

5-2011

Information Security and Privacy—Rethinking Governance Models

Kirstin Gillon

ICAEW, kirstin.gillon@icaew.com

Louis Branz

Edward Jones

Mary Culnan

Bentley University

Gurpreet Dhillon

Virginia Commonwealth University

Robert Hodgkinson

ICAEW

See next page for additional authors

Follow this and additional works at: <https://aisel.aisnet.org/cais>

Recommended Citation

Gillon, Kirstin; Branz, Louis; Culnan, Mary; Dhillon, Gurpreet; Hodgkinson, Robert; and MacWillson, Alastair (2011) "Information Security and Privacy—Rethinking Governance Models," *Communications of the Association for Information Systems*: Vol. 28 , Article 33. DOI: 10.17705/1CAIS.02833

Available at: <https://aisel.aisnet.org/cais/vol28/iss1/33>

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Information Security and Privacy—Rethinking Governance Models

Authors

Kirstin Gillon, Louis Branz, Mary Culnan, Gurpreet Dhillon, Robert Hodgkinson, and Alastair MacWillson

Communications of the Association for Information Systems

CAIS 

Information Security and Privacy—Rethinking Governance Models

Kirstin Gillon

ICAEW

kirstin.gillon@icaew.com

Louis Branz

Edward Jones

Mary Culnan

Bentley University

Gurpreet Dhillon

Virginia Commonwealth University

Robert Hodgkinson

ICAEW

Alastair MacWillson

Accenture

Abstract:

Concerns about information security and privacy continue to make headlines in the media and pose serious challenges to business. While there are many good practices that an organization can adopt to manage information security and privacy, there are also underlying areas of contention about the protection of personal information in a digital environment. This ICIS panel considered three challenges facing businesses in developing effective strategies for information security and privacy—innovating with personal information, building robust governance models, and connecting security and privacy with business goals. In the process, the panel brought together a range of research disciplines and senior business representatives to critique current practice and develop a future research agenda.

Keywords: regulation, information privacy, information security, information governance

Volume 28, Article 33, pp. 561-570, May 2011

I. INTRODUCTION

As the use of IT systems has become ubiquitous in business and government operations, there has been a steady rise in the number of failures to protect personal information. These failures have been accompanied by growing concerns from consumers and citizens about the erosion of privacy, as businesses and governments look to exploit the value of personal information to their organizations. Such failures and concerns can cause significant financial loss to businesses and individuals, both in terms of direct losses and longer term reputational damage. Therefore, they present serious challenges to businesses, especially those which rely extensively on the use of personal information in their business model.

Conventional thinking focuses on steps that individual businesses can take to enhance their performance in these areas. These include well-established good practices and governance processes, such as the adoption of the information security standard ISO 27001 and the audit of information security and privacy controls. However, are incremental improvements to the status quo an appropriate and sufficient approach to continuing failures in information security and concerns about privacy? Or is more radical thinking required? This ICIS panel aimed to critique current approaches to information security and privacy in academia and practice and to develop a future agenda for research and industry solutions.

Background

IT systems and the Internet present businesses and governments with many opportunities to increase the value that they offer customers, citizens, shareholders, and other parties. However, in order to sustain IT-based value, businesses and governments also need to manage significant concerns from customers, citizens, and other stakeholders about IT so that they retain their trust. These concerns are fuelled by:

- Individual experience of identity theft, phishing e-mails, spam, and computer viruses
- Incidents of high profile data breaches and the loss of sensitive information by governments and businesses, such as the UK government loss of personal data concerning 25 million recipients of child benefits or TJX's exposure of the credit card details of 45 million customers
- Controversial use and exploitation of personal information by governments and businesses, for example, the proposed development of a national ID card system in the UK or some of the behavioral advertising practices which have developed over the Internet

These continuing failures around information security and privacy are a matter of grave concern. Businesses can suffer direct losses when data is wrongly exposed, including regulatory fines, remediation costs, and reputational damage [Culnan and Williams, 2009; Ponemon Institute, 2009]. Individual consumers and citizens are put at direct risk from harm by criminals when their personal information is not secured properly. They may also feel that their rights have been infringed when information is used or shared in particular ways. As a result, these failures potentially damage trust in individual businesses and could limit the value that is ultimately realized from their investments in Information Technology.

In addressing this challenge, conventional thinking focuses on the way individual businesses can enhance their performance by improving governance processes around information and implementing good practices. Many of these good practices are well-established and are supported by a wide range of industry solutions, for example, the ISO 27001 information security standard, the COBIT methodology for IT controls, and the ITIL practices for managing IT operations. These practices include technical solutions, as well as processes to change the way things are done within organizations and to manage external relationships effectively.

However, are incremental improvements to the status quo an appropriate and sufficient approach to regular failures in information security and concerns about privacy? Or are there deeper issues which are contributing to the continuing difficulty in this area?

The panel session was underpinned by the contention that there is growing confusion over who should have access to personal information and what they should be able to do with it, especially in evolving areas such as social networking, data mining, and collaboration. This is shown in a range of symptoms, for example:

- Uncertainty over how to manage information about individuals, which in itself is not especially sensitive, such as location, but which has a newly acquired value due to improvements in data capture, aggregation, and analysis techniques
- Heightened tensions between interest groups over the benefits of using and sharing personal information against the benefits of strong privacy rights, for example, in the case of national security
- Changing social attitudes with regard to the voluntary sharing of personal information in return for financial or other benefits

This uncertainty leads to practical problems in businesses as good governance practices require strong foundations based on an accepted framework of rights and obligations. Therefore, the lack of clarity around new uses of personal information may be undermining the application of good practices around information, for example:

- Hindering business innovation
- Limiting the perceived business value of governance processes and turning them into meaningless compliance activities
- Reducing management and organizational commitment to good practices, making it difficult to change behavior and embed practices

On this basis, individual businesses will not be able to resolve many of the issues seen here simply by changing internal practices. Instead, more radical thinking on the nature, scope, and applicability of privacy may be necessary in order to establish firm foundations for governance and other business practices within the digital environment.

Panel Structure

To debate these issues and look at future challenges for information security and privacy, ICAEW¹ organized a panel session at ICIS 2010 entitled “Information security and privacy—rethinking governance models.”

The panel was composed of people from a mix of disciplines and backgrounds in order to provide a wide range of views and experience. It was moderated by Robert Hodgkinson, Executive Director, Technical at ICAEW. There were two representatives from the academic community—Professor Mary Culnan and Professor Gurpreet Dhillon. There were also two representatives from the business community—Louis Branz, Chief Privacy Officer at Edward Jones, and Dr Alastair MacWillson from Accenture. Brief background statements about each panelist can be found at the end of this article.

In this article, we outline the broad arguments made by panelists in the session. We then consider some of the implications from the discussion for practice and for research and teaching.

II. INNOVATING WITH PERSONAL INFORMATION

The moderator, Hodgkinson, first challenged panelists with the proposition that current uncertainties around personal information are creating significant issues for businesses that are trying to innovate in this area.

To innovate successfully with any technology, a business needs to develop a product or service which is both technologically competent and also meets a market need [Klein and Rosenberg, 1986]. Regulation provides boundaries for how businesses can operate in particular situations and, therefore, can be an important driver to the development of new markets. As a result, where the regulation of a particular new market or process is unclear, it potentially increases the risks and costs of innovation.

IT is a particularly disruptive form of technology because it radically changes the economics of information [ICAEW, 2008]. It shifts the supply and demand curves of information by reducing its costs and increasing the benefits that can be gained through it. This creates a vast new space of economically efficient information, making new activities

¹ Institute of Chartered Accountants in England and Wales

viable and profoundly changing the way that businesses create and deliver value to customers. However, these radical changes also lead to heightened contests over the control of valuable information and create confusion as new activities become possible.

As a result, IT presents businesses with tremendous new dilemmas on how to use information in innovative ways that are also socially acceptable and respect the rights of individuals. What can seem like a fantastic innovation to one person can seem like a violation of privacy to others, for example, Google's Street View. This is likely to become an even bigger challenge in future years, given the amount of information that businesses across many industry sectors are collecting about individuals, from RFID tags to smart electricity meters. Without greater clarity on the limits of using personal information, Hodgkinson reasoned, businesses will find it increasingly hard to innovate successfully.

The panelists largely disagreed with this argument. Culnan argued that the Fair Information Principles (FIPs) provide sufficient clarity to enable businesses to operate and innovate successfully. The FIPs were developed in the 1970s and are reflected in many regulatory frameworks and codes of conduct, from the European Union's data protection directive to the Federal Trade Commission's (FTC's) code in the U.S. Culnan contended that these principles provide substantial guidance to businesses on the protection of personal information, while also giving them flexibility on how to deliver the appropriate protection. She went on to assert that if all businesses were to implement governance programs based on FIPs, there may be less security and privacy failures.

This view was supported by Branz, who confirmed that Edward Jones followed FIPs in its treatment of clients' personal information. It took the approach that personal information belongs to the individual, and Edward Jones is merely a custodian of the information for a particular purpose. In Branz's view, the use of these principles had not hindered Edward Jones's innovation, and they continued to find new ways to use personal information while adhering to the principles. However, he recognized that there was inevitably some uncertainty at the leading edge which pioneering businesses would simply have to manage.

MacWillson agreed that innovation was not being hindered and that the pace of innovation driven by IT today was as fast as he had ever seen it. Indeed, he observed that some of the greatest areas of innovation are ones that could be viewed as privacy-sensitive, such as data mining, collaboration, and mobile technology. He also maintained that all businesses have to face a degree of uncertainty in their operations and innovation and there was nothing particularly different about uncertainty around personal information.

MacWillson did accept, though, that in many cases privacy is a secondary concern for businesses. Regulators often struggle to keep up with business innovation and businesses are focused on rolling out new products or services. Therefore, privacy is simply not a prime consideration in many cases of innovation. Data mining was cited by panelists as an area with potentially many concerns about the use of personal information, and as yet without a serious debate about privacy. As a result, while concerns about privacy are not hindering innovation today, they may still arise at some point in the future.

Providing some support for the initial argument, Dhillon outlined a concrete example in the area of Electronic Health Records in which businesses were being held back and innovation hindered. He highlighted concerns drawn from an Electronic Health Records outsourcing study, which highlighted the lack of principles in this area for innovating companies. It took the U.S. regulators a full year to decide on a definition for the "reasonable use" of healthcare information, making businesses stand by and wait during this period. In response, MacWillson suggested that the digitization of health information provides an opportunity to improve an area of privacy that has traditionally been very poor. Therefore, although digitization may delay implementation, it can also improve the protection provided to individuals as well as resulting in business benefits.

However, while there was general consensus that substantial innovation was happening in privacy-sensitive areas, it could nonetheless be argued that the presence of innovation does not in itself disprove the original statement. Uncertainty could still be acting as a barrier and stopping innovation in other areas. However, we simply cannot see what innovation is potentially being hindered and what ideas would be pursued if there were greater certainty over the use of personal information.

III. BUILDING ROBUST GOVERNANCE MODELS

Second, Hodgkinson challenged panelists about the suitability of current governance models. He argued that the concept of governance is concerned with balancing the conflicting claims of different stakeholders, such as the rights of shareholders against the rights of managers. Governance practices, therefore, are predicated on a clear framework of stakeholder rights to which a business can align its practices. Without that clarity, governance

processes, such as decision rights, accountability, risk processes, and verification activities, such as audits, have little meaning for a business. Instead, they become compliance measures or tick-box exercises which are a burden and without value.

As a result, incremental improvements to governance practices will have only limited effectiveness in improving business performance. Instead, governance practices in information security need to be linked more explicitly to rights to control access to personal information to provide the necessary foundations. And while there continues to be uncertainty over the limits and application of rights in this area, businesses will struggle to implement effective governance processes.

The panel presented a range of views in response to this argument. Some of the panel took the view that there were sufficiently clear frameworks in place to provide good foundations for governance. Branz, for example, maintained that the law provides this clarity. Even where the law is not clear, he believed that businesses are still able to develop fully-functioning governance models.

Culnan went on to highlight the role of culture and the leadership of a business in setting the right tone. She also focused on the role of ethics in this area, arguing that businesses should follow the ethical principle of “do no harm” with regard to personal information and think carefully before they use it [Culnan and Williams, 2009]. Culnan drew a parallel between shareholders’ cash and a data subject’s personal information. While both are valuable assets to a business, the business is ultimately just a custodian in both cases, looking after the assets on behalf of the shareholder or data subject. Furthermore, there are significant information asymmetries in both cases, with managers at a major advantage against the shareholder or data subject. As a result, Culnan reasoned, a business should have a fiduciary duty regarding personal information in the same way that they do with regard to shareholders’ investments.

However, there was some skepticism about how governance really worked in most businesses. MacWillson asserted that unless an industry is highly regulated, for example, financial services or healthcare, most businesses struggled with governance concepts in practice. He described three sets of competing interests, which create inherent tension:

- Regulators, who typically lag behind what is happening in business
- Businesses, who are focused on maximizing profits and minimizing constraints
- Consumers, who display a wide variety of views and behavior in practice

Therefore, where regulators are behind the curve and consumers are divided, governance models often fail to work effectively.

Dhillon suggested that the success of governance measures and laws depended on the specific context and contrasted two scenarios which had seen very different results due to the solidity of underlying principles. On the one hand, there were state-level security and privacy policies that were based on ill-conceived standards, leading to weak foundations and inability of the agencies to comply. On the other hand there were instances of well grounded policies, particularly in the Las Vegas Casino industry, thus making positive strides in anti-money laundering efforts. Dhillon noted that it really boils down to how well conceived a given set of governance measures is and how well the measures reflect the ground realities.

A final point came from the audience regarding the difficulty in linking governance policies with specific practices. Even where the policies are clear, businesses can still fail to implement them effectively in the business, leading to major failures. Google’s Wi-Fi incident was cited as an example of the challenge here. In this case, Google collected all kinds of personal information from unsecured Wi-Fi connections as it was building its Street View application. While this had not been intended, the code had nonetheless found its way into Google’s operations. If one of the world’s leading technology companies cannot effectively marry its privacy policies with its business practices, it was argued, it raises significant questions for less technologically-sophisticated businesses.

IV. CONNECTING SECURITY AND PRIVACY WITH BUSINESS OBJECTIVES

In the final part of the panel, Hodgkinson challenged panelists with the assertion that although many businesses have invested substantially in information security and privacy practices in recent years, in many cases, good practices have not become embedded in the way that people do things. Most failures still stem from human error,

carelessness, or malevolence. Unless businesses can fundamentally change the way that employees approach security and privacy, and make it a higher priority for them, failures are likely to continue.

This problem can be traced to a more general failure to link good security and privacy practices to broader business objectives. Many practices seem to be implemented simply because they are “good practices” and without any particular consideration for the costs and benefits of measures. As a result, employees may circumvent them or apply them inconsistently. An analogy is often made by information security specialists with health and safety practices, comparing the way that these practices have become embedded into organizations. However, there is a clear business objective with health and safety, and the benefits are obvious. This is often not the case with information security and privacy practices, where the benefits of applying practices may not be at all clear.

MacWillson first contended that it is possible for businesses to put success around information management at the heart of business success, when the drive is from the top of the organization and it is central to the brand. Where a business manages to do this, it becomes a very powerful proposition, with policies embedded and practices aligned to business objectives [Accenture, 2009]. However, few organizations have reached this stage of maturity, and, where they have, it is largely in the regulated industries of healthcare and financial services.

In practice, most businesses do not manage to make this link effectively, and they continue to make information security or privacy a much lower priority than other business activities or drivers. As a result, they continue to find it hard to embed good practices across the organization.

Dhillon agreed that security practices should be aligned to underlying security objectives and values. These go far beyond the established security objectives of confidentiality, integrity, and availability. He highlighted nine categories of fundamental objectives—enhancing management development practices, providing adequate human resource management practices, developing and sustaining an ethical environment, maximizing access control, promoting individual work ethic, maximizing data integrity, enhancing integrity of business processes, maximizing privacy, and maximizing organizational integrity [Dhillon and Torkzadeh, 2006].

Culnan and Branz agreed that in most businesses, protecting personal information is unlikely to be a major business objective. However, it will matter in some businesses more than others. Culnan compared the case of security failures by Choicepoint and TJX, two very different businesses [Culnan and Williams, 2009]. Choicepoint is an information-based business and was, therefore, substantially damaged by their information security breach, both in terms of regulatory fines and reputational damage. By contrast, TJX is an off-price retailer and, therefore, even though they exposed the credit card details of 45 million customers and suffered financial damages, the failure had less direct and long-term impact.

These differences are reflected in the application of market incentives around personal information and security. The panel agreed that the market should provide discipline and encourage good behavior in the long term. However, market incentives are limited in practice and vary across industry sectors, depending on the way in which personal information is used in a particular industry and the weight that consumers put against the protection of personal information versus price and service quality.

V. IMPLICATIONS FOR PRACTICE

The discussion with the audience, as well as between panelists after the panel had ended, raised a number of implications for businesses and regulators, which we outline in more detail in this section.

Regulatory Challenges

One result of continuing security and privacy failures in practice has been the growth in regulation around personal information and the pressure for further regulation. Many of these changes are in response to new business practices, such as behavioral advertising, and a range of recent or proposed laws were mentioned throughout the panel, for example:

- The spread of breach notification laws from the U.S. to Europe
- Proposals to allow individuals not to be tracked online by third party advertising networks
- The information security law in Massachusetts which requires compliance with specific security processes for personal data relating to Massachusetts residents, independent of where the data are housed
- The intention of the European Commission to update and strengthen European data protection laws

- A new report from the Federal Trade Commission in the U.S., suggesting that, where uses of personal information are not part of a well-understood and routine business practice, consent of the data subject should be required

However, regulators in this area are faced with significant challenges. First, the pace of change in technology means that regulators are usually well behind the curve of business innovation. This is compounded by the fact that good regulation takes time to develop, as it requires effective stakeholder consultation and should be based on robust evidence as far as possible. The principle of technology-neutrality can reduce the risk of regulation becoming outdated or tied to specific platforms. However, regulators are likely to find ongoing engagement and discussion with leading-edge businesses increasingly important, as formal regulatory activities take time to catch up with business innovation.

The increasingly global nature of business today also leads to regulatory challenges. Many organizations have developed global operations and service markets around the world. In contrast, the protection of personal information is governed by diverse legal regimes which reflect very different approaches. The U.S. takes a targeted regulatory approach, for example, with laws regulating specific pieces of sensitive information, such as health, and voluntary codes of conduct elsewhere. Beyond that, reliance is placed on the market for driving good business conduct. By contrast, the European Union has a comprehensive data protection regulatory regime which imposes a wide range of duties on businesses regarding the protection and use of personal information. Even here, though, approaches are diverse. The UK, for example, takes a more flexible and market-driven approach than countries such as Germany. This makes compliance complex and expensive for many businesses.

Developing a more global approach is likely to be difficult, and we have yet to see global institutions mature to provide oversight or governance in this area. While a degree of global convergence has happened in areas such as intellectual property, and there is some international cooperation on Internet governance in areas such as child pornography, this has not yet happened with privacy.

One of the barriers to such global cooperation is deep cultural differences regarding personal information. Legal approaches taken to protecting personal information are rooted in diverse cultures and political philosophies [Whitman, 2004]. In the U.S., for example, the notion of privacy is strongly linked to notions of liberty and freedom from state interference. However, it is often in conflict with competing cultural values, such as the freedom of the press or the operation of free markets, which may ultimately trump it. By contrast, the notion of privacy in Germany supports human dignity and draws from the Kantian concept of rights. Furthermore, in many parts of Asia or Africa, there may be limited cultural support for privacy. As a result, developing a common approach will remain particularly challenging in this area and businesses are likely to find international compliance complex and costly.

Personal Data and Intellectual Property

One particularly topical question concerned Wikileaks and the impact that their public postings of confidential government information may have on information assurance practices within business and government bodies.

This question raised an interesting connection between personal information and intellectual property. Wikileaks is not posting personal information. It is posting information more akin to intellectual property. However, in the process, it is breaching a notion of corporate or government privacy, drawing parallels with personal information.

It could be observed more broadly that digital technology has led to growing links and overlaps between personal information and intellectual property. As all pieces of information become digitized into bits and bytes, an address, a photograph, and a music file all start to look very similar. Furthermore, as businesses are capturing ever larger amounts of data about individual customers or potential customers, personal information is becoming an increasingly important asset of many businesses. As a result, there are growing tensions in this area as businesses increasingly look to exploit personal information as part of their business model.

However, rights over personal information and rights over intellectual property are reflected in two distinct and separate areas of analysis and debate. There are good historical reasons why these debates have been conducted largely in isolation from each other. Privacy was originally based on notions of physical protection regarding the home or person. It became focused on information only in the second half of the twentieth century. Intellectual property, by contrast, focused on information content such as books, or inventions. They are also underpinned by very different philosophical arguments. Privacy is underpinned by political ideals or notions of human rights. By contrast, intellectual property is largely an economic debate about incentives for content creators.

This division is reflected today in distinct areas of legal practice. Responsibility within businesses for these areas may be split between different functions or different parts of the legal department. Responsibility for information security may also sit in the IT function.

It may be that, as these links become stronger, businesses need to develop a more holistic view of information governance, which links the protection of personal data and intellectual property with information security. This could be reflected in:

- Risk management processes, bringing together a wide range of information risks that a business may face
- Organizational structures, connecting different areas of expertise and responsibility

One suggestion from the panel was that the role of the Chief Privacy Officer (CPO) could evolve into something broader, with responsibility for a wider range of information. Often held by a lawyer, the CPO role is currently seen largely in major U.S. businesses. This may reflect a more commercial and high profile approach to privacy, rather than the European approach, which may see privacy protection as a more administrative task primarily focused on compliance with data protection requirements. The CPO role is likely to evolve as many businesses place increasing importance on the exploitation of personal information in their business model and thereby raise the risks attached to personal information. There may be an opportunity to expand the role to support a more coherent approach to information risks.

VI. IMPLICATIONS FOR TEACHING AND RESEARCH

The final topic discussed by the panel concerned future research questions and implications for IS curricula. Research can play an important role in support of two key areas of decision-making:

- To provide robust evidence around the benefits of particular practices and thereby help business decide on which good practices to adopt and how to implement them effectively
- To provide robust evidence around policy options for regulators, looking at benefits and costs, as well as long-term implications of change

However, to date information security and privacy have not been mainstream areas of Information Systems teaching and academic research. The current trend in both Europe and the U.S. to focus on accountability and privacy by design in organizational governance means that privacy and security deserve more attention in IS curricula at all levels.

Possible Research Areas

Panelists made the point that there is a particular dearth of research around organizational practices in information security and privacy. Generally, prior research found organizational practices were largely reactive and driven by external pressures with senior management not involved until the organization faced a crisis. See Culnan and Williams [2009] for a brief review of this prior research. Therefore, most of the research areas mentioned here focus on building greater understanding of best practices and how businesses currently manage issues given the contemporary risk landscape.

It was suggested that case studies which look at individual business practices could be useful to highlight what drives success (see Dhillon [2007] for a sampling of security and privacy case studies), for example:

- Organizational structures and accountability
- Cultural, leadership, and ethical dimensions
- Risk management and return on security investments
- Security objectives and values
- Identity management and authentication
- Skills and knowledge of specialists and across the business more generally

The link with the law was raised as an area of potentially rich research. How do laws shape consumer or client expectations, for example, and what is the interplay between changing attitudes and changing laws? What is the impact of new regulations on organizations?

Economics is another area of rich analysis and the field of information security economics has developed in recent years to consider the misalignment of economic incentives around security [e.g., Anderson, 2004]. Although there is a long history of economics of privacy, behavioral economics is also starting to develop new insights into the trade-offs that individuals make with regard to their personal information [e.g., Acquisti, 2004]. Both of these areas can potentially provide useful insights into security and privacy which could support policy-making as well as individual business practices.

VII. CONCLUSIONS

We took a straw poll of the audience on each of the questions to get a broad understanding of where opinions generally lay. The audience was fairly split on the first contention that innovation was being hindered by uncertainty around the use of personal information. On the other two contentions, that governance models were based on weak foundations and that businesses did not connect information security with business objectives, the audience was weighted toward agreeing with Hodgkinson.

Therefore, while the audience was generally optimistic about the ability of individual businesses to improve their performance through greater focus and alignment with business objectives, it did seem to recognize that there were potentially deeper issues which also needed to be addressed.

Looking to the future, it is likely that information security and privacy will become increasingly important topics for teaching and research as technology becomes more ubiquitous, risks around information grow and more and more businesses build value propositions around the exploitation of personal information.

Given this context, there is a real need for more investment and research around these areas which draws on a range of disciplines and aims to balance the different interests which we see. Research should support further pushes for new laws and regulation in this area, which are based on media and public concerns and continuing business failures. It should also aim to improve understanding of how businesses currently manage information security and privacy issues, as well as identifying key practices which are used by leading businesses.

REFERENCES

- Accenture (2009) *How Global Organisations Approach the Challenge of Protecting Personal Data*, New York, NY: Accenture.
- Acquisti, A. (2004) "Privacy and Security of Personal Information" in Camp, J. and R. Lewis (eds) *The Economics of Information Security*, Dordrecht, Netherlands: Kluwer, pp. 179–186.
- Anderson, R. (2001) "Why Information Security Is Hard—An Economic Perspective", *Proceedings of the 18th Annual Computer Security Applications Conference*, pp. 358–365.
- Culnan, M. and C.C. Williams (2009) "How Ethics Can Enhance Organizational Privacy", *MIS Quarterly* (33)4, pp. 673–687.
- Dhillon, G. and G. Torkzadeh (2006) "Value-Focused Assessment of Information System Security in Organizations", *Information Systems Journal* (16), pp. 293–314.
- Dhillon, G. (2007) *Principles of Information Systems Security: Text and Cases*, Hoboken, NJ: John Wiley & Sons, pp. xii, 45.
- Klein, S. and N. Rosenberg (1986) "An Overview of Innovation" in Landau, R. and N. Rosenberg (eds.) *The Positive Sum Growth: Harnessing Technology for Economic Growth*, Washington, D.C.: National Academy of Sciences, pp. 275–305.
- ICAEW (2008) *Measuring IT Returns*, London, England: ICAEW.
- Ponemon Institute (2010) *2009 Annual Study: Cost of a Data Breach*, Menlo Park, CA: PGP Corporation.
- Whitman, J. (2004) "The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal* (113), pp. 1152–1221.

ABOUT THE AUTHORS

Louis Branz has been with Edward Jones in the position of Associate General Counsel since 1984. He is the firm's Chief Privacy Officer. He was in private practice with the firm of Schuchat, Cook & Werner of St. Louis, Missouri, from 1982 to 1984. He served as the Chairman of the Securities Industry Association Committee on Brokered Deposits from 1995 to 2003. Mr. Branz received his Bachelor of Arts degree from Southern Illinois University in 1978, and received his Juris Doctor degree from Washington University School of Law, St. Louis, in 1982.

Professor Mary Culnan is Slade Professor of Management and Information Technology at Bentley University. Her current research interests include information privacy and social media. Her publications include papers in the published *Journal of Public Policy and Marketing*, *Journal of Interactive Marketing*, *Journal of Social Issues*, *The Information Society*, *MIS Quarterly*, *Management Science*, and *Organization Science*. She serves on the editorial board of The Information Society. She served as a Commissioner on the President's Commission on Critical Infrastructure Protection and the FTC Advisory Committee on Access and Security.

Professor Gurpreet Dhillon is a Professor of Information Systems at the Virginia Commonwealth University School of Business, U.S. Professor Dhillon is a graduate of the London School of Economics and Political Science, U.K., where he studied organizations and information. His research led him to explore aspects of information security, identity and assurance. He has authored over 100 research articles that have been published in various journals. Professor Dhillon is also an author of six books, including *Principles of Information Systems Security: Text and Cases* [Wiley, 2007]. He is the Editor-in-Chief of the *Journal of Information System Security*, besides serving on the board of several flagship journals.

Kirstin Gillon is a technical manager in the ICAEW IT Faculty and is responsible for the Faculty's Making Information Systems Work thought leadership program. She was the principal author of the Faculty's 2008 publication *Measuring IT Returns* and co-author of 2009 ICIS panel report "Creating, Capturing and Measuring Value from IT Investments—Could We Do Better?" in the *Communications of the Association for Information Systems*. She joined ICAEW from PricewaterhouseCoopers, where she was a Senior Consultant in its IT consultancy practice. Prior to that, she was a project manager and business analyst at IBM. She has a Master's degree in international law from McGill University, Montreal.

Robert Hodgkinson is Executive Director, Technical at ICAEW, a world leading professional body which represents 135,000 members, over half of whom work in business. The ICAEW IT Faculty published a report on IT value in 2008, entitled *Measuring IT Returns*, of which he was co-author with Kirstin Gillon. He also moderated the panel "Returns on IT Investments: Could We Do Better?" at ICIS 2009 and is a co-author of the panel write up, which was published in the *Communications of the Association for Information Systems* in 2010. He is a Chartered Accountant and a Board member of the International Federation of Accountants. He graduated in Philosophy, Politics, and Economics from Corpus Christi College, Oxford University.

Dr. Alastair MacWillson is the Global Managing Partner of Accenture's global security practice, which comprises over 2,500 security professionals, and works with business and government leaders around the world on critical issues relating to technology strategy and risk, operational performance and management, cyber and information security, and critical infrastructure protection. Based in London, he also serves on the leadership council of Accenture's global technology consulting business. Prior to joining Accenture in 2002, Dr. MacWillson was the global leader of the technology consulting practice in PricewaterhouseCoopers. Dr. MacWillson has a B.Sc. in Theoretical Physics, postgraduate diplomas in Computer Science and Digital Imaging, and a Ph.D. in Cryptography.

Copyright © 2011 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from ais@aisnet.org.



Communications of the Association for Information Systems

ISSN: 1529-3181

EDITOR-IN-CHIEF
Ilze Zigurs
University of Nebraska at Omaha

AIS SENIOR EDITORIAL BOARD

Guy Fitzgerald Vice President Publications Brunel University	Ilze Zigurs Editor, CAIS University of Nebraska at Omaha	Kalle Lyytinen Editor, JAIS Case Western Reserve University
Edward A. Stohr Editor-at-Large Stevens Institute of Technology	Blake Ives Editor, Electronic Publications University of Houston	Paul Gray Founding Editor, CAIS Claremont Graduate University

CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer University of California at Irvine	M. Lynne Markus Bentley University	Richard Mason Southern Methodist University
Jay Nunamaker University of Arizona	Henk Sol University of Groningen	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

CAIS SENIOR EDITORS

Steve Alter University of San Francisco	Jane Fedorowicz Bentley University	Jerry Luftman Stevens Institute of Technology
--	---------------------------------------	--

CAIS EDITORIAL BOARD

Monica Adya Marquette University	Michel Avital University of Amsterdam	Dinesh Batra Florida International University	Indranil Bose University of Hong Kong
Thomas Case Georgia Southern University	Evan Duggan University of the West Indies	Mary Granger George Washington University	Åke Gronlund University of Umea
Douglas Havelka Miami University	K.D. Joshi Washington State University	Michel Kalika University of Paris Dauphine	Karlheinz Kautz Copenhagen Business School
Julie Kendall Rutgers University	Nancy Lankton Marshall University	Claudia Loebbecke University of Cologne	Paul Benjamin Lowry Brigham Young University
Sal March Vanderbilt University	Don McCubbrey University of Denver	Fred Niederman St. Louis University	Shan Ling Pan National University of Singapore
Katia Passerini New Jersey Institute of Technology	Jan Recker Queensland University of Technology	Jackie Rees Purdue University	Raj Sharman State University of New York at Buffalo
Mikko Siponen University of Oulu	Thompson Teo National University of Singapore	Chelley Vician University of St. Thomas	Padmal Vitharana Syracuse University
Rolf Wigand University of Arkansas, Little Rock	Fons Wijnhoven University of Twente	Vance Wilson Worcester Polytechnic Institute	Yajiong Xue East Carolina University

DEPARTMENTS

Information Systems and Healthcare Editor: Vance Wilson	Information Technology and Systems Editors: Sal March and Dinesh Batra	Papers in French Editor: Michel Kalika
--	---	---

ADMINISTRATIVE PERSONNEL

James P. Tinsley AIS Executive Director	Vipin Arora CAIS Managing Editor University of Nebraska at Omaha	Sheri Hronek CAIS Publications Editor Hronek Associates, Inc.	Copyediting by S4Carlisle Publishing Services
--	--	---	--

