters.

The Danes are set to follow the Norwegians in offering every citizen a personal 'my page' for government interaction, while the Finns have a comprehensive network of online services requiring secure IDM solutions including property registries.

> "Finland is very well advanced in IDM and e-services; it's had an ID card since 1999; transacting online is a way of life in Finland. A survey of e-government services in April 2006 found that the most popular websites in Finland are actually those of local authorities."
>
> **Keith Besgrove**

Mr Besgrove mentioned the OECD Working Party on Identity Management in which such international experience and best practice could be shared.

Discussion

Paul Ashley, IBM Software Group, noted that Identity Management and security projects had tended to be 'proprietary' with individual organisations developing their own incompatible schemes. He saw 'Federated Identity Management', with partners working together to produce common standards and protocols, as the way forward.

Michael Coomer agreed that banks in particular had locked their customers into their organisation to protect their data, but that today's tendency towards individuals employing multiple identities through card based technology was making this untenable.

Philip Argy, Australian Computer Society, pointed out that competing technologies each had their own standards and that a drive towards uniformity might preclude better options for the future. He stressed the need to encourage a variety of alternatives without sacrificing the need for interoperability.

Michael Coomer agreed on the need to examine solutions based on legislation, education and behavioural standards before simply 'throwing technology' at the problem.

Keith Besgrove noted that criminals had exploited the public's fondness of personal social engagement through one on one 'phishing' to circumvent impersonal security barriers.

Michael Coomer praised the leadership of the federal government in this area, but warned against 'railway gauge problems' in a federal, decentralised nation.

Dr Audun Josang, Associate Professor at QUT, confirmed that Federated Identity Management does allow multiple identities and is particularly useful where related organisations wish to bundle services together.

Peter McNally, KPMG, questioned the willingness of global banks and international organisations to change their established practices in order to meet future Australian standards.

Keith Besgrove acknowledged this as a problem, but stressed Australia's leadership role in setting standards in these areas, along with the UK, Scandinavia and Korea.

Prof Bill Caelli, Information Security Institute at QUT, agreed that Australia could take the lead, and offered EFTPOS as an example of a national innovation which helped set International Standards through co-operation with international groups such as OECD and the International Federation for International Processing. He said the Motor Vehicles Standards Act could act as an example, with government setting the standards which manufacturers were free to meet in whatever way they choose. The problem was not establishing the identity of the claimant and verifier, but the security of the channel through which they communicated.

Prof Vijay Varadharajan, Macquarie University and Microsoft Chair Professor, observed that maintaining trust, rather than establishing identity, was paramount and that the problem was not setting standards but ensuring compliance with them. He agreed on the importance of securing channels of communication.

Michael Coomer agreed that Australia had played a leading role in developing similar technology in the past, but stressed that new methods had to be developed and adopted much quicker in today's fast moving technological environment. They had to be simple to use and cost effective to implement.

James Kelaher observed that high speed Broadband has only been widely adopted in the last two years, and that broadband encourages internet use which in turn invites fraud. He noted that consumers are being asked to provide time consuming identity checks which they will soon reject if they fail to benefit from them. He wanted to see more 'trusted' sites as at present people were being asked to credential themselves in tedious ways with no guarantee that the site they were accessing was genuine.

Michael Coomer said that savings from preventable fraud created a strong business case for banks to build their own identity infrastructure and that costs could be reduced by creating a shared system.

Michael Gill from Cisco observed that secure sharing of information was vital to improve the speed and quality of health care.

Graham Ingram, General Manager of AusCERT, acknowledged the complexity of the problem and promoted 'trust federations' as a possible solution.

Session 2 - "National and Government Initiated Identity Management: Opportunities and Directions for Further Development"

The Hon. Gary Nairn
Special Minister of State
Federal Minister responsible
for e-Government,
Australian Government

Mr Gary Nairn outlined a number of government schemes to increase electronic participation, including trials to allow electronic voting for the visually impaired and military personnel serving overseas.

'E-government' should allow citizens to connect more easily with government services. Mr Nairn praised the work of the Australian Government Information Management Office in this regard. He outlined the 'e-Government Strategy Responsive Government and New Service Agenda' and reiterated the goal of 'australia.gov.au' becoming a fully functional online service point with individual user accounts for citizens and simple access to government services including prepopulated forms. Citizens would be presented with a single government brand and solution.

Mr Nairn also favoured the 'spatial enablement' of government, by using mapping techniques to identify where resources were needed regarding health, education, business and the environment.

The Health and Human Services Access Card is a smart card designed to operate in a framework agreed by state and federal governments to assure compatibility with other systems and maintain high standards of privacy and usability. Although the use of biometric options to protect users' online identities and the adoption of the Access Card did provoke some debate about privacy issues, Mr Nairn said the success of social networking sites such as 'MySpace' showed that young people did not see data privacy as a major problem. Indeed people may expect government to share information if it reduces risk of injury or loss in case of bush fires, cyclones and floods, and would not understand if privacy legislation prevented the sharing of such data. He hoped that citizens would be able to give permission for their addresses and mobile phone numbers to be given to emergency organisations so they can be contacted automatically in extremis.

> "If we look at the generations X and Y and their readiness to put all sorts of personal information on to social networking sites such as MySpace and YouTube, there certainly doesn't seem to be the concern about privacy that some people would portray."
>
> **The Hon. Gary Nairn**

The percentage of the population contacting the government online has risen from 14% to 19% in a year, and when this figure reaches 30-40%, the ramifications for government will be profound. People expect instant service online, and engines such as ACT based RuleBurst may enable automated support in decision making based on legislation and associated regulations.

Mr Nairn underlined the Australian Government's commitment to Identity Management as more citizens chose to interact online. He favoured building on existing systems in agencies and the private sector and said the framework 'Identity Management for Australian Government Employees' (IMAGE) will seek a common approach across agencies in the short term and eventually allow for identity credentials to be cross-recognised across government. He singled out Centrelink is a pioneer agency for IMAGE.

He supported the often expressed idea that individuals should be able to lodge and control a variety of identity credentials with government and choose which they wished to use to access particular services. Although not endorsing a centralised database of comprehensive personal data, Mr Nairn favoured rationalising the current confusing plethora of ID to minimise redundant processes and increase the reliability and security of data. He supported the establishment of national standards for handling the electronic exchange of names and addresses and the use of commercial third parties to authenticate identities.

He expressed the government's intention to help victims of identity theft re-establish their bone fides though the creation of a consolidated list of identity registers.

The Council of Australian Governments has agreed to a national approach to identity security and the Australian Government Information Management Office is working on related matters with the Attorney-General's Department, Defence Signals Directorate and the Department of Communications, Information Technology and the Arts under the banner of the e-Security National Agenda.

Mr Paul Summergreene
Executive Director
Information Management Division
Queensland Transport

Mr Paul Summergreene discussed the new Queensland Driver Licence Project in terms of fraud, privacy, technology, procurement and services.

This 'smart card' will be introduced in late '08 to replace a simple card which is vulnerable to fraud. It will affect 2.8 million people in Queensland, 85 per cent of the adult population, and be a qualitative improvement on other state's licence provision. It is being produced in a Public/Private Partnership.

Queensland's TRAILS (Transport Registration and

Integrated Licensing System) is a mainframe system which holds records of external customers in Queensland Government. It is Service Orientated Architecture, enabling every component to be broken down and delivered in a different mechanism. The Card is designed to be 'open standard' and adaptable to other uses in the future. It will feature holograms and an embedded chip.

> “Any technology architect worth their salt, in my opinion, who would design a system that wasn’t open standard and adaptable, would not be doing their job appropriately.”
> **Paul Summergreene**

Mr Summergreene discussed the necessity of creating common standards across Australia, maintaining privacy and linking the system to the Births, Deaths and Marriages registry to improve the integrity of the data. The information given on application will be checked to ensure its accuracy before the card is issued.

Scandinavian countries introduced 'person numbers' in the early seventies with strong privacy safeguards. This unique identifier is used instead of a plethora of different cards.

Discussion

Philip Argy argued that cards such as the Queensland Driver Licence could protect privacy by offering less, rather than more, information, and questioned the need for the card to do more than establish the holder's entitlement to drive a car under Queensland law. The Human Services Access Card embodies the difference between an identity card and an access card. It establishes the cardholder’s right to benefits, but does not offer unnecessary information beyond that.

Shelley Oldham, Director of Transformation for the Victorian Government, discussed various identity projects including Directions Plus at the Commonwealth Games, the KPMG Health and Access Card Report and the Transport Ticketing Authority, and highlighted difficulties caused by discord between state and federal governments.

Warwick Watkins, NSW Surveyor General and Chair of the Australia New Zealand Land Information Council, explained the significance of the Land Titles office to the functioning of the economy and the importance of establishing identity and authentication within it.

> “When you consider that 70 per cent of properties across Australia on average are mortgaged, I’d say that the economic and social framework for Australia is underpinned by the property.”
> **Warwick Watkins**

Graham Fletcher of IBM advocated the use of SIM cards, packaged with a battery, Smart Card reader and pin pad, for the new driving licence, a suggestion **Paul Summergreene** said had been considered and rejected. He reiterated his commitment to new technology, but stressed that the information held on the card, rather than the nature of the card itself, was the priority.

Gary Nairn agreed that technology could allow citizens to engage in two way interaction with government bodies.

John Rimmer observed that secure two-way communication allowed such interaction between citizens and the tax office.

Prof Bill Caelli of QUT ISI warned that Smart Cards were prone to fail in conditions of high humidity.

Stephen Wilson from Lockstep was optimistic about the potential for technology to preserve privacy. Identities based on number codes were insecure when used online, but SIM cards and similar devices could be used to authenticate them.

Julia Nesbitt from the AMA disputed the assertion that technology necessarily delivered privacy and security.

> "I think the statement that you own the card is a meaningless statement. It means nothing in terms of privacy until we understand what the governance and management strategies around the card and the information are."
>
> **Julia Nesbitt**

Other speakers observed that the opaque nature of such technology invited public suspicion as to its efficacy and intention and allowed a far wider range of people to access it from diverse locations. It was also noted that IT allowed the tracking of exactly who accessed what information and when and so actually increased security.

Graham Ingram from AusCERT pointed out that information was vulnerable to criminal activity when it was moving between relatively secure cards and databases over the internet. Criminals paid no regard to privacy laws and jurisdictions.

Greg Stone, Regional Technology Officer for Microsoft, believed that 'honey pots' of information would inevitably draw criminal activity and that minimising the amount of data which could be lost and maximising the citizen's involvement in the process, e.g. in controlling his own access card, was paramount.

Speakers advocated the rationalisation of Australia's historically chaotic and complex system of identity checks. Technology to check identities would be fatally flawed if identities could not be properly established in the first place.

Nicole Waterson of the Queensland Department of Justice advocated the creation of a 'privacy culture' in organisations rather than ad hoc technological solutions. Organisations such as Centrelink might have excellent privacy controls on paper, but this had not prevented a number of their employees abusing the privacy of citizens in the past.

Lynda O'Grady from Telstra said citizens wished to claim ownership of their own information, rather than such data being seen to be the property of the state.

Prof Bill Caelli advocated seeing people as playing roles – e.g. of driver, patient or passenger – and said the data held on them should be limited to the roles they play in those specific situations.

Lunch Session

Mr David Sykes

Vice President & General Manager
Pacific Region, Symantec Australia

In introducing guest speaker Phil Stradling, David Sykes explained Symantec's leading role in protecting computer users from online threats through safeguarding infrastructure, information and interactions and the paramount role which the establishment of identity plays in IT security.

> "Symantec today protects more people from more online threats than any other organisation on the planet. And when we look at protection, we think about it in three ways - protecting the infrastructure, the devices and the network."
>
> **David Sykes**

Mr Phil Stradling

Global Industry Technology Strategist
Public Services and e-Government
Microsoft Corporation, USA

Phil Stradling noted that people are replicating many aspects of their personal and work lives in the virtual environment. It was vital to establish trustworthy identities 'online', but new technology had changed historically stable relationships between people and organisations in the real world. He advocated the creation of an 'ecosystem' of identity providers to build trust in a variety of specific scenarios, with organisations subcontracting the burden of validation to specialised public bodies and new private firms.

The internet is not controllable through a top down autocracy, and interactions involving consumers, citizens, enterprises and governments now blend in new and unique combinations. He differentiated between identities issued by banks and governments, and those established by users of such websites as eBay.

> "I think the biggest thing that identity management experts and analysts have learnt from eBay is the importance of reputation and credentials and how well they work."
>
> **Phil Stradling**

He outlined the growth of computer technology from isolated mainframes to today's integrated wireless internet and warned that identity protocols established in the past were no longer applicable today as centralised controls were overwhelmed by the viral, unpredictable and anonymous challenges of the internet. He recounted the commercial failure of proposed bank issued smart cards in the UK due to funding issues.

He believed the rise of the 'me' culture would see citizens demanding individually tailored and user-friendly identity solutions and that the 'centre of gravity' would continue to tilt towards the individual user's demands, rather than the provider's convenience.

The growth of download speed, storage capacity and processor capability creates the possibility of large numbers of people simultaneously immersing themselves in 'virtual worlds', and establishing the identity of one's companions there may become an important issue.

Employment relationships are changing, with ever more people juggling home, consultant and client roles throughout their working day. This creates a patchwork of identity needs that span consumer, private and public enterprises, and their complicated and insecure nature threatens the benefits such 'liquid' technology should bring.

Secure networks already facilitate military co-operation, and similar systems could revolutionise identity management for all.

Session 3 - "Consumer Centric Identity Management: Opportunities and Directions for Further Development"

Malcolm Crompton

Managing Director
Information Integrity Solutions

Malcolm Crompton saw better Identity Management as a necessary facilitator for improved standards of service and convenience. He advocated 'Consumer Centric Identity Management' and observed the willingness of people to volunteer personal information in return for real benefits on sites such as Amazon.

The public's unwillingness to give organisations information was based on their fatigue with unnecessary intrusion, rather than fear of criminal exploitation. Mr Crompton noted that an overloading of unnecessary identity information on everyday transactions merely created new opportunities and incentives for criminals to exploit weaknesses in any system.

Mr Mark Bregman

Executive Vice President & Chief Technology Officer, Symantec USA

Mark Bregman offered a perspective on how Symantec manages security issues for both individuals and governments. As the internet has grown, the threat has changed, from one of ad hoc vandalism to gain notoriety, to organised crime for financial game. A recent US survey showed that 14% of those who had used an online banking service had abandoned it due to security concerns. 53% had stopped giving personal information online and so requests for such information would diminish participation on such sites.

> "Threats that are the subject of concern have changed pretty dramatically; today they've become very targeted, very silent and much more focused on crime than on vandalism, on economic gain rather than notoriety. As a result, consumers are now personally concerned for their safety and for their privacy. A recent US survey showed that 14% of those who had used an online banking service had abandoned it due to security concerns. 53% had stopped giving personal information online due to fears about privacy."
>
> **Mark Bregman**

People cannot provide physical proof of identity such as drivers licences online and therefore the 'cyber world' requires new solutions, perhaps in the manner of the credit industry which relies on 'credit scores' compiled without specific interaction with the consumer.

Mechanisms exist for people to examine, dispute and correct their credit rating and this template could be employed regarding identity.

Identity can be constructed through the use of known ISP numbers ranking higher than cyber cafe ISPs, or ones from unlikely locations. Such techniques allow identities to be built without difficult technological issues being presented to the consumer. Consumers cannot be expected to pay for identity solutions themselves. The firms which offer the best systems will reap the benefit from extra business.

Dr Audun Josang
Associate Professor
School of Software Engineering & Data Communication, Queensland

Dr Josang outlined the short history of online identity management and offered ideas for its future.

The identity of individuals and organisations can be defined by multiple characteristics or a unique identifier and, when digitised, can be processed electronically. Every entity has different identities in different circumstances.

People are overwhelmed by the profusion of passwords they are required to remember online, and the usability of security systems suffers as a result. Dr Josang proposed three laws of security usability: certainty of website identity, provision of sufficient information to allow swift decision making, and a reasonable number of steps to navigate any particular transaction.

> ”We are in a crisis at the moment because we get more and more online identities we need to manage. We all suffer from identity overload and password fatigue.“
> **Dr Audun Josang**

Individual passwords have become outdated as the internet and the demand for a 'single sign-on' have grown. Such systems are now common inside large organisations, but have proved impossible to implement globally, with Microsoft’s Passport Initiative failing to find widespread approval.

The federated identity model allows users to maintain their “silo identity name spaces” and simply maps users together. It is currently being standardised and supported by large industry bodies and allows, for example, students at one Australian technical university to access the library of any other with the same identifier. This elegant model works well between related organisations or services and could prove valuable for government.

A 'user centric' model would facilitate consumer-friendly identity management by giving users technology to manage their identities online. Microsoft's 'Card Space' offers software in Explorer which allows identity management through the 'trusted third party' of Microsoft.

Unfortunately, phishing, trojans and viruses can steal passwords as they are typed or when logging on to identity providers. A rogue Java Applet can create a window that looks like Card Space and trick the user into typing their information into it. Another difficulty lies in mobility as one's identity card is locked in a browser stored on a desktop computer. Though it provides better usability and security, it complicates the process by adding a third party to every identity transaction, which inevitably creates more vulnerabilities for criminals to exploit.

> "Complexity is the enemy of security because when you have more complexity, there are more vulnerabilities being introduced."
> **Prof Audun Josang**

A true user-centric solution would not use a third party, but as the standard Linux or Windows platform is inherently vulnerable, one cannot rely on identity management technology installed on standard platforms. Security must be based on a separate portable hardware device.

The need for the identities of organisations and service providers to be assured is largely ignored, but consumers must be able to trust that they are sending their information to a bone fide bank, rather than a sophisticated phishing site. Despite sophisticated cryptography, merely clicking on a 'padlock' is no guarantor of authenticity.

Discussion

Mark Bregman warned of the ease by which digital identities could be forged in vast numbers, compared to physical documentation.

Darrell Williamson, Smart Internet CRC, believed that giving users responsibility and control of their information would encourage responsible management and trust.

Mark Bregman warned against privacy protection based on treating multiple identities as separate entities in certain situations. A criminal should not be able to repeat his crimes by adopting a different persona. Mr Bregman advocated an Identity Management solution which allowed users to choose whether to offer personal information as the price for participation, just as a young adult is required to show ID before buying a drink at a bar. He favoured public education to make the registering process in such schemes less of a trial and said government and industry shared a responsibility to inform people about good practice.

> "In the electronic world, it's very easy – in fact it is the nature of the technology – to generate literally millions or billions of false credentials very quickly."
> **Mark Bregman**

Michael Gill wondered what procedures should be created to allow people to recover compromised identities and where the control of data should reside.

Dr Audun Josang acknowledged the dangers of biometric data being stolen, as the victim is unable to change their fingerprints or irises as one might change a compromised password, and admitted that the complexity of identity management made understanding the flow and usage of information problematic for most people. He, too, suggested a system by which people might offer set 'profiles' of varying complexity for purposes of identification.

Mark Bregman observed that the passport of US citizens remains the property of the state and can be recalled at any time, giving the government access to an individual's history of international travel. Other ID is often mistakenly assumed by the public to be their property, when in legal terms it is not.

One time use credit card numbers have been used to separate the identifier for a single transaction from a person's long-term identity, but their complexity made them hard to use and opened more vulnerabilities for abuse.

As digital identities can be stolen and used many times before one is aware of their theft, Mr Bregman advocated a mechanism by which suspicious changes in patterns of use could be immediately highlighted as is currently the case with credit cards.

Dr Audun Josang agreed that patterns of behaviour form part of one's identity and so constitute a characteristic which a criminal is by definition unable to alter. This gives such patterns potential as unstealable identifiers.

> "Your pattern of behaviour is part of your identity, it describes you and it is a characteristic of you. It would be difficult for somebody to imitate your particular pattern of behaviour. So in some sense that is an unstealable identifier."
>
> **Dr Audun Josang**

Nicole Waterson of the Queensland Department of Justice questioned the notion of 'user control' in transactions for government benefits. Users had no choice whether to hand over information or not. It was simply a requirement of living in that state.

Dr Audun Josang agreed that users currently had little basis on which to decide whether to give personal information and no control over how it was used.

Mark Bregman advocated the creation of a 'trust centre' which could vouch for someone's identity to a third party without disclosing additional information about them. Criminal entities would be unlikely to engage with such a centre, giving individuals additional protection from fraud.

James Kelaher noted that different countries have different privacy traditions regarding such things as ID cards, but that international regulations concerning passports are pushing countries towards a more uniform position and this may spread to commercial transactions. Compliance rather than trust will become the issue. He also favoured stronger government action in terms of establishing basic identities.

Dr Audun Josang believed that technological solutions to prevent unauthorised access, on the New Zealand model, were misconceived, and favoured a strong policy approach. He used the analogy of a society agreeing on speed limits, rather than speed limiters in cars.

Darrell Williamson favoured a case management scenario enabling doctors or officials to access the information they required, but no more than that on a case by case basis.

Malcolm Crompton recommended www.trustguide.org.uk as a repository for research undertaken by the UK Department of

Trade. He remarked that people learn to use computers and the internet by 'playing' with them, rather than reading books or taking courses and that ID management needed a similar approach with safeguards reducing the risks of failure and offering user-friendly restitution.

Session 4 - "The Way Forward for Australia"

Mr Peter Ford

Chairman, National Consultative Committee on Security and Risk

Peter Ford noted that the National Identity Strategy has been agreed between all Australian state governments and will continue to improve the integrity of information and identity over time.

He predicted that the access card will inevitably expand its scope in practice, but said existing information privacy principles offer acceptable protection.

He praised Australia's technology-neutral legislation for allowing innovation by not mandating any particular type of application, and acknowledged the growing threat of identity crime to internet commerce.

He reiterated three topics for further discussion: the creation of a competitive market in the provision of ID management to ensure customer centric customer control, identification of the best forums in which such a system could be developed, and future practical projects for implementation.

Ms Louise Sylvan

Deputy Chair, Australian Competition and Consumer Commission

Louise Sylvan said the Adjudication committee of the ACCC can use a provision in the Trade Practices Act in Australia to authorise anti-competitive conduct into the market if the public benefits merit such an undertaking.

She explained the role of the Australasian Consumer Fraud Taskforce, which she chairs. It comprises 16 government agencies at state, territory and Commonwealth level, and two in New Zealand, that share a consumer protection remit. It works as part of the International Consumer Protection Enforcement Network which recognises that the global nature of fraud makes its perpetrators hard to apprehend and so focuses on hardening systems and educating the public.

The taskforce, in co-operation with private partners, will launch a major publicity campaign in March to educate people about the dangers. Professionals and small businesses are particularly targeted by fraudsters. The 4 themes will be ‘protect your money’ led by ASIC, ‘protect your phone’, led by ACMA, 'protect your computer' and 'protect your identity' led by the Attorney General.

Customers need systems which are both secure and user-friendly as expensive and complex procedures remove the convenience which online transactions should offer. Current protection protocols cost consumer’s time and money they may soon be unwilling to pay.

She worried that individuals, rather than banks or organisations, would be asked to bear the brunt of the costs of identity theft, as that would greatly reduce people's willingness to transact business online, and criticised the lack of provision for people seeking to rebuild a compromised identity.

> “The value proposition needs to be there for the consumers in terms of the transaction costs. That implies that protecting themselves is, number one, affordable for them, and number two, it is easy and not complex. We need the good identity systems and the safe channels that we can rely on, and that has to be paired with things like who contractually is going to be made to bear the risk of this if something goes wrong and what do we do about that as a society in relation to a devastating outcome for people.”
>
> **Louise Sylvan**

She advocated the construction of safe, reliable and trusted channels of communication and clear contractual rules about who bears the risk when identities are misappropriated. This would require co-operation between the public and private sectors, citizens and consumer protection bodies.

Mr Philip Argy

Senior Partner, Intellectual Property & Technology Group, Mallesons Stephen Jaques, President, Australian Computer Society

Philip Argy advocated the recognition of 'bundles' of rights, including human, property, legal and contractual rights. He delineated the difference between technology, people and systems which are 'trusted' by the public, sometimes without good cause, and those which are genuinely 'trustworthy'. He advocated building trustworthy frameworks to increase consumer confidence through the promotion of ethically aware professionalism above mere technical competence. These 'assurance frameworks' would depend on a 'hierarchy of trust' akin to the current Asian model of valuing personal relationships over abstract qualifications. Mr Argy believed that consumers need to be able to give 'informed consent' about the use of their information and that such data should only be used on a 'need to know' basis.

> “I will bet most of you would quite happily give me your ATM card, reasonably relaxed about my inability to enter your pin. But when you think about it, you’ve got four-digit pins and you get three attempts before the card is swallowed up. That means I have a one in 3333 chance of guessing your pin. Imagine you’d buy lotto tickets if you had odds that were that good.”
>
> **Philip Argy**

Few people realise that the small print in the 'VeriSign' digital certificate explicitly disclaims liability for its own reliability. The public are remarkably trusting with their personal information, particularly with small sums of money, and internet phenomena such as eBay rely on such trust, but such faith breaks down where larger sums are involved.

Bilateral PKI systems allow people to lodge tax returns online, but there is no public key registry allowing multilateral PKI. The creation of such an entity would greatly improve the security of online information exchange. If securing such a path for data transfer is too problematic, the alternative is to encrypt information sent by insecure means.

> “Education and IT literacy has to start at preschool”
> **Philip Argy**

Mr Argy favoured better and earlier instruction in IT to arm consumers against fraudsters and warned against the temptation to import, rather than domestically develop, IT skills.

Discussion

In rejecting an argument which placed confidence in transaction safeguards over trust in individual vendors, **Philip Argy** argued trustworthiness could be based on enforceable safeguards.

Louise Sylvan recognised the difficulties faced by individuals in rebuilding stolen identities and identified the need to develop police and consumer frameworks to facilitate this. She observed that many consumers chose to use a particular credit card online, and such ad hoc risk reduction strategies had great potential.

Prof Vijay Varadharajan of Macquarie University discussed the difference between trusted processes and trustworthy individuals and the role the internet has played in eroding hierarchies of trust and placing the emphasis back on peer to peer relationships.

Prof Bill Caelli voiced a fear that too much emphasis was being placed on consumers protecting themselves, rather than developing secure systems.

Louise Sylvan acknowledged that some unscrupulous firms have attempted to subvert consumer protection legislation, by attempting to disclaim general warranties through being 'online' and that the global nature of the internet made intervention by national enforcement agencies problematic.

Keith Besgrove hoped that a current review of Australia’s e-security system, conducted by four federal departments, would address some of these issues.

Kevin Kitson, from the Australian Crime Commission, pointed out that organised crime is not hampered by the need to outline new policy proposals or conduct post-operational assessments and so is continually a step ahead of bureaucratic enforcement agencies.

He envisioned a possible return to a pre-technological state, in which individuals would trust insiders inside organisations rather than vulnerable impersonal systems, but reminded delegates that while fraud was on the rise, detection systems were also improving apace.

He outlined the process by which the Crime Commission interacts with other stakeholders through the Suspected Financial Crimes Intelligence Network, a connected system through which government, law enforcement agencies and private industry can access databases of suspected or known fraud cases. This allows trends in identity theft to be monitored and addressed and can contribute to the rebuilding of identities by understanding the compromises which commonly occur.

Peter Fritz asserted his belief in the value of consultation and advocated the continuing role of GAP in providing a forum for the discussion of such complex issues. He closed the congress by thanking the Queensland Government, AGIMO, Baycorp Advantage, Symantec, Microsoft, the National Consultative Committee on Security and Risk, all the speakers, participants and organisers and looked forward to their involvement in future events.

Appendices

PROGRAMME

Day One - Thursday, 30 November 2006

River Room, Stamford Plaza Hotel
Cnr Edward & Margaret Sts, Brisbane QLD

6:30pm	*Pre-Dinner Drinks, Registration*	
7:00pm	*Dinner*	
	Welcome and Introduction	**Mr Patrick Callioni** Division Manager, Australian Government Information Management Office (AGIMO) Department of Finance and Administration
	Keynote Address	**The Honourable Judy Spence MP** Minister for Police and Corrective Services Queensland Government
	Vote of Thanks	**Mr Peter Ford** Chairman, National Consultative Committee on Security & Risk (NCCSR)
10:30pm	*Close*	

Day Two – Friday, 1 December 2006

Legislative Assembly Chamber, Parliament House
Cnr George and Alice Sts, Brisbane QLD

8:30am	*Registration*	
9:00am	Welcome and Introduction	**Ms Erica Hughes** General Manager, Business Information Services & Solutions, Baycorp Advantage
9:10am	Opening Address	**The Honourable Kerry Shine MP** Attorney-General and Minister for Justice, Minister Assisting the Premier in Western Queensland
9:25am	**Session One**	**Identity and Access: A Global Perspective**
	Session Chair	**Mr Chris Jordan AO** New South Wales Chairman, KPMG
		Mr Michael Coomer Group Executive, Business & Technology Solutions & Services, Westpac Banking Corporation
		Mr Keith Besgrove Chief General Manager. Access & Consumer Division Department of Communications, Information Technology & the Arts, Australian Government
9:55am	Discussion	
10:30am	*Morning Tea*	

10:50am	**Session Two**	**National and Government Initiated Identity Management: Opportunities and Directions for Further Development**
	Session Chair	**Mr John Rimmer** Partner, Joint Technology Partners; Co-chair, National Consultative Committee on Security & Risk (NCCSR)
	Keynote Address	**The Honourable Gary Nairn MP** Special Minister of State, Federal Minister responsible for e-Government, Australian Government
		Mr Paul Summergreene Executive Director, Information Management Division Queensland Transport
11:35am	Discussion	
12:30pm	*Break*	
12:45pm	**Lunch**	**Parliament House**
	Introduction	**Mr David Sykes** Vice President & General Manager, Pacific Region Symantec Australia
	Keynote Address	**Mr Phil Stradling** WW Industry Technology Strategist, Public Services and e-Government, Microsoft Corporation, USA
2:00pm	**Session Three**	**Consumer Centric Identity Management: Opportunities and Directions for Further Development**
	Session Chair	**Mr Malcolm Crompton** Managing Director, Information Integrity Solutions
		Mr Mark Bregman Executive Vice President, Chief Technology Officer, Symantec
		Dr Audun Josang Associate Professor, School of Software Engineering & Data Communication, Queensland
2:40pm	Discussion	
3:15pm	*Afternoon Tea*	
3:35pm	**Session Four**	**The Way Forward for Australia**
	Session Chair	**Mr Peter Ford** Chairman, NCCSR
		Ms Louise Sylvan Deputy Chair, ACCC
		Mr Philip Argy Senior Partner, Intellectual Property & Technology Group, Mallesons Stephen Jaques President, Australian Computer Society
4:10pm	Discussion	
4:45pm	Closing remarks/Vote of thanks	**Mr Peter Fritz AM** Managing Director, Global Access Partners
4:50pm	*Close*	

Appendix 2 – Sponsors' Profiles

Australian Government
Department of Finance and Administration
Australian Government Information
Management Office

Better Services, Better Government

The Australian Government Information Management Office (AGIMO), Department of Finance and Administration (Finance), is working to make Australia a leader in the productive application of information and communications technologies to government administration, information and services.

AGIMO fosters efficient and effective use of information and communications technology (ICT) by Australian Government departments and agencies. It provides strategic advice and leadership in activities relating to the application of ICT to government business.

Maximising government benefits from ICT investments

AGIMO acts as a catalyst for change in government to improve the delivery of services and achieve long-term efficiencies by using the enabling capabilities of ICT. The application of new technology, combined with changes to existing processes and practices, enables government policies, programs and services to be connected in ways that support both the increasing demand for multi-agency and whole-of-government responses the needs of citizens.

AGIMO works across all tiers of Australian government to maintain and develop Australia 's position as a world leader in the use of ICT in government. It provides leadership in government-wide ICT strategy, standards, and technical architecture, and security and resilience issues in the use of ICT.

In cooperation with other government bodies, AGIMO manages international contacts and represents Australia in world forums on ICT related issues.

Whole-of-government focus

AGIMO's responsibilities include:

- supporting the Secretaries' Committee on ICT (SCICT), the Chief Information Officer Committee (CIOC), as well as the Cross-Jurisdictional Chief Information Officers' Committee (CJCIOC)
- working with government agencies to develop standards to integrate services across agencies
- promoting improved government services through technical interoperability and integration of business processes across government jurisdictions
- measuring the use of and satisfaction with e-government services by citizens and business users
- leading the development of new approaches in government to citizen engagement
- developing and enhancing government e-procurement processes m
- managing whole-of-government telecommunications arrangements p
- promoting clear citizen engagement strategies
- identifying and promoting the development of ICT infrastructure necessary to implement emerging Australian whole-of-government strategies
- managing the FedLink system, to enable secure government online communications
- developing e-Government authentication frameworks for verifying electronic communications
- managing Gatekeeper, the Government's system for certifying digital signatures
- managing online and printed directories, whole of government websites and guidance for the online use of the Australian Government brand.

Baycorp Advantage

Baycorp Advantage is Australasia's leading provider of business intelligence services and solutions.

Through the integration of data sets, analytics and technologies, Baycorp Advantage provides solutions which enhance and integrate with the processes our clients use to identify, select and optimise the value of relationships with their customers.

Our data driven solutions assist our customers to enhance value through improved efficiencies to customer acquisition, the ability to implement value and risk base pricing, portfolio risk management and when necessary, recovery of customer value.

Baycorp Advantage’s electronic identity verification and identity fraud prevention services are extensively used in both the Australian and New Zealand Financial Services and Telecommunication markets. As a custodian and manager of Credit Fraud, Credit Risk and Personal ID Data, Baycorp Advantage is uniquely positioned to play a central role in these emerging markets.

To enhance this special market position, Baycorp Advantage is investing significantly in product development initiatives in the area of electronic identity verification. Amongst other new product concepts, we are currently developing an identity verification service to satisfy the Safe Harbour requirements for low to medium risk customer of the pending Anti Money Laundering Bill. Furthermore, Baycorp Advantage is working on an advanced high integrity electronic identity verification service that can be utilised to support the verification of individuals falling outside of the Safe Harbour requirements in the near future.

Converting global issues into business opportunities

Global Access Partners (GAP) is a proactive and influential network which initiates high-level discussions at the cutting edge of the most pressing commercial, social and global issues of today. Through forums, conferences, missions and advisory boards, we facilitate real and lasting change for our stakeholders, partners and delegates, sharing knowledge, forging progress and creating input for Government policy.

GAP promotes Australia's capacity to find novel solutions to the challenges facing the global community, and translates these innovative solutions into business opportunities. We focus on practical economic outcomes for Government and Business, and offer a landmark opportunity for those involved in the GAP process to discuss Australia's future in a high powered environment.

Moving from rhetoric to action

GAP's reputation for excellence is founded on its strong record of successful high-level national and global initiatives covering a wide range of industries and issues.

In seeking to foster the links between Government, Business, Industry and Academia, GAP has developed its unique model of an interactive multidisciplinary task force. Each GAP project, be it a national round table or an international symposium, constitutes the beginning of a process. One of the major outcomes is the formation of Australian Government Consultative Committees, which work to ensure the recommendations flowing from each GAP initiative become reality.

"Any survival is the result of cooperation"

Global Access Partners is part of the TCG® Group of Companies – an Australian-owned group of independent, mutually supportive private enterprises. We have been in the business of building businesses for over 30 years.

GAP INITIATIVES

2007

- *GAP Online Open Forum*
- *GAP Congress on Regulatory Affairs*
- *GAP Congress on Wellness and Ageing*

2006

- *Virtual Opportunity Congress IV: Identity & Access*
- *GAP Forum on Commercialising Nanotechnology*
- *GAP Forum on Leveraging Networks in Business*

2005

- *GAP Congress on Knowledge Capital*
- *Australian National Consultative Committee on Electronic Health*

2004

- *Better Health Care Through Electronic Information*
- *Australian National Committee on Business Building Sustainable Cities*
- *GAP Forum on Ecological Sustainability*
- *Australian National Consultative Committee on Security and Risk*

2003

- *Virtual Opportunity Congress III: Security and Risk*
- *GAP Forum on Informatics in Biology and Medicine*
- *Australian Government Consultative Committee on Knowledge Capital*
- *Australia/Central Europe Entrepreneurial Study Mission*

2002

- *Vendor Management and Outsourcing Forum*

Microsoft

Microsoft was founded in 1975 with a dream of helping people realise their true potential through technology. That vision has ultimately changed how people around the world communicate, work, learn and play.

At Microsoft, we're motivated and inspired every day by how our customers use our software to find creative solutions to business problems, develop breakthrough ideas, and stay connected to what's most important to them. We are committed long term to the mission of helping our customers realize their full potential. Just as we constantly update and improve our products, we want to continually evolve our company to be in the best position to accelerate new technologies as they emerge and to better serve our customers.

Our commitment to Australia:

Our relationship with millions of Australians extends from the home to the office and our technology is fundamental to people working in business, government and the community. Our local operation started in 1983 with only 20 people. Since then, Microsoft Australia has grown to a staff of more than 700 working in capital cities across Australia, as well as ninemsn (a PBL and Microsoft joint venture) and Microsoft's Home and Entertainment Division, which includes the Xbox business

Microsoft technology plays a key role in today's Australia – from local community groups, to remote and higher educational institutions, all levels of government, big and small business and the thinkers and entrepreneurs who will ensure our future.

Queensland
Government

Since 1998, the Queensland Government has been positioning Queensland as the Smart State – a State where knowledge, creativity and innovation drive economic growth to improve prosperity and quality of life for all Queenslanders.

The Smart State Strategy recognises that Government leadership in collaboration with industry specialists, researchers, educators and the wider community is critical in delivering on our strategic objectives.

The Smart State Strategy is a long-term investment in our future and it is already delivering real benefits to the people and businesses of Queensland.

As a result of good economic and financial management and investments in infrastructure and our people, our economy is booming, our unemployment is the lowest in 30 years and our quality of life is the envy of others.

But the world is moving quickly, so we must continue the push to transform Queensland into a knowledge-based economy if we wish to remain globally competitive, achieve higher-value jobs, enhanced prosperity and a sustainable economic future.

We must make the right investments now to ensure future generations of Queenslanders continue to enjoy the lifestyle and environment we take for granted.

Creating a smarter future is not just the role of the Government and Queenslanders everywhere are playing their part in making the Smart State a reality.

Symantec is a global leader in software, appliances and services that help individuals, small and mid-sized businesses, and large enterprises assure the security, availability and integrity of their most important asset: information. Headquartered in Cupertino, California, Symantec has operations in more than 40 countries and is focused on helping customers protect their infrastructures, information and interactions.

Symantec was founded in 1982 and now employs more than 15,500 people around the world. The company has a number of Security Operations Centres and Security Response Labs that provide 24x7 information security expertise. It also has more than 25 Support Centres globally, helping individuals and enterprises with their security and availability needs.

Symantec helps protect an organisation's physical systems, operating environments, and applications – across all tiers of its infrastructure.

Symantec also protects a broad range of information types – from email to business documents to digital photos to audio and video files – and ensures that the interactions are all protected, too.

Industry Leadership

As a recognized industry leader, Symantec helps enterprises and consumers keep their infrastructures up and running 24x7. Symantec helps customers access information anytime and anywhere by keeping their critical systems up and running all the time. One of the ways Symantec achieves this is through Symantec DeepSight Alert Services which provide early warning of potential security threats. Delivered via email, SMS, voice, fax and a secure website, these alerts are designed to help an enterprise maintain business continuity and improve adherence to emerging security regulations – all at a fraction of the cost of building a customised in-house solution.

Technology Overview

At our research and development facilities, more than 3,500 Symantec engineers build solutions to help individuals and enterprises assure the security, availability and integrity of their information.

Appendix 3 – List of Delegates

Mr Philip Argy
Senior Partner, Intellectual Property
& Technology Group
Mallesons Stephen Jaques
President, Australian Computer Society

Dr Paul Ashley
Senior IT Architect, Enterprise Integration
Solutions team, Asia-Pacific South Region
IBM Software Group

The Hon. Neil Batt AO
Executive Director
Australian Institute for Health Research

Mr Keith Besgrove
Chief General Manager, Access &
Consumer Division, Department of
Communications, IT & the Arts

Mr Mark Bregman
Chief Technology Officer, Symantec

Ms Teresa Brennan
Principal Policy Officer
Security Planning and Coordination
QLD Department of the Premier
and Cabinet

Mr Edward Bristow
Senior, Security Projects and Mobile
Office, Information & Communication
Technology Group
Australian Taxation Office

Mr Murray Bruce
Head of Security Solutions
Telstra Corporation

Prof Bill Caelli AO
Assistant Dean, Faculty of Information
Technology,Queensland University
of Technology

Mr Patrick Callioni
Division Manager, Australian Government
Information Management Office,
Department of Finance and Administration

Mr Robert Carlsson
CSO BankId

Mr Andrew Carriline
General Manager, Risk BTSS
Westpac Banking Corporation

Ms Christine Castley
Law and Justice Policy
QLD Department of the Premier and Cabinet

Mr Paul Chadwick
Former Victorian Privacy Commissioner
Advisory Group for the ALRC review of
the Privacy Act

Mr Michael Coomer
Group Executive, Business & Technology
Solutions & Services
Westpac Banking Corporation

Mr Malcolm Crompton
Managing Director
Information Integrity Solutions

Mr Shaun De Wet Stayn
Senior Manager, Risk Awareness
Westpac Banking Corporation

Mr John Dunne
Director of Business Development
Trust Centre

Mr Michael Dupe
Branch Manager, Investments and Enabling
Projects, Australian Government
Information Management Office
Department of Finance and Administration

Mr Michael Ebeid
Chief Financial Officer
Trust Centre

Mr Graham Fletcher
General Manager, Financial Services
Sector, Aus/NZ, IBM

Mr Peter Ford
Chairman, National Consultative
Committee on Security & Risk

Mr Peter Fritz AM
Chair AGCCKC, Group MD
TCG Group

Mr Chris Gallagher
Principal Legal Officer
Attorney-General's Department

Mr Michael Gill
Lead, Internet Business
Solutions Group, Cisco

Mr Chris Gration
Head of External Relations & Compliance
Baycorp Advantage

Mr Darryl Hamilton
Online Child Sex Exploitation Team,
Intelligence, Australian Federal Police

Mr Kate Hargreaves
Legal Officer, Critical Infrastructure
Protection Brunch, Attorney-General's
Department

Mr Brian Hay
Detective InspectorFraud and Corporate
Crime Group, Queensland Police Service

Ms Erica Hughes
General Manager, Information Services
and Solutions, Baycorp Advantage

Mrs Lee Hunter
Head of Executive Office, Business &
Technology Solutions & Services
Westpac Banking Corporation

Mr Graham Ingram
General ManagerAusCERT
(Australian Computer Emergency
Response Team)

Mr Rod Irvine
Adviser, Office of the Hon. Gary Nairn MP
Special Minister of State

Mr Chris Jefferis
Research Consultant
Information Integrity Solutions

Mr Chris Jordan AO
NSW Chairman, KPMG

Dr, A/Prof Audun Josang
Associate Professor, School of Software
Engineering and Data Communications
Queensland University of Technology

Mr Martin Kaldor
Vice Chair, Australian Information
Security Association

Mr James Kelaher
President, Neoteck Business Solutions

Ms Kathryn Kerr
Manager of Analysis and
Assessments, AusCERT

Mr Tony Keyes
Executive Director, Law and Justice Policy
QLD Department of the Premier and Cabinet

Ms Agnes King
IT Reporter
Business Review Weekly

Mr Kevin Kitson
Director, National Criminal Intelligence
Australian Crime Commission

Ms Jennifer Lang
Assistant Director, Strategic Policy
Department of Justice and Attorney-General, QLD Government

Mr Jon Malone
National Fraud Manager
GE Money; Australia & New Zealand

Ms Catherine Martsch
CEO Trust Centre

MsCathyMcCahon
Registrar-General
Registry of Births, Deaths and Marriages
Department of Justice and Attorney-General, QLD Government

Ms Robin McKenzie
Principal Consultant
Information Integrity Solutions

Mr Peter McNally
Partner KPMG

Ms Nerida Mead
Acting Business Services Manager
Registry of Births Deaths and Marriages
Department of Justice and Attorney-General, QLD Government

Mr Alan Munro
Managing Director
Lenovo (Australia & New Zealand) Pty Ltd

The Hon. Garry Nairn MP
Special Minister of State

Mr Theo Nassiokas
National Executive Chair
Australian Information Security Association (AISA)

Ms Julia Nesbitt
Director General Practice & e-Health
Department, Australian Medical Association

Mr Branko Ninkovic
Managing Director
Dragonfly Technologies Pty Ltd

Ms Lynda O'Grady
Managing Director, Convergent Solutions
Group, Telstra Corporation

Ms Shelley Oldham
Director, Transformation
Office of the Chief Information Officer
Government of Victoria

Mrs Jackie Orchard
Enterprise Messaging, Product & Channel
Transformation, Westpac Banking Corporation

Mr Matthew Osborne
Principal Policy Officer, Law and Justice
Policy, QLD Department of the Premier
and Cabinet

Ms Judy Oswin
Acting Deputy Director General
Queensland Transport

Mr John Pane
Chief Privacy Officer
Australian Postal Corporation

MsTamara Plakalo
CEO Open Forum

Ms Tracey Rankin
A/Deputy Registrar-General Registry of Births
Deaths and Marriages, QLD Department of
Justice and Attorney-General

Mr John Rimmer
Partner, Joint Technology Partners
Co-Chair, National Consultative Committee
on Security & Risk

Mr Colin Shadbolt
Head of Partnership
Baycorp Advantage

Mr Charles Shavitz
Account Manager, Cisco

The Hon. Kerry Shine MP
Attorney-General and Minister for Justice
Minister Assisting the Premier in Western
Queensland, Member for Toowoomba
NorthQueensland Government

Mr Matt Sinclair
Chief Technology Officer
Trust Centre Australia

Ms Glenn Singer
Acting Privacy Services Manager
Privacy NSW

Mr Martin Smith
Senior Security and Fraud Manager
HSBC Bank Australia Limited

Mr Andrew Smith
Head of Portfolio & Strategic Risk
Westpac Banking Corporation

The Hon. Judy Spence MP
QLD Minister for Police and
Corrective Services

Mr Andrew Stein
IdentityPoint Pty Ltd

Mr Greg Stone
Regional Chief Technology Officer
Microsoft ANZ

Mr Phil Stradling
WW Industry Technology Strategist
Public Services and e-Government
Microsoft Corporation, USA

Mr Paul Summergreene
Chief Information Officer, Directorate
Queensland Transport

Mr David Sykes
Vice President & General Manager, Pacific
Region, Symantec Australia

Ms Louise Sylvan
Deputy Chair, ACCC

Ms Jackie Taranto
Managing Director
Hannover Fairs Australia

Mr Jeff Tendero
DirectorQueensland Government
Chief Information Office

Ms Kay Thawley
Partner, Financial Services Industry
Deloitte Touche Tohmatsu

Ms Lisa Thomson
Chief Privacy Officer, Customer Feedback,
Operational Risk & Compliance
National Australia Bank Ltd

Mr John Trotter
Global Leader, Enterprise Risk Services
Deloitte Touche Tohmatsu

Mr Simon Tutt
Senior Policy Adviser to the Hon. Judy
Spence, QLD Minister for Police and
Corrective Services

Mr Michael Vainauskas
General Manager - Risk, Wealth Management
and Retail, St George Bank

Prof Vijay Varadharajan
Professor and Microsoft Chair in
Computing , Macquarie University

Mr Steve Venning
Senior Business Manager (Licensing
D92and Identity) Policy Advice
Queensland Transport

Mr Steve Vesperman
Senior Assistant Commissioner, Change
Program , Australian Taxation Office

Mr Andrew Want
Managing Director
Baycorp Advantage

Mr Mark Warren
Commercial Manager for NSW and the
ACT, Australia Post

Ms Nicole Waterson
Principal Policy Officer, Privacy, Freedom
of Information - Privacy Unit
Department of Justice and Attorney-
General, QLD Government

Mr Warwick Watkins
Director-General
NSW Department of Lands

Mr Darrell Williamson
Chief Executive Officer & Research
Director, Smart Internet Technology CRC

Mr Stephen Wilson
Managing Director
Lockstep Consulting Pty Ltd

Dr Anna Yang
Australian Taxation Office

A/Prof John Yearwood
School of Information Technology
and Mathematical Science
University of Ballarat

ATTORNEY-GENERAL
THE HON PHILIP RUDDOCK MP

MESSAGE: Virtual Opportunity Congress IV on Identity and Access

I would like to congratulate Global Access Partners and the National Consultative Committee on Security and Risk for hosting Virtual Opportunity Congress IV on Identity and Access.

Identity security is central to Australia’s national security, law enforcement and economic interests. False identities underpin terrorist and criminal activity and undermine border and citizenship controls and efforts to combat terrorist financing and financial crime. Stolen identities are also used to open bank accounts or to fraudulently apply for credit cards, passports or government benefits.

The Government is addressing the issue on a number of fronts.

The Council of Australian Governments in September 2005 agreed to the development of a National Identity Security Strategy to protect the identities of Australians. Work on the strategy includes the design of better enrolment practices, more physically secure identity documents and improved authentication procedures.

The Australian Government is committed to enhanced identity security. For example, the Minister for Human Services, the Hon Joe Hockey, has begun work on replacing our seventeen health and social welfare cards and voucher cards with a single smart card.

Smart card technology is safer than the traditional cardboard and magnetic strip cards most Australians carry around in their wallets.
It will also have a person’s photo on it.

But Governments cannot act alone. Businesses, too, need to ensure that they have adequate procedures in place to protect identity data which they hold.

The conference promises to be a challenging one, and I urge all of you to make the most of the opportunities on offer.

Philip Ruddock

Queensland Government

Premier of Queensland
and Minister for Trade

MESSAGE FROM THE PREMIER OF QUEENSLAND

I have great pleasure in welcoming the Virtual Opportunities Congress IV to Brisbane, where experts will discuss identity and access in this rapidly evolving electronic world.

It seems that almost every day we read about problems of identity theft and how to manage situations in which people and organisations are vulnerable to this very serious invasion of privacy.

It's a matter that concerns governments as much as individuals.

The Queensland Government is delighted to support the congress and I am sure it will be a great success.

P Beattie

PETER BEATTIE MP
PREMIER AND MINISTER FOR TRADE