11-2014

Current Status, Issues, and Future of Bring Your Own Device (BYOD)

Aaron M. French

University of New Mexico, afrench@unm.edu

Chengqi Guo

Department of Computer Information Systems & Business Analytics, James Madison University

J.P. Shim

Department of Computer Information Systems, Georgia State University

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

Recommended Citation

French, Aaron M.; Guo, Chengqi; and Shim, J.P. (2014) "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," *Communications of the Association for Information Systems*: Vol. 35 , Article 10.

DOI: 10.17705/1CAIS.03510

Available at: <https://aisel.aisnet.org/cais/vol35/iss1/10>

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.

Communications of the Association for Information Systems

Current Status, Issues, and Future of Bring Your Own Device (BYOD)

Aaron M. French

Department of Management Information Systems, University of New Mexico
afrench@unm.edu

Chengqi (John) Guo

Department of Computer Information Systems & Business Analytics, James Madison University

J.P. Shim

Department of Computer Information Systems, Georgia State University

Abstract:

This paper summarizes the panel discussion that occurred on the 2013 Americas Conference on Information Systems to discuss the current status, issues, and future direction of the use and adoption of bring your own device (BYOD). BYOD is widely used around the world. The invited panelists comprised five faculty members from the United States and Korea specializing in information systems. The covered BYOD topics included current use, real-world cases, adoption, pros and cons, issues (cultural, security, privacy), and future directions. The panel also covered bring your own service (BYOS) and bring your own apps (BYOA).

Keywords: Bring Your Own Device, BYOD, Security, Culture, Adoption.

Volume 35, Article 10, pp. 191-197, November 2014

The manuscript was received 14/04/2014 and was with the authors 1 months for 1 revisions.

I. INTRODUCTION

Smart mobile devices have emerged as an extension of the self: that is, they have become closely tied to the personal behaviors and preferences of the people who own them. Over the past several years, there has been a virtual explosion in the IT landscape of the bring your own device (BYOD) phenomena. Indeed, increasing numbers of organizations and corporations are increasingly embracing this shift in IT culture. BYOD allows employees to bring their own computing devices such as laptops, smartphones, and/or tablets to work and incorporate them into the corporation or organization network rather than using company-owned devices. The BYOD program, to varying degrees, shifts costs to the employee from the company itself. Numerous corporations and organizations have taken the lead in adopting BYOD, such as Intel, Citrix Systems, Unisys, the White House, Apple.

BYOD's benefits are clear: employees are more familiar and satisfied with using their own device(s), and employers save money by not having to pay for high-priced devices and data plans. Companies' goals with BYOD are to increase the flexibility, convenience, and portability of devices that cater to their employees' workflows, which increases productivity and morale. A recent study showed that 80 percent of respondents reported an increase in productivity following the introduction of BYOD (Twentyman, 2012), and more than two-thirds of the respondents attributed an increase in revenues to BYOD (Twentyman, 2012). However, some corporations and organizations may have to experiment with different models of BYOD. Depending on the industry and external regulations, the corporation and organization can have an impact on the approach.

A panel of professors from several U.S. based universities discussed various topics on BYOD. Topics included current use, real-world cases, adoption, pros and cons, issues (cultural, security, privacy) and future directions. This report consists of four sections. In Section 2, we present BYOD's benefits and shortcomings. In Section 3, we discuss several issues such as cultural, security, and privacy. Finally, in Section 4, we discuss future directions.

II. OVERVIEW OF BYOD

BYOD is a trend that organizations are being forced to contend with. With consumer penetration of smart devices (i.e. smartphones, tab devices, etc.) reaching critical mass, organizations are having to find ways to address the use of these personal devices in the workplace. It's no longer a matter of "if" they should implement a BYOD strategy but "how" do they do it. The Ovum BYOX (bring your own anything) study (Eddy, 2013) found:

- That 67.8 percent of smartphone-owning employees use theirs for work
- That 15.4 percent of those do so without the IT department's knowledge, and
- That 20.9 percent of those do so in spite of an anti-BYOD policy.

With large numbers of employees already having smart technology, some organizations view this as an opportunity to implement new technology without having to pay for the devices themselves. Although BYOD could be seen as a cost-saving measure for numerous organizations and corporations, it could actually be more expensive due to the difficulty of managing various platforms. Additionally, there exist looming security issues that remain to be addressed. Some major corporations and organizations choose to avoid changing their security protocols and migrate to BYOD because they do not want to risk the increased exposure to cyber threats and data breaches. Another major reason why some corporations avoid switching to BYOD is because it is still relatively new and poses far numerous security threats, from a data security point of view, which could be found in the devices or even in their apps. Employees are have concerns about privacy that need to be considered. As such, companies face numerous questions when preparing BYOD policy. They need to consider how to decide which network a given device is allowed onto. Device enrollment, licensing evaluation, security policy, and compliance, education, and security training are other major considerations.

There are many important and interesting BYOD topics. In general, there are advantages and benefits to operating a business with policies such as BYOD to improve productivity, efficiency, and employee satisfaction. Whatever the organization's level of BYOD, security must be its the top priority. BYOD security policy should be holistic and proactive. There are advantages to employees and to the organization in allowing employees to use their own mobile devices in the workplace. Whether or not an organization accepts BYOD can be the determining factor in whether a recruited employee chooses to come onboard. The following aspects of BYOD are most appealing to employees and organizations: device preference, increased productivity, reduced mobile device costs, reduced training costs, and better operational efficiency.

If an organization deals with confidential and sensitive information, the choose your own device (CYOD) model may be appropriate. In the CYOD model, the organization still owns the IT devices/equipment, but provides more options for the user to choose from (Twentyman, 2012). BYOD is widely used around the world, particularly in mature markets in the Americas region, and parts of Europe, with much potential to expand in emerging, high-growth markets, such as the BRIC countries. There are several promising trends, pros, and cons in regards to BYOD. Current issues (e.g., increased productivity, security, safety, privacy, etc.) and future directions in IS education under BYOD environment should be evaluated, along with bring your own service (BYOS) or bring your own apps (BYOA).

III. CURRENT STATUS OF BYOD

BYOD has often been viewed as a policy allowing employees to use their mobile devices at work. However, with BYOD's recent popularity, it has become more than just the use of mobile devices at work. BYOD has become associated with the benefits gained from employees using their personal devices at work in order to increase their productivity, job satisfaction, and mobility. Organizations can choose to take either a passive or active approach to BYOD. The passive approach is where organizations allow employees to bring their personal devices to work and use them for work activities. The active approach is where organizations create an explicit BYOD policy and implement it in the work environment. An active approach to BYOD relies on personal devices and requires an infrastructure to support and evaluate efficiency (Hockly, 2012).

The use of smart technology at the workplace has been around since the invention of the Blackberry. Organizations often provided these devices to increase the mobility and productivity of their employees. However, the introduction of new smart phones such as iPhone and Android have fueled BYOD in the workplace. Employees desire to use devices that they are more familiar with, and younger employees particularly have grown up with many of these devices prior to entering the workforce (Mansfield-Devine, 2012). While smart devices are considered a primary source of the BYOD trend, BYOD is not limited to just these devices. BYOD devices include any device that is mobile and purchased by the user themselves, such as laptops, netbooks, e-readers, smartphones, tab devices, and so on (Thomson, 2012).

The BYOD phenomenon has reached a global scale with over 71 percent of companies worldwide changing at least one process to allow for BYOD (Qing, 2013). The United States saw an 18 percent increase of active BYOD implementation in 2013 over 2012 (Nusca, 2013). Examples of BYOD implementations can be seen in schools (University of Tennessee Knoxville, University of South Florida, Seton Hall University), school districts (Napa Valley Unified School District, Plum Borough School District), and organizations (Cisco, Colgate-Palmolive, IBM). The U.S. Government has gotten on board with BYOD by providing a toolkit to support federal agencies that wish to implement BYOD. Apple and Samsung have provided information on their websites to help organizations implement their own BYOD solutions, while companies such as Cisco, IBM, and Intel offer BYOD solutions to organizations. While the trend of BYOD continues to grow in the US, the highest penetration of BYOD can be viewed in Pacific Asia with a 77 percent increase in 2013 over 2012 (Nusca, 2013). European companies have displayed a different trend in terms of BYOD implementation with a reported 15 percent reduction of BYOD usage in 2013 over 2012 (Yahoo!, 2013). To compensate for the reduction of BYOD devices, companies in Western Europe have increased the number of corporate-liable devices by 43 percent (Nusca, 2013).

Table 1: BYOD change from 2012 to 2013	
Region	Percent Change (2012 → 2013)
United States	+18%
Asia	+77%
Europe (BYOD)	-15%
Europe (Corporate owned devices)	+43%
<i>Note: 71% of companies worldwide changed at least one process to adapt to BYOD.</i>	

Despite a high penetration of BYOD among organizations in the US and Pacific Asia, not all employees actually use their own devices at work (i.e., not all are "BYOD enabled"). Many BYOD implementations are limited to specific areas and roles in organizations. For example, IBM has a reported 435,000 employees worldwide with only 80,000 (18.4%) of those employees being BYOD enabled. There are certain positions in an organization that fit very well with a BYOD strategy and other positions that don't. A common misconception about BYOD is that having employees purchase their own devices can save the company money, but recent data proves to contradict this notion. As Pepin (2013) reports, many BYOD solutions require the company to pay voice and data service charges for their employees' devices. However, the reality is that many organizations report that they implemented BYOD to increase productivity rather than reduce costs (Intel, 2012). While BYOD has shown several advantages such as increase mobility, job satisfaction, and productivity, there are many challenges that companies face when implementing these strategies.

The three top requirements that organizations cite for successful implementation of BYOD include having an employee code of conduct, installing security programs, and requiring management rules (Intel, 2012). Personal devices could be distracting in the workplace if used for personal reasons. In addition, using a personal device for work could be disruptive to an employee's personal life outside of work as they are continuously connected to their job. Employee code of conduct and management rules are necessary to limit the disruptive capabilities of using personal devices for work-related purposes. They are also required to ensure the security of sensitive corporate information. Some of the top barriers organizations cite when deciding on a BYOD strategy include government regulations and difficulties in supporting security, encryption, and remote wiping (Intel, 2012). Heavily regulated industries such as the medical field and the banking industry have to be even more cautious if implementing a BYOD strategy due to government regulations. In many European countries, national law prohibits organizations from processing personal data (Vandendriessche, 2012). With personal and work related data being stored on the BYOD device, this creates difficulty for companies managing the BYOD strategy and following national law. Many companies in Pacific Asia face challenges due to some countries being highly developed while other countries being less developed. Differences in service availability and network quality cause problems with mobility for BYOD-enabled employees. Varying workplace practices and cultures also present a unique challenge in Pacific Asia in addition to varying regulatory environment.

There are various advantages and challenges when it comes to implementing BYOD. A BYOD solution may not be suitable for every industry or even every employee in a company. But, when implementing a BYOD strategy, there are several considerations that must be taken to help improve the possibility of success. First, a company must decide on an implicit or explicit BYOD strategy in order to determine how to support its employees and secure its network. Then, it must decide which departments or employees will participate in the program. There are many job functions that could benefit significantly from a BYOD strategy and others that would not. Next, managers must determine the processes that would take advantage of a BYOD strategy and what applications would be needed to execute the strategy. After identifying the users, job functions, and processes to integrate a BYOD strategy for, the organization should establish an end-user agreement and training schedule. The end-user agreement should provide details including a code of conduct and appropriate uses of BYOD technology. Training should be conducted to further educate users about the BYOD policy and how to properly secure their devices. Appropriate and inappropriate behaviors should also be included in the end-user agreement and training. Finally, backup and recovery should be addressed in the instance of a lost or stolen device. This is important to organizational security and for getting the affected employee back to work and performing their regular job duties.

The use of BYOD is a recent trend but the future looks promising. As technology continues to advance, so will the capabilities associated with BYOD. Mobile speeds continue to increase as we prepare for true 4G service implementations that are projected to have speeds comparable to broadband service. This would render Wi-Fi services obsolete and pave the way for a truly ubiquitous computing environment and ultimately a ubiquitous working environment. Users will have the same computing capabilities through their mobile devices that they have sitting at their desk at work. With the addition of cloud computing, people will be able to access data anytime and anywhere, which allows them to be fully mobile while conducting the same job duties as they did in their office. BYOD will further enable companies to compete in a global environment and compete for the best talent all over the world.

IV. A GLIMPSE OF BYOD POLICY STATUS QUO

Several studies have noted that there are big gaps in BYOD policies adopted by today's organizations. According to an industrial report, nearly 60 percent of companies are vulnerable to BYOD risks (Network World Asia, 2013). Because BYOD significantly relieves the financial pressure of acquiring new IT hardware, it has been touted as a game-changer among business entities ranging from Fortune 500 corporations to non-profit organizations. The current status of BYOD use is not encouraging, however, due to simple security precautions, underestimation of risks associated with content sharing, and increasingly complicated infrastructural technology (Osman, 2013). Such facts create challenges for policy makers attempting to establish overarching codes of conduct pertaining to BYOD adoption. The high penetration of Apple products, for example, complicates compatibility and interoperability issues witnessed by corporate IT helpdesks. Companies must re-evaluate their compliance situation on how data is stored and shared across the corporate network and long-lasting impacts to how information workers behave in a BYOD environment. In the past, employees with mobile devices had to overcome technical and financial barriers to access corporate data from a remote site. Today, it takes just several taps to open a portal (or an app) through which many tasks can be performed remotely. Another troublesome fact is the imbalance between work productivity and policy. An overzealous policy is unfavorable for employees' morale, but a poor policy may lead to tardiness and distractions from work.

Strategic Fitness of BYOD

Today's companies face a variety of technological transformations: big data, social media, and ubiquitous, technology-centered BYOD. These transformations must be handled properly to maintain compliance from external auditing to internal control. In the long term, adopters of a BYOD strategy typically aim to leverage the embedded technology used by various functional units for different goals. At the operational level, managers and officers must monitor, evaluate, and handle compliance issues including employees' needs, government regulations, change of best practices, and so on. To implement a BYOD strategy, a fleet management mindset is required. According to Neville Burdan, general manager of Microsoft Solutions, "the whole idea is there has to be control, whether it is an agent, mobile device management (MDM), or mobile application management (MAM)" (Leong, 2013).

A major challenge of fitting BYOD into a company's current strategy lies in making the right decisions about internal and external compliance requirements. Therefore, auditing programs are used to conduct risk management so that environmental intelligence can be obtained. MDM, for example, builds on the existing corporate technology to enforce secure practices among employees, who must consent to the codes of conduct of BYOD adoption. This strategy builds a foundation for a comprehensive trace of corporate data activities 24/7 in a company. On the other hand, categorizing organization-level IT solutions in functional units allows decision makers to clarify adoption strategies, which help managers to identify who is using what application. Some practitioners take the perspective of customer and use a customer-centric strategy to mitigate control issues brought by BYOD. Such strategy has been widely seen in service industries who strive for optimal personalized service by accommodating to diversified end user technology. Companies including Google apply business intelligence (BI), which is obtained by measuring customer experience, in customizing their service content. Using the same methodology, these companies analyze compliance requirements to generate a profile of information worker. Such profiles depict various dimensions (e.g., database, peer network) of employee behavior that can be used for creating or personalizing BYOD policy.

Operational Checklist of BYOD Implementation

There are many schools of practices when it comes to implementing a BYOD strategy. Nearly all of them have a security model as their centerpiece. The security models around BYOD have boiled down to two varying approaches: hands-off devices where enterprise services are delivered through desktop or application virtualization, and hands-on devices model where the enterprise has tighter control of the device and the behavior and use of it by the end user (Scarfo, 2012). Each model has advantages and blind spots but generally contains the following aspects of control: client device oriented, network oriented, code of conduct training, top-down management. In regards to the organization, a policy must be in place prior to large-scale BYOD implementation. Rotate pilot projects to gauge individual needs of participating entities. Particular consideration should be given to:

- Policies regarding privacy, security, and data ownership.
- Instill ethical values regarding data rights and privacy.
- Emphasize the importance of safe-guarding data given to them (Miller, Voas, & Hurlburt, 2012).

BYOD action plans should clearly establish the objective, baseline, and stakeholders. Make policy content easy to communicate. Create whitelist/blacklist of end user applications. Enforce data encryption protocol subscription. Establish incident response for lost/stolen device. Configure rules of operations or exceptions on multiple levels: individual, team, department, cross-department, and organization. Utilize MDM/MAM and domain policy to conduct control activities. Realize that MDM or alike solutions have their downsides (e.g., coarse granularity of control), therefore, it is important evaluate BYOD program and revise according to technical/behavioral changes.

V. BYOA/S: THE INCLUSION OF APPLICATIONS AND SERVICES TO BYOD

The concepts of BYOD continue to grow and enter other areas of technology that are influenced by the users (i.e. employees). BYOD is about who controls the device. The device is just a platform where the user accesses applications that can be used to provide specific services to meet the user's needs. Beyond the purchase of devices, the responsibility to purchase applications can also be put on the employee as long as the services to be selected from. Bring Your Own Applications (BYOA) is about who provides ambient intelligence to do your job. Today, "employees" are contractors. A mobile device facilitates this. You or firms must offer/support/augment apps that facilitate this. Thus, BYOD is the requirement and BYOA is the objective. In short, BYOD is a "shibboleth"; there are security issues. Bring your own application/services (BYOA/S) is the competitive landscape, i.e., to align current employee-use and/or customer friendly services to mobile; to rethink how mobile disrupts and improves there; and to offer cutting-edge services/apps that enhance employee performance outcomes.

VI. CONCLUSION

Managing and enforcing a BYOD strategy and operational plan in enterprises is crucial. A compromise or lack of compliance can have far reaching impact. The rapidly changing IT landscape require solutions that deliver visibility and insight that assist organizations to make informed decisions, create reliable action plans, and monitor ongoing progress. It has been revealed that many organizations are risking their data confidentiality and employees' privacy by not having appropriate security policy in place. Simply seeking for financial benefits and ignoring managerial challenges beat the purpose of implementing BYOD strategy. Operational corruptions and malicious data activities gain more popularity in the absence of ethical corporate culture. On the other hand, remedies such as BYOD education, security steps, and data flow management are cost effective and require affordable administration overhead. The real challenge, therefore, is the embrace of BYOD readiness on the high level management, which can be achieved with the help of timely research and ongoing knowledge sharing between industry and academia.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge Matti Rossi and an anonymous reviewer for their comments on the earlier draft of this paper. The authors also acknowledge Professors Daniel Mittleman and Richard Welke as panelists at the panel session.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Eddy, N. (2013). Businesses must adapt to permanent BYOD presence: Ovum. *eWeek*. Retrieved July 29, 2013, from <http://www.eweek.com/small-business/businesses-must-adapt-to-permanent-byod-presence-ovum/>

Hockly, N. (2012). Tech-savvy teaching: BYOD. *Modern English Teacher*, 21(4), 44-45.

Intel. (2012). Peer research report: Insights on the current state of BYOD. Intel's IT Manager survey. *Intel IT Center*. Retrieved July 29, 2013, from <http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf>

Leong, K. B. (2013). How to fit BYOD into an enterprise mobility strategy. *Network World Asia*, 12-14.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*, 2012(4), 14-17.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, 14(5), 53-55.

Network World Asia. (2013). Nearly 60% of companies are vulnerable to BYOD risks. *Network World Asia*, 5.

Nusca, A. (2013). BYOD: North America and Asia embrace it; Western Europe, not so much. *ZDNet*. Retrieved July 29, 2013, from <http://www.zdnet.com/byod-north-america-and-asia-embrace-it-western-europe-not-so-much-7000016802/>

Osman, H. (2013). CIOs in Asia-Pacific are embracing BYOD. *Computerworld Philippines*, 22(5), 41-41.

Pepin, C. (2013). IBM Connection 2013: BYOD at IBM. *Slideshare IBM Network*. Retrieved July 29, 2013, from <http://www.slideshare.net/chrispepin/ibm-connect-2013-byod-at-ibm>

Qing, L. Y. (2013). BYOD on rise in Asia, but challenges remain. *ZDNet*. Retrieved July 29, 2013, from <http://www.zdnet.com/byod-on-rise-in-asia-but-challenges-remain-7000010660/>

Scarfo, A. (2012). New security perspectives around BYOD. In *Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications* (pp. 446-451). Washington, DC: IEEE Computer Society.

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, 2012(2), 5-8.

Twentyman, J. (2012). BYOD: OMG! Or A-OK? *SC Magazine: For IT Security Professionals*. 18-23.

Vandendriessche, J. (2012). Understanding BYOD legal issues under European privacy and data protection law. /SACA. Retrieved July 29, 2013, from http://www.slideshare.net/Johan_Vdd/understanding-byod-legal-issues-under-european-privacy-and-data-protection-law

Yahoo! (2013). Q1 BYOD smartphone sales surge in North America and Asia but Western Europe fights the growing trend. Retrieved July 29, 2013, from <http://finance.yahoo.com/news/q1-byod-smartphone-sales-surge-120000004.html>

APPENDIX A: LIST OF PANELISTS

Topic: Bring Your Own Device (BYOD): Current Status, Issues, and Future Directions

Panelists: J. P. Shim, Georgia State University
Daniel Mittleman, Depaul University
Aaron French, University of New Mexico
John Guo, James Madison University
Richard Welke, Georgia State University

ABOUT THE AUTHORS

Aaron M. French is currently an Assistant Professor of Management Information Systems in the College of Business at Kyungpook National University in South Korea and will be joining the faculty of the University of New Mexico this summer. He received his PhD in Business Information Systems at Mississippi State University. He has received outstanding teacher of the year awards at Mississippi State University and Kyungpook National University. His research has been published in the *Journal of Information Technology, Behaviour & Information Technology, Communications of the Association for Information Systems, Pacific Asian Journal of the Association of Information Systems, Journal of Internet Banking and Commerce*, and *The Journal of Internet Electronic Commerce Research*. His research interests include social networking, eCommerce, cross-cultural studies, and technology acceptance.

Chengqi (John) Guo is an Assistant Professor and Madison Research Fellow of Computer Information Systems and Management Science in the College of Business at James Madison University. He received his PhD in Business Information Systems from Mississippi State University. He received a Masters of Operations Management and Information Systems from Northern Illinois University and a B.S. in International Marketing from Guangdong University of Foreign Studies, Guangzhou, China. He is a senior consultant and Director of International Business Development at JDArray Co. Ltd, Beijing China. His research interests are Information Systems security, social media, mobile computing, technical innovation, human computer interaction (adoption, trust, privacy, and communication), innovative technology in education, and cross-cultural studies.

J. P. Shim is Executive Director of Korean-American Business Center and a faculty of Computer Information Systems at Robinson College of Business at Georgia State University. He is currently teaching Business Telecommunications, Managing Information Technology. Before joining at GSU in 2011, he was faculty of BIS and Larry and Tonya Favreau Notable Scholar at Mississippi State University. During the past twenty-seven years at MSU, he was a seventeen-time recipient of outstanding faculty awards, including John Grisham Faculty. He is Professor Emeritus of BIS at MSU. He has published five books and seventy journal articles. His coauthored paper has been cited as top in SSCI citations, Elsevier citations, and downloads in DSS. He serves on Wireless Telecommunication Symposium as Program chair. He has received awards, grants, and distinctions, including NSF, Microsoft, U.S. Small Business Administration, Korea Foundation, and Japan Foundation. He has been interviewed by the media (CBS TV, AP, AJC) and worked as a consultant for Booz Allen, U.S. EPA, Kia Motors, Hyundai Motors, and others.

Copyright © 2014 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

Matti Rossi
Aalto University

AIS PUBLICATIONS COMMITTEE

Virpi Tuunainen Vice President Publications Aalto University	Matti Rossi Editor, CAIS Aalto University	Suprateek Sarker Editor, JAIS University of Virginia
Robert Zmud AIS Region 1 Representative University of Oklahoma	Phillip Ein-Dor AIS Region 2 Representative Tel-Aviv University	Bernard Tan AIS Region 3 Representative National University of Singapore

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	Michel Avital Copenhagen Business School
--	---

CAIS EDITORIAL BOARD

Monica Adya Marquette University	Dinesh Batra Florida International University	Tina Blegind Jensen Copenhagen Business School	Indranil Bose Indian Institute of Management Calcutta
Tilo Böhmann University of Hamburg	Thomas Case Georgia Southern University	Tom Eikebrokk University of Agder	Harvey Enns University of Dayton
Andrew Gemino Simon Fraser University	Matt Germonprez University of Nebraska at Omaha	Mary Granger George Washington University	Douglas Havelka Miami University
Shuk Ying (Susanna) Ho Australian National University	Jonny Holmström Umeå University	Tom Horan Claremont Graduate University	Damien Joseph Nanyang Technological University
K.D. Joshi Washington State University	Michel Kalika University of Paris Dauphine	Karlheinz Kautz Copenhagen Business School	Julie Kendall Rutgers University
Nelson King American University of Beirut	Hope Koch Baylor University	Nancy Lankton Marshall University	Claudia Loebbecke University of Cologne
Paul Benjamin Lowry City University of Hong Kong	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	Jeremy Rose Aarhus University
Saonee Sarker Washington State University	Raj Sharman State University of New York at Buffalo	Thompson Teo National University of Singapore	Heikki Topi Bentley University
Arvind Tripathi University of Auckland Business School	Frank Ulbrich Newcastle Business School	Chelley Vician University of St. Thomas	Padmal Vitharana Syracuse University
Fons Wijnhoven University of Twente	Vance Wilson Worcester Polytechnic Institute	Yajiong Xue East Carolina University	Ping Zhang Syracuse University

DEPARTMENTS

Debate Karlheinz Kautz	History of Information Systems Editor: Ping Zhang	Papers in French Editor: Michel Kalika
Information Systems and Healthcare Editor: Vance Wilson	Information Technology and Systems Editors: Dinesh Batra and Andrew Gemino	

ADMINISTRATIVE

James P. Tinsley AIS Executive Director	Meri Kuikka CAIS Managing Editor Aalto University	Copyediting by Adam LeBroq, AIS Copyeditor
--	---	---