Inf Syst Front (2014) 16:347–352
DOI 10.1007/s10796-014-9501-x

Using scenarios to understand the frontiers of IS: Fifteen years later (a postscript)

Anat Hovav

Published online: 22 May 2014

1 Introduction

Fifteen years ago, Paul Gray and I wrote the above article describing four potential trajectories technology may take (Gray and Hovav, 1999). The trajectories were developed based on a number of general assumptions and by using scenario building methodology. When I read the paper over in preparation for writing this postscript, it occurred to me that "had I known then what I know now…" I found our outlook somewhat naïve, techno centric and at points shortsighted. Hindsight is of course always 20/20. The key to good scenario building is not to try and describe a predictable future but to create a set of diverse futures and analyze the drivers and consequences of each.

As such, scenario building methodologies often represent the views of the researchers that use them and the state-of-affairs at the time they are developed. In the late 1990s, our discipline's foci were on organization, inter-organization and at best industry level use/effect of technology. As the reach of the Internet increased and technologies such as Web 2.0, social networks, mobile computing (smart phones, tablets) and the cloud became dominant, our discipline expanded its investigative boundaries to include topics such as the effect of technology on society, ethics, and culture, and unintended consequences of technology (e.g., addiction, cyber bulling). In this postscript, I will highlight the differences between our predictions and the current state-of-affairs. The rest of the postscript is organized as follow: in the next section, I describe the main drivers and propose a slightly different approach to the four scenarios that Paul and I introduced in 1999. Then, I briefly summarize the variables that did follow our initial proposed trajectory followed by a section discussing the variables that did not materialize as we predicted. In section five, I introduce globalization as a potential catalyst. Section six describes two trends we did not include in our 1999 paper. I end with concluding remarks and call for action.

A. Hovav (✉)
Korea University Business School, Seoul, South Korea
e-mail: anatzh@korea.ac.kr

2 The main drivers

The two dimensions we deemed fundamental for the development of our scenarios, social acceptance and technological development, are still key drivers in the course IT is taking. For example, much of the research in Information Security has been composed of the development of technical countermeasures by computer scientists, and more recently, the influence of human behavior by MIS researchers. However, in retrospect, I feel that our definition of each driver was limited in scope and vision.

Future advances in telecomm were a major driver in 1998–99, especially with the advent of the Internet as a commercial space and the explosion of the dot com. Although telecomm is still a major driver (especially mobile communications), a new potential factor has emerged in the early 2010s, namely big data and data analytics. Recent events such as the Snowden case and the NSA spying crisis have introduced data management related ethical questions society will have to address in the near future. That leads us to the second dimension Paul and I chose as a driver in our 1999 paper, social acceptance (Gray and Hovav, 1999). Our basic premise at the time was (and it still holds) that technology changes much faster than people and society. Although I still believe that social acceptance is an essential influencer in the direction any technology will assume, globalization has made the conceptual definition of social acceptance complex and ambiguous.

For example, one of the variables we included in our 1999 paper was "privacy." The social definition of privacy is more

intricate now than it was then. The Western definition of what is considered private and who should enforce privacy laws is not universal. Research has shown that individuals in collectivistic cultures (particularly Asian cultures) are less concerned with privacy (Kim 2008). In 2009, the South Korean government implemented a "real name" identity system for using blogs and other Web 2.0 type services.[1] The law was proposed after slanderous postings resulted in the suicide of a local celebrity, JinSil Choi (the law was repealed in 2012 as unconstitutional since it required users to provide their resident ID number). An informal survey of over 100 Korean students (ages 19–25) suggested that a majority of them were willing to forgo their right to privacy in order to minimize the scope and reach of cyber bulling incidents. Conversely, google.com refused to impose a "real name" system on YouTube citing anonymity and privacy as fundamental rights. This is not to say that cyber bulling or any other exploitation of the Internet is (or should be) an acceptable behavior in any society. The point of the above examples is to suggest that different cultures view the concept of privacy differently. In addition to culture, age plays a role in peoples' perception of privacy. It is stipulated that younger individuals are becoming less concerned with privacy especially when using social network sites (SNS) such as Facebook. Therefore, it is possible that overtime, issues such as digital privacy will become mute (at the individual level) as future generations accept the lack of privacy as an integral part of "being connected."

Table 2 in the original paper lists close to thirty variables and their expected values under each of the four scenarios depicted in Fig. 1 (Gray and Hovav, 1999). In the next section, I discuss a slightly different scenario space. The proposed space is still a simplification of a "real" future since it is limited to four possible outcomes. However, it is my hope that the scenario space in Fig. 1 is slightly more socio-technically balanced than our original space in Gray and Hovav (1999).

2.1 The four scenarios: Then and now

The Utopian and Dystopian scenarios were developed based on a paper by Kling and Lamb (1996). Utopia suggests that technology can be used to solve most social problems; Dystopia suggests that technology can interfere with our social fabric via job displacement, socioeconomic (digital) gap, and privacy invasion. The above definitions are techno-centric and naive as they assume that with enough technology, the universe can solve most of its problems. Therefore, I propose the following scenario space (Fig. 1) as an alternative:

The first scenario assumes slow technological development and low social acceptance of new technology. This

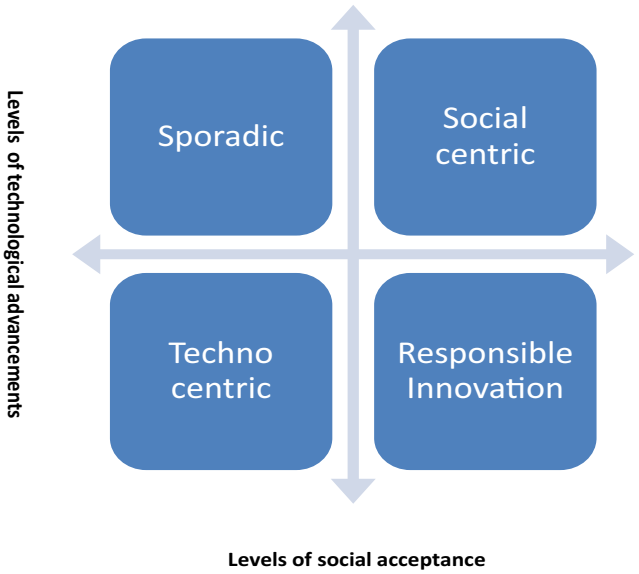

Fig. 1 Proposed scenario space

scenario is likely to result in slow and *sporadic* adoption of new technology. Such a scenario could occur if there is no universal agreement on who should manage the Internet, resulting in the deterioration of its backbone combined with increase in security breaches and privacy infringements. The second scenario in Fig. 1 is *techno-centric*, which assumes a rapid introduction of new technology regardless of the social impact. Such a scenario could occur in developed countries if Hi-Tech companies use their profits to increase their lobbying power, a trend we have seen in 2012–2013.[2] Such a scenario is also likely because developing countries increasingly rely on technology as an economic growth driver. Governments of these countries are likely to support technological advancements with minimal regard for their social impact. The *social centric* scenario in Fig. 1 assumes that the path technology takes is driven primarily by social concerns and norms rather than by technological innovations. I admit that at present this scenario is the least likely to occur. However, major catastrophic events such as a cyber-terrorism attack on a national grid or a detrimental security breach against Wall Street might increase Luddites behavior. E-trash, techno-stress and teen addiction might also increase social resistance to unruly diffusion of new technology.

I initially named the fourth scenario in Fig. 1 "*desirable*." I later revised it to *responsible innovation*, a term discussed in the paper by Wakunuma and Stahl (2014). Either labeling is of course biased. Balancing technology and social needs is a very subjective notion. As mentioned above, determinants such as culture, age, and accessibility may influence the definition of social acceptance. In

[1] http://en.wikipedia.org/wiki/Real-name_system [last accessed on 02/25/2014].

[2] http://www.opensecrets.org/news/2013/01/learning-from-microsofts-mistakes-g.html [last accessed 12/3/2013].

addition, who is to determine what level of social consideration is optimal? China might consider the need for economic growth a socially desirable outcome regardless of the potential health and environmental impact of its factories. The EU, on the other hand, might consider privacy and environmental sustainability as its main social drivers. As thorny as the fourth scenario is, I offer it for completeness.

In the following sections we discuss the variables listed in Table 2. For the sake of brevity, I will mention in passing most of the variables and only discuss in detail the few that took a noticeably different trajectory than we initially expected. The discussion is based on the Utopian scenario in the original paper (Gray and Hovav 1999).

3 Variables that followed our line of prediction

Some of the variables we listed in Tables 1 and 2 were rather simplistic and indeed followed the course charted for them. Many of the variables listed under the heading "Information Systems" in Table 2 have achieved (or are headed in the direction of) what we termed Utopian. ERP, decentralization, packaged software, web based EDI (although today the more common terms used are B-2-B, portals, purchasing agents), networked PC (i.e. Tablets), and e-commerce are widespread in 2014. Others listed in the above category have not reached dominance but are progressing in the direction we prescribed. We predicted that keyboards will become obsolete, except for heavy data entry operations. Indeed, tablets and smart phones enable the functionality of 1999 PCs (and more) without the use of a keyboard. Voice recognition still has limitations but the use of kinetics (hand and body motions) to activate and control devices is progressing rapidly and may trump voice activated technology. Under the "technology" section in Table 2, Moore's law is still in play, computers have not become obsolete, the Y2K problem was solved without any major catastrophes, the rate of technological change has increased slightly but is still manageable, and the cost of storage capacity is plummeting rapidly. Finally, although we did not achieve Internet III (the world is still using the same protocol first developed by DARPA in the 1970s – i.e., TCP and IP version 4), the speed and reach of the Internet has increased but not necessarily in the geographical regions we anticipated (see discussion below). The two variables under the political category did occur as was predicted for all four scenarios. Two of the variables listed under the title "socioeconomic" also transpired as expected: Globalization and complete absence of Luddites activities. The rest of the socioeconomic variables will be discussed in the next section.

4 Variables that did not follow our line of prediction

4.1 Technology and system

Four variables from the "information systems" category have not progressed as predicted. The most obvious variable is the existence of secure e-cash. Not only that we are still using credit cards for most online purchasing, but most online transactions would not be considered "secure." In retrospect, e-cash should have been placed under the "political" category since it is more of a policy issue than a system issue.[3] The use of outsourcing as defined in 1999 has been mixed. While some companies are still outsourcing portions of their IT function, others are back-sourcing (e.g., GM).[4] However, with the advent of cloud computing and SaaS (Software as a Service), new forms of sourcing are developing and will likely replace the large cumbersome contracts of the 1990s. Finally, in our discussion of the Utopian scenario, we suggested that software standards will be developed by international agencies and vendors will rarely create de facto standards. This trend proved completely reversed. Network economics and externalities created an environment where "winner takes all" and first mover (i.e., Apple, Facebook), or at best fast second mover (i.e., Samsung, Google) control the market. As a result, most current standards are de facto although not all are proprietary. While Apple computing continued success depends on a closed, proprietary system, Google relies on open architecture (i.e., Android). From Microsoft Windows operating systems to Intel's USB drive most current standards have been developed by vendors.[5]

4.2 Socioeconomic

Unlike technology and systems, the socioeconomic variables were much more difficult to predict. This may be because Paul and I are technologists by training, not sociologists. Or maybe it is because humans are more fickle than computers.

As to environmental consciousness, the jury is still out and the progression of "green" depends on who you ask. Computer literacy is increasing as young persons enter the job market. However, a digital divide still exists within and between countries. Therefore, although computer literacy is improving, our conjecture that it will become ubiquitous by 2010 was naïve at best. Interestingly enough, our initial scenarios

[3] Technically e-cash is available as is apparent from the use of cyber money by game and SNS sites. The obstacles are mostly political. The implementation of a universal e-cash system requires financial agreements among participating countries.

[4] For example see GM back sourcing announcements at: http://www.cio.com/article/718053/GM_Bets_on_Insourcing_Brings_Back_10_000_IT_Jobs [last accessed 12/3/2013].

[5] One exception are the IEEE802 wireless network standards of which the most commonly used is the Wi-Fi.

assume no economic and/or energy crises. Both occurred and neither had much influence on the direction technology took. The cost of fuel has increased by 250 % since 1999.[6] In 2002, thousands of dot com companies failed and with it the availability of venture capital (VC) and the NASDAQ (as of November of 2013, the NASDAQ is still lower than its highest value of 5048.62 circa March 2000). In 2008, a much more connected and globalized world suffered another financial crisis. The U.S. "subprime mortgage" crisis and the collapse of several major U.S. investment and commercial banks spread throughout the global financial markets within days. Although both crises were attributed (directly or indirectly) to the use of information technology and systems, neither created a Luddite effect. On the contrary, investments in technology and the use of technology in business and society have increased over time.

The last variable I will discuss in this section, privacy, was presented as an example in the introduction. Our utopian scenario predicted medium privacy. We also predicted that the U.S. would follow the EU's privacy laws. This prediction did not metalize with one exception. As of 2014, U.S. companies that operate in Europe have to comply with the EU directive 95/46/EC. To do so, American companies may opt into the US-EU safe harbor program.[7]

However, our 1999 scenario space did not explore the threats to privacy from hackers, internal misuse and social engineering (e.g., spam, phishing). The number of identity theft type attacks has increased over the past 15 years. Major incidents such as the TJX attack (Hovav and Gray, 2014) and more recently the Target attack threaten the privacy of anyone engaging in commerce (on or off line). In addition, regulatory actions by various governments (e.g., censorship, real name ID, surveillance) also threaten personal privacy (as defined by Western standards). Yet, as of 2014, none of the above privacy challenges deter people from using information systems for commerce, socializing, education, and entertainment. As such, it is unclear if including a more comprehensive definition of privacy in our 1999 discussion would have resulted in a different set of "futures."

5 Globalization as a catalyst

I chose to discuss globalization as a catalyst for several reasons: First, the reciprocal relationships between technology and globalization; while the rapid increase in global commerce is credited to the commercialization of the Internet, globalization has been driving the rapid dissemination of new technological innovations. Globalization also introduced a number of new players into the technology and innovation arena. Although our 1999 paper was titled "the frontiers of IS," it predominantly concentrated on the future of IS in the U.S. and Western Europe. In 2014, one cannot ignore the dominance of several Asian countries in areas such as mobile technology, smart homes, appliances and grid, and consumer electronics.

One of the issues discussed in Gray and Hovav (1999), was the "last mile" problem – the connection from the curb to the home. In the paper, we suggested mobile networks as a solution. Indeed in many countries, the "last mile" bottle neck has been resolved by using third (3G) and fourth (4G) generation wireless communication to access local Internet service providers. Many metropolitans have also implemented WiMax (IEEE 802.16) to support wireless broadband accessibility. Yet, upgrades of the infrastructure to fiber optics (Fiber-To-The-Home) have also been used to provide high speed broadband accessibility. These broadband upgrades were mostly facilitated by local telecommunication companies who can then charge higher fees for faster connectivity. Thus, our scenarios partially predicted the trajectory of connectivity towards wireless solutions. What we failed to predict was the shifts in global connectivity; some are due to leapfrogging by developing countries and some are due to strong governmental policies. We also failed to identify the main players that influenced these changes.

Based on a recent OECD report,[8] the U.S. is not the most connected country in the world. While the average wired broadband speed for OECD countries is 12 Mbits per second, the U.S. is listed 15th (with less than 10 Mbits/second) and behind countries such as South Korea, Greece, Poland and Slovenia. As to wireless broadband connectivity, the U.S. is listed 6th behind countries such as Finland, Sweden and South Korea. Transitional economies of the late 1990s have used Hi-tech as a growth engine. For example, the South Korean government's Internet infrastructure polices (Hovav et al. 2011) enabled Korea to emerge from the 1997 Asian financial crisis and become one of the leading economies in the world. Again, our definition of First World Countries (see p. 22) was limited in scope and ignored potential fundamental changes in the world economy post the commercialization of the Internet.

An adverse effect of globalization is the proliferation of cyber security attacks. In the late 1990s, cyber incidents were for the most part, the result of attacks by individual hackers. The Internet commercial influence was in its infancy and many of the known cyber attacks were initiated by what hacker culture literature labeled as white hat or ethical hacking.[9] In 2014,

[6] http://www.eia.gov/dnav/pet/pet_pri_gnd_dcus_nus_w.htm [last accessed 02/25/2014].
[7] http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles [last accessed 12/04/2013].
[8] OECD Science, Technology and Industry Scoreboard 2013: INNOVATION FOR GROWTH.
[9] For more information see: http://en.wikipedia.org/wiki/White_hat_(computer_security) [last accessed 02/25/2014].

cyber attacks are the result of coordinated efforts by well organized professional hacking teams (Hovav and Gray, 2014). These global groups (such as the one responsible for the TJX attack) operate much like conventional multinational firms. Professional hacking teams exploit political, economic and human resource conditions across continents to maximize their profits and minimize the risk of exposure and repercussions. Technical savvy computer scientists in Eastern Europe (where skilled scientists receive relatively low salaries) create the code needed to break into the target system. Identities are sold in black markets housed on servers in Asian countries where policing such activities is intermittent. Fake credit and debit cards using these identities are produced and used in rich countries (i.e. U.S., Germany). These organizations rely on the anonymity of the Internet, the existence of "safe heavens" and lack of cohesive international cyber laws. Another example of a globalized cyber peril is the existence of interconnected bots and internationally distributed networks of zombies.[10] These networks are offered for sale on cyber black markets and are often used for distributed denial of service attacks (DDOS), website hijacking, cyber extortion, cyber espionage and spam. For additional details of the economy of bots, see Stone-Gross et al. (2011).

6 Some variables we did not discuss

One of the trends we did not anticipate was the explosion of Web 2.0 and social networks, and the impact they will have on society, governments and political movements. Here too, our discussion was focused on technological advances (we assumed that Internet II will become prevalent) rather than functionality.[11] I doubt that it is necessary to discuss here the explosive influence that Web 2.0 and social networks have had on the way people interact, share, and are entertained. What is important to note is that the existence of these technologies has, to some extent, broadened the foci of IS research from an organizational to societal. The existence of Web 2.0 facilitated positive social movements along devastative acts of terror. Twitter have been used in emergency situations (e.g., to save lives during the Mumbai attack[12]) and in social movements (e.g., the Arab spring and the uprising in Egypt). Unfortunately, advances in social networks also have had unintended consequences such addiction, cyber bullying, unethical use of data and information, digital surveillance and cyber terrorism. Neither our utopian nor our dystopian scenarios of 1999 account for any of these eventualities.

[10] Zombies are computer that have been taken over by bots. Hackers can use to them to launch an attack unbeknown to the owner.

[11] To clarify, Internet II refers to advances in the infrastructure the Internet uses, while Web 2.0 refers to the functions afforded by the Web.

[12] For details see Oh et al. 2011.

Another emerging trend we did not predict (although the capability to implement such technology existed in 1999) was the Internet of Things (IoT), the ability to interconnect everyday physical objects through an elaborate network of wireless sensors. IoT can be used to develop sustainable future, support an aging population, and provide health and other social services to remote communities and developing world regions. However, IoT, wrongly used, can result in privacy infringement, and loss of control, autonomy and self worth in the populace. For further discussion of the ethical implications of Ambient Intelligence, see the paper by Wakunuma and Stahl (2014) in this special issue. If the assertion above that these new technological developments have introduced a change in our research foci holds true, should IS also change its research paradigm? This question is briefly discussed in the next section.

7 Closing remarks and call to action

The above discussion was not meant to merely evaluate the accuracy of our 1999 scenarios. Rather, the goals of the discussion were threefold. First, I wanted to illustrate the value of scenarios and futures methodologies as research tools design to describe potential trajectories of a given phenomenon. Although one or two drastic changes (i.e., the bust of the dot com, the financial crisis of 2008) could have lead IS on a different path than we anticipated in 1999, many of the variables we proposed remain relevant. These variables may apply more broadly or may be more complex than Paul and I have portrayed in our 1999 article, but fundamentally the trajectory remained the same. For example, Olla and Choudrie (2014) state in their article, that the scenario that materialized was the "*probable scenario*." The "*optimal scenario*" was more of a wishful thinking by the authors (much like the *responsible innovation* scenario in Fig. 1). Yet, they concluded that using Ethnographic Futures Research (EFR) provided them with an insight to how mobile communication can influence services in developing countries. Their conclusion supports our assertion that Futures research methodologies do not necessarily provide a solution. Rather, these methods can be used as a tool to investigate potential "futures" and subsequently as a basis for analyzing what if a certain course is taken.

As mentioned above, scenarios are often subjective. Caution should be taken to avoid groupthink and preconceived notions. The second goal of the postscript was to highlight our naiveté in 1999. Both Paul and I were immersed in Western culture. We failed to address the influence of global changes and cultural differences partially to keep the paper short (see our basic set of assumptions) and partially due to our limited awareness. Since then, I have lived and worked in South

Korea for nine years. Although this exposure to Asian culture augmented and widened my horizons, the analysis presented in the postscript is still based on the views of one person. However, this deficiency in futures research methodologies can be mitigated using current technology. In 2014, the IS discipline is well positioned to objectify Futures research by utilizing social networks, crowd sourcing and the availability of thousands of global experts a click away.

Finally, the third goal of this postscript and the special issue is to advocate the need for Futures research in our discipline. As MIS embarks on new research topics, the discipline needs to expand its toolbox of research methodologies and potentially augment its research paradigm. Rather than being a passive conduit of the post hoc effect of information technology on various stakeholders, IS research should engage in active leadership. As stated by Markus and Mentzer (2014), Futures methodologies are most appropriate to investigate ethical issues in IS, while the article by Wakunuma and Stahl (2014) explores the lack of ethical conceptualization by IS professionals. By using Futures methodologies, IS can switch from being a passive observer of innovation to an active participant and true change agent in what von Schomberg (2011) termed responsible innovation. For example, Futures research may enable MIS scholars to investigate potential positive and undesirable outcomes when a technology is at its preliminary stages of development and subsequently propose mechanisms (e.g. design, policies, standards) to facilitate favorable effects and overcome adverse consequences. To implement such mechanisms, researchers, technologists and policy makers need to engage in a multi disciplinary discourse. Futures research and scenario building can also be used as tools to explore techno-policy related questions such as: Which policies can be globally acceptable? Who is to decide what is desirable (or what is responsible)? Who is in a position to implement and enforce such policies? How do we measure the success of these policies and when?

Using a rigorous methodology to analyze various technological trends might encourage forward thinking research. Analyzing such trends can also highlight areas that IS research is lacking (e.g. the digital divide, culturally dependent theories, and unintended consequences of IT). To achieve such a shift, we need to explore how other disciplines use Futures methodologies and augment the way we educate managers and MIS scholars.

As Paul used to say: "Our discipline's research is like driving through the rearview mirror." It is my belief (and maybe that of the contributors to this special issue) that we as a multifaceted discipline are ready to begin driving looking frontward.

References

Gray, P., & Hovav, A. (1999). "Using scenarios to understand the frontiers of IS. *Information Systems Frontiers, 1*(1), 15–24.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: a stakeholder analysis. *Communications of the Association for Information Systems, 34*(50), 893–912.

Hovav, A., Hemmert, M., & Kim, Y.-J. (2011). Determinants of internet standards adoption: the case of South Korea. *Research Policy, 40*(2), 253–262.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants of computer-mediated transactions: a cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13–45.

Kling, R., Lamb, R. (1996). Analyzing Alternate Visions of Electronic Publishing and Digital Libraries. Scholarly Publishing: The Electronic Frontier. R. Peek and G. Newby. Cambridge: The MIT Press, 1:17–54.

Markus, L. M. & Mentzer, K. (2014). Foresight for a responsible future with ICT. *Information Systems Frontiers, 16*(3). doi:10.1007/s10796-013-9479-9.

Oh, O., Agrawal, M., & Rao, H. R. (2011). Information control and terrorism: tracking the Mumbai terrorist attack through twitter. *Information Systems Frontiers, 13*(1), 33–43.

Olla, P., & Choudrie, J. (2014). Mobile technology utilization for social development in developing countries: an ethnographic futures research study. *Information Systems Frontiers, 16*(3). doi:10.1007/s10796-013-9477-y.

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. (2011) The underground economy of spam: a botmaster's perspective of coordinating large-scale spam campaigns, Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats, March 29, 2011, Boston, MA.

von Schomberg, R. (2011). Introduction. In: R. von Schomberg (ed.): Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. A report from the European Commission Services. European Commission, Directorate-General for Research Science, Economy and Society, pp. 7–15. http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf [last accessed 02/25/2014].

Wakunuma, K. J., & Stahl, B. C. (2014). Tomorrow's ethics and today's response: an investigation into the ways information systems professionals perceive and address emerging ethical issues. *Information Systems Frontiers, 16*(3). doi:10.1007/s10796-014-9490-9.

Anat Hovav is a professor at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, innovation management, and Futures research. Anat Hovav has published in internationally refereed journals such as *Information Systems Research (ISR), Information & Management, Communications of the ACM, Journal of Business Ethics, Research Policy, Computers & Security, Information Systems Journal (ISJ), Information Systems Management (ISM), Communications of AIS (CAIS), Information Systems Frontiers,* and *Risk Management and Insurance Review*. Dr. Hovav is the winner of the 2013 citation of excellence award. She has presented her work internationally in academic and industry conferences and workshops.