Profiles for Convenient Front-end Privacy

Ronald Maier
Dept. of Information Systems
University of Innsbruck
Innsbruck, Austria
ronald.maier@uibk.ac.at

Johannes Sametinger
Dept. of Information Systems – Software Engineering
Johannes Kepler University
Linz, Austria
johannes.sametinger@jku.at

***Abstract*— Privacy can be described as the state of being unaccompanied or unobserved without unauthorized intrusion. We define front-end privacy as privacy when accessing data from a device, e.g., when working jointly on a computer. This is a matter of visibility with the problem that information can get directly disclosed. In this paper, we will define kinds of information that we want to consider for not being disclosed or for being hidden on the screen. Starting from typical knowledge situations we will categorize what we call front-end situations and define risk levels. We then introduce spheres and profiles as a means to effectively and conveniently ensure front-end privacy. Usability and implementation considerations wrap up our approach to tackle this neglected form of privacy.**

Keywords-privacy; front-end privacy; profiles;convenience;

I. INTRODUCTION

In recent years, the share of work that can be characterized as knowledge work (KW) has risen continuously [1], comprising key characteristics of a wide array of activities concerned with creating, translating or applying new knowledge [2,3,4]. KW has strong communication, coordination and cooperation needs, is highly mobile, flexible, distributed and requires a strong yet flexible, personalized and adaptable support by information and communication technologies (ICT) [5]. Consequently, knowledge workers as users of advanced ICT want to have data with them, have full control about access to them, share them when, where and with whom they decide and yet be confident that valuable information and knowledge is protected against unauthorized access and use. Increasing requirements concerning usefulness, ease of use and convenience have been fulfilled with a plethora of ICT solutions that deploy simple mechanisms such as the more data are on the server, the more convenient is the access from wherever or the more data is on a mobile device, the easier it can be accessed by its user. However, users' valuable data are distributed across applications and computers, so that managing access privileges and knowing what happens to the data has become a nuisance to users. While organizations are increasingly aware that strong management of information security on an organizational level is important in today's knowledge economy and while on a societal level there has been substantial debate about privacy or the lack thereof backed by showcases such as the introduction of Google Streetview in Germany [6], awareness of the individual knowledge worker's role in information security management has only recently been put on the radar of information security management initiatives, e.g., [7,8,9]. Early computers were used to solve specific problems, e.g., spreadsheets to perform business calculations. Over the years and decades, we have moved more and more data onto our computers and have long ago reached the point where a work life without computers is not possible any more for most of us. In the early computing days, all data was kept centrally on mainframes. The personal computer has brought computing power onto our desktop, and the amount of data being administered has increased. The Internet has interconnected all these computers and taken more data on the computers, e.g., personal communication via e-mail. There is also a trend to centralize data again. Companies use servers to store and secure information. But also individuals use servers for the purpose of having data available on several client machines, e.g., to synchronize data between servers, both organization-internal and external to an organization, e.g., social business networks like XING or LinkedIn, laptops, smart phones, and home/office computers. Also, people increasingly use subscriptions to information, e.g., to get current weather information or to get current news headlines.

In the course of these developments, many knowledge workers have increasingly given personal information away for convenience and functionality. From the perspective of actual behavior, privacy seems to be a lesser concern for individuals. At the same time, many are annoyed about the lack of convenient possibilities for keeping their information secluded from unwanted access. In addition to the considerations on privacy of data held in remote servers and sent between the servers and the person's device which typically cannot be easily designed by individuals, knowledge workers enjoy freedom to personalize and design their own KW space, the front-end towards the diverse interconnected information spread over heterogeneous systems. People want to design (Gestalt) their KW space (including a network of selected people) in order to increase their individual productivity. They then use these KW spaces in diverse situations with a variety of requirements concerning privacy. It does make a difference whether we access our KW space alone or in company, at home, at an office or in a public place, just to mention a couple of cases. So far, there is a lack of concepts guiding us in secluding information from others while accessing it. Although individual applications offer numerous functionalities in order to decide how much information is disclosed, these functionalities are inconvenient, because knowledge workers typically switch continuously between accessing a plethora of applications with data distributed over many systems in order to pursue their activities.

In this paper, we will address the question on how users can balance convenience and privacy in various situations concerning a (set of) KW space(s) they access for activities they are engaged in. The paper's main aims are to describe barriers that

many knowledge workers face with respect to ensuring privacy of their data while still being able to perform their work tasks, to review opportunities offered by current applications that in combination can address the requirements and to provide concepts helping to design convenient solutions for managing front-end privacy. The paper is structured as follows. Section 2 discusses conflicting priorities between convenience and privacy. Front-end privacy is introduced in Section 3, where we also consider knowledge situations as well as privacy situations. At the end of Section 3 we discuss how users typically handle risks to front-end privacy and present some basic solutions. In Section 4, we introduce spheres and profiles as a means to provide front-end privacy. Usability and realization considerations are given in Section 5. Section 6 concludes the paper.

II. CONVENIENCE AND PRIVACY

Convenience is the "fitness or suitability for performing an action or fulfilling a requirement or something (as an appliance, device, or service) conducive to comfort or ease" [10]. It can be anything that is intended to save resources like time or energy. Inconvenience leads to frustration. The meaning of "convenience" can change over time. Something that is convenient today may be regarded as commodity in the future, e.g., mobile access to the Internet, GPS positioning. Privacy can be described as the quality or state of being apart from company or observation with the freedom from unauthorized intrusion [10]. Cultures and individuals have different considerations of what is private that are generally related with the particular environment in which privacy has to be considered [11], but there are also commonalities. Privacy is related to anonymity, where people remain unnoticed or unidentified in the public or in the Internet. Privacy is also an aspect of security. Privacy and convenience are at odds with each other. According to a poll, almost 70 percent of consumers do not mind if their identities are authenticated when they make a purchase, as long as their personal information is not collected [12]. It is surprising that users feel comfortable with the authentication of their identity. They want to have a secure, trusted transaction experience. Sometimes, they value convenience higher than privacy. Another survey has revealed that the top three privacy concerns of Internet users in the US have not changed from 2002 to 2008 [13]. This is despite the fact, that these years have seen a significant increase in online purchases. But people have become more concerned about the disclosure of their purchasing patterns. They also express a stronger desire to be notified about protection measures of their personally identifiable information. People also have become more concerned about the tendency of web sites to store information about sites that had been visited previously [13]. A requirements taxonomy for the reduction of web site privacy vulnerabilities is given in [14].

There are many examples, where convenience beats privacy, see for example [15]. Amazon can tell its customers what kind of books or music they might be interested in. Also, they do not have to retype their credit card numbers every time they make a purchase. Customers are happy because it is convenient. We often give away private information, because we get something valuable in return, e.g., frequent flyer miles, reduced prices in supermarkets, access from any device to documents stored on the web, exposure to significant others in social networks. We distinguish several forms of privacy:

- Information privacy. Privacy of any information that is personally identifiable, e.g., medical information, financial information, location-based information, information about someone's troubles with the law, lifestyle information, political information.
- Internet privacy. Same as information privacy, but considering any activities on the Internet, e.g., information that is shared in social networks, financial information that is transmitted and disclosed during online banking sessions. In social networks, users often are not aware of specific privacy settings and their consequences. This results in disclosed information without knowledge or consent of users.
- Back-end privacy. Privacy of data and activities on remote peers and servers. This is a matter of storage and whether we trust our service providers.
- Front-end privacy. Privacy when accessing data from a device, e.g., when working jointly on a computer. This is a matter of visibility with the problem that information gets directly disclosed. We usually want to see everything when alone, but want to hide specific things when not alone.
- Connection-based privacy. Privacy of data that is transferred between a local device and a remote machine. This is a matter of leaving data traces with the known problem of eavesdropping, e.g., unencrypted transfer of data like e-mail messages.
- Administrational privacy. Privacy of data protected from being disclosed to administrators. This is about access rights and needed trust to our administrators.

Privacy impact assessments are a public reaction against privacy-invasive actions of governments and corporations [16]. People increasingly want to know about organizations' activities and to have more control over their accesses.

III. FRONT-END PRIVACY

Front-end privacy is about information that we want to be displayed on our screens in specific situations.

A. Information on the Screen

Before we proceed, we have to define kinds of information that we want to consider for being hidden on the screen.

- File system. Branches of the file system can contain information that we do not want to be disclosed, i.e., we do not even want someone else to see that there is some information. Seeing the name of the file or folder can already be too much information. And, we do not want to have to say no when somebody else, e.g., our boss, asks us to open a specific folder or file.
- Applications. We sometimes do not want to disclose the fact to someone else that we have installed a specific application. For example, we do not want to unfold that we have a weakness for playing poker. Information about applications includes the start menu, control panel entries, desktop shortcuts, etc. In some situations, it is okay to disclose that we have an application installed (and often will not be seen anyway), but we

do not want to disclose the fact that we are currently running this application or that we have recently or frequently used it. With some applications, the opposite might be true so that we do not want to get caught not having (sufficiently) used the application.

- Application-specific information. Some applications manage extensive information and we want to disclose this information only partially. This is especially true for office applications like browsers, e-mail, contacts, and calendar. Information we do not want to unfold to everyone include specific calendar entries, specific contact information, parts of the browser history, etc.
- Alerts and Notifications. Alerts and notifications are given by the operating system or by applications. We treat them separately, because there are situations where we do not want to be disturbed by them at all.
- Connections. Which connections can be seen and used? At what level of detail can they be accessed?

B. *Knowledge Situations*

In organizations, it is common that administrators have full access to computers of employees. This makes administration of the ICT infrastructure much easier. Additionally, administrators can conveniently solve employees' ICT problems by using remote desktop connections, i.e., by having full control over employees' machines. Thus, administrators have potential access to an enormous amount of private data. We can argue that a computer paid for by a company is not supposed to have any private data on it. But even if this is the case, there are many possibilities to invade someone's privacy, e.g., data about what someone is currently working on, e-mail messages, and logon/logoff times. All too often we are unable to decide ourselves about how much privacy we are willing to barter for perceived value in general and convenience in particular. This is the case when using the infrastructure of our employer. When we use web sites and services like those provided by Amazon, Apple, Facebook or Google, then we often have two choices. Either we refrain from using the site or service. Or we give up privacy in accordance with the site or service provider. In addition to administrators and service providers, people around us to whom we can, should or must disclose our screen can intrude our privacy. When, for example, we sit in our office working on our computer, and someone is approaching us in order to make an appointment, we open our calendar and reveal information about delicate appointments. While disclosure of private data to administrators and service providers typically is on the radar of information security professionals and often dealt with using, e.g., awareness raising measures, policies and software-based counter-measures, the decision about how much information our work environment should disclose to us and others around us is not a simple one. Example privacy situations with potentially increasing attention from outsiders towards what happens on our screen are:

- Isolated. We work privately and isolated from other people, e.g., in a personal office or at home.
- Office work. We are surrounded by colleagues.
- Meeting. We are in a meeting with participants sitting together having our mobile devices in front of us.
- Public. We work in a public location, with outsiders being able to freely roam next to our mobile devices.
- Approached. We get approached by uninvited persons.
- Presentation. We present slides in front of people.
- Joint work. We jointly work on our computer.

These examples show how diverse situations can be among which people can switch. For example, in a team that closely works together, people would be expected to instantly switch between isolated work, approached and joint work as well as office work, joint work, ad-hoc meetings and presentations, just to mention a few switches that might occur frequently every day. The members of the team are not necessarily limited to organization-internal people. Advanced collaboration technologies foster virtual teams so that members can switch between these situations without being geographically collocated, e.g., using co-authoring tools, multi-party videoconference, screen and application sharing systems such as Adobe Connect, GoogleDocs, Microsoft Sharepoint or Skype. Our list of example privacy situations is non-exhaustive and can be extended almost to an infinitely long list of specific situations describing (slightly) different requirements towards privacy. However, with respect to the consequences for profiling and for restricting access of others to valuable personal information, the depicted dimensions seem to sufficiently describe a set of circumstances of privacy that seems conveniently manageable.

For example, we get informed about the fact that a new update from software XY is available as an inconvenient interrupt during a presentation. Or we get a notification about the arrival of an e-mail message, maybe even including information about its sender and the subject. Or we use the browser and reveal information about our browsing history. If we sit in front of our computer and jointly write an e-mail message, all too often this reveals much information about our e-mail traffic, like senders, receivers, subject lines, used e-mail accounts, folders, etc. As teachers at the university we sometimes need to look up an individual entry in a list like student grades in a spreadsheet. How do we get this information with the student next to us without revealing information that is not intended for this person? In contrast to the situation where we do something with someone else in front of our computer (known intruders), there are situations where someone approaches us without invitation (unknown intruders). If we work in a public place, people sitting next to us will see information that we are not willing to reveal, e.g., in an airplane, at the airport, at a conference. How do we foil uninvited people from staring at our screen? There are solutions that limit visibility of screens horizontally, however, this also encumbers joint work sharing the screen and people sitting behind us will still be able to observe our screen.

C. *Front-end Situations*

Applications typically operate based on the assumption that once a user is authenticated and authorized, she is the only one in front of the computer or all other persons that get a glance of the screen are authorized to see all information that the application reveals. In other words, the application interacts with the user without any consideration of the circumstances of the situation at hand. Take the example of online banking which not by coincidence has been termed "home banking". If a user

is in a public environment and simply wants to transfer an amount of money, this is often not possible without revealing further financial information such as the current balance on all accounts or the most recent transactions. We distinguish the front-end privacy situations *exposed*, *surrounded*, *together*, and *secluded*, see Fig. 1.

- Exposed. The display is exposed to the looks of others. For example, we make a presentation, or someone approaches us in order to set up an appointment.
- Surrounded. We are surrounded by people. The display is not directly exposed to the looks of others, but people can get a glimpse of what is on the screen. We may be approached rather quickly, e.g., we work in the lounge of an airport or in some other public place.
- Together. We are together with people we know and with whom we work together, e.g., in project meetings.
- Secluded. The screen cannot be seen by other people, e.g., we work alone in our office or at home.

The distinction among these situations is not always clear, but a finer granularity will counteract convenience.

D. *Front-end Risks*

The term risk is discussed heterogeneously and focuses either on its causes or its impacts. Risk is related to any business operation and includes possible losses that result from the realization of uncertain undesired events [17]. Risk can also be defined as a condition in which a deviation from a desired outcome can occur [18]. Deviations can refer to targets, plans or results of a decision. A potential positive deviation is considered as opportunity and a negative as threat or risk in a narrow sense. Moreover, risks can be characterized by a probability that an undesired event occurs and an extent of loss that goes along with the occurrence of this event [17]. Risk management typically comprises identification, assessment, governance and evaluation as basic steps [19]. Risk management has also been discussed with respect to knowledge assets, e.g., [20,21], and is part of formal organizational initiatives such as information security management initiatives, e.g., [7,8]. Risk management includes measures about how to deal with risks, specifically avoidance, acceptance, transfer, reduction, e.g., [22], based on [23]. Examples in this paper's domain are:

- Reduction**.** Privacy risks can be reduced, e.g., by using private acronyms and "cryptic" expressions in a calendar. Thus, if other people see the calendar entries, they at least do not immediately make sense to them.
- Acceptance. Many simply accept risks. If someone sends a job application via email from her current employer, then there is definitely a risk. Sometimes this is simply ignorance or lack of technological knowledge, i.e., the facts that email messages are sent via plain text and that administrators can easily read them.
- Avoidance. Risks can be avoided, for example, by sending text (SMS) from a private telephone instead of using email or by not storing selected sensitive information on a computer at work.
- Transfer. Risks can also be transferred to another party, for example, by insuring against problems resulting from information being disclosed to competitors. However, this is associated with additional costs.

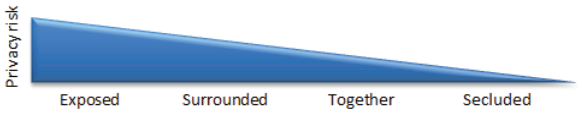

Figure 1. Risk levels of front-end privacy situations

Most individual users will not go to the trouble of formally assessing their risks and deploying corresponding personal risk management measures. Instead, users resort to convenient measures in order to save time and energy and interfere as little as possible with the pursuit of their goals. Concerning connection-based privacy, users on the one hand typically trust secure connections like https or VPN and on the other hand do not have any alternatives in regular transactions they are engaged in. Concerning administrational privacy, many users are aware that the policies in place are not sufficient and that they have to take into account the possibility that administrators access their data beyond administrational duties. While users are increasingly aware of back-end privacy issues, it seems like most people are not yet aware of potential breaches of front-end privacy which are consequently not dealt with appropriately.

E. *Partial Front-end Solutions*

There are solutions available that solve parts of the problem. For example, MindGems offers *Boss Key,* an application that hides and restores windows when pressing a hotkey. It covers tracks of running programs, even from the task bar and the system tray. These applications are kept hidden in the background and can later be restored from the point of interruption [24]. MS Outlook provides the possibilities to create several folders for mails, contacts, calendars and task lists. These folders can be given different permissions and they can be visualized in overlay mode. But all data still resides on one single server. It is not possible to combine information from two different servers, say one for a highly confidential research project and another one for corporate use.

IV. SPHERES AND PROFILES

Data, applications and network connections can be used for several purposes. Some of them are closer to one purpose than to another. For example, a project manager uses project management software, presentation software and a collaboration client to manage data about a project and to communicate with project members while she uses an enterprise resource planning software accessing data on personnel, material and other resources for administrative purposes. In this case, the workspace can straightforwardly be divided into two parts. However, the two parts can overlap due to using the collaboration client also for exchanging data with administrative or controlling units.

A. *Spheres*

The phenomenon of overlapping workspaces can be described with the metaphor of information spheres. The term sphere means "any of the concentric and eccentric revolving spherical transparent shells in which according to ancient astronomy stars, sun, planets, and moon are set", a "natural, normal, or proper place", "an area or range over or within which

someone or something acts, exists, or has influence or significance" [10]. An information sphere is a collection of objects, specifically information (contents, documents etc.), applications and pieces of information used in these applications. Objects in spheres "gravitate" around a user-defined purpose. Examples are a project or an ongoing individual or collective activity, e.g., joint experience or collaboration with persons. Spheres have conceptual rather than physical boundaries and are transparent with respect to where, i.e. on which devices or machines, objects are located. Using the metaphorical analogy of the term denoting parts of the celestial system, gravitational forces metaphorically mean that objects are attracted to other objects. Objects potentially belong to several spheres as gravitational forces from objects in several spheres can be at work. The definition of spheres is inherently a user task. But automatic definition can be supported by classifications based on machine learning algorithms that are similar to the ones that are used for task detection. The following dimensions can help to guide a user in defining a sphere:

- When. Time is the primary dimension for presenting objects. It is the pace making dimension of KW.
- Why. Purpose is a leading dimension because it defines the center of a sphere and the gravitational forces that are at work. It is the sense making dimension of KW.
- Who. The dimension about persons and institutions defines who else is involved in a sphere. For example, it influences access rights to others' collections of objects or allocation of communication acts to spheres. This is the networking dimension of KW.
- How. Format and type define how knowledge is materialized and is the representational dimension of KW.
- What. Topic and domain define what a sphere is about thematically and thus is the content dimension of KW.
- Where. Location primarily acts as a proxy for contextual factors that come into play when accessing a sphere in a specific geographical location. It is the situational dimension of KW.

Meta-information about documents contains values for these dimensions, e.g., time of document creation or modification, names of authors, file types. The risks of front-end privacy breaches can be reduced by defining and activating spheres and consequently by restricting data, applications and connections that are disclosed in a situation to those that are part of the currently activated sphere. In order to simplify this process we suggest profiles, which are described in the subsequent section.

B. *Profiles*

We suggest the use of profiles that we see as filters and set them in order to selectively reduce the amount of information being disclosed on the screen. For that purpose, we define ranges for the dimensions presented in the previous subsection. Values can be including or excluding. For example, let's say we define the range 2013 in the dimension "when". This includes everything within the year 2013. The range "not 2013" has the opposite meaning. We can filter persons or organizations in the "who" dimension. The how dimension lets us filter specific file formats or information items like calendar items, etc. Figure 2 shows a profile sample where we include everything in the year 2013 that is about front-end privacy and has the persons R. Maier and J. Sametinger assigned. Additionally, we restrict the profile to text documents, images, slide presentations, and email messages. It will be useful to let users combine file extension like .gif, .jpg, .png and others to an image category, or any office document to an office category.

Dimension	Filter
When	2013
Why	Front-end privacy
Who	R. Maier, J. Sametinger
How	.doc, .ppt, .jpg, email
What	-
Where	-

Figure 2. Sample profile

Some values in our dimensions can easily be filled automatically, e.g., the when dimensions. Every file in a file system has dates associated with it, e.g., date of creation or last modification. Persons and organizations can also be retrieved quite easily. The why and what dimensions are more difficult to fill. Users are not willing to manually fill in meta-information for their documents. Simple automatisms and heuristics have to be used for that purpose. For example, folder or file names can be used for the why dimension. In the example of Fig. 2, this will include everything that is stored in folders named "front-end privacy". The "what" dimension defines topics. For user convenience, we suggest to let users define values for this dimension arbitrarily. For the "why" dimension we suggest heuristics to be defined in order to assign useful values. The dimension "where" can be seen in many different ways. It can mean the location where information is stored. This can be a geographic location or the name of a server or a cloud. It can also be the location that is assigned to a person or organization. For example, Linz and Innsbruck can be used in that dimension and can, thus, include all persons that live or work in these towns. In this case, contact information can be used to find out who is at which location. However, contact information usually illustrates the current situation. If someone moves from one location to another, then automatic assignments become more difficult and error-prone. For information filtering, we have to define the effects of filters for different types of information.

- File system. Meta-information about files and the names of enclosing folders for the "why" dimension.
- Applications. Applications can be restricted to the ones that are necessary to work on documents that pass a specific filter. Separate application profiles can also be used in order to hide applications in specific situations.
- Application-specific information. Applications often store information in big files. If stored separately, meta-information about the separate files could be used for filtering. Thus, filtering can be done outside the application. If single files are used, then the application will have to do the filtering.
- Alerts and Notifications. Applications running in the background can send alerts and notifications at any time. If applications are filtered, then their alerts and notifications should be postponed until the application becomes active, i.e., unfiltered, again.

V. USABILITY AND REALIZATION

In this section we will discuss the usability of filters and how profiles can be implemented.

A. Usability

Even though front-end privacy is important to users in various situations, they are usually not willing to expend any extra effort for that purpose. Particularly, they cannot be expected to fill in meta-information for documents. As mentioned earlier, we have to define simple heuristics in order to provide values for specific dimensions. We imagine a widget with 4 front-end privacy situations, the 3 most commonly used profiles, and the other ones available via pop-up. These should be pre-configured along the lines described above and the widget should offer the possibility to create new and configure existing profiles. We also imagine an intrusion hotkey. Profiles should be switchable via hotkeys and they should not (always) be visible on the screen, because others get suspicious if they realize that we switch to not-alone when they are approaching. If we add a new contact or create a new file, it can automatically be assigned to our current spheres or spheres are determined by the category we assign it to in our mail system.

B. Realization

It is not possible to develop an application that can implement the functionality on top of current operating systems and applications. Spheres and profiles are hard to implement without modifications in an operating system. The file system has to filter files according to active profiles. Application-specific information is specific to applications only because these applications, i.e., their developers, have decided to do so. For example, contact and date entries can be stored as file each in a specific location on disk. If filtering is done on the file level, then applications do not have to care about filtering. Alerts and notifications are usually done by calling operating system functions that open a dialog or display a message. If the operating system had the information about active profiles and knows that the call of a function, i.e., displaying information, is in order to provide an alert or a notification, then this information can be postponed until an application becomes unfiltered again. Apple's notification center provides some of this functionality.

VI. CONCLUSION

We discussed conflicting priorities of privacy and convenience. After the description of various forms of privacy we introduced front-end privacy in more detail, considering knowledge situations, front-end situations, and front-end risks. There are rudimentary approaches for front-end privacy, but they are far from being helpful in typical settings and practices of knowledge workers. We then described spheres and profiles that can provide front-end privacy conveniently and effectively. We outlined possible solutions but we have so far stood back from implementing such a solution, because we need some extensions to the operating system with additional interfaces for applications. And, not all but some of today's most frequently used applications, with the MS office suite as a prominent example, will have to store information in a different way. We believe, however, that our reflections on front-end privacy are helpful to embark on a learning journey of how to improve their front-end privacy. Our suggested changes are not really extensive, yet would greatly enhance chances that users not only are aware of front-end privacy, but can readily deal with the issues they identify. If we attribute enough importance to this form of privacy, software vendors will follow suit.

REFERENCES

[1] E.N. Wolff, The growth of information workers. CACM, 48, 37-42, 2005.

[2] P.F. Drucker, Landmarks of Tomorrow, New York, Harper, 1959.

[3] E.K. Kelloway, J. Barling, Knowledge Work as organizational behavior. International Journal of Management Reviews, 2, 287-304, 2000.

[4] U. Schultze, On Knowledge Work. In: HOLSAPPLE, C. W. (ed.) Handbook on Knowledge Management. Berlin Springer, 2003.

[5] R. Maier, T. Hädrich, R. Peinl, Enterprise Knowledge Infrastructures, Berlin, Springer, 2009.

[6] Spiegel, Google Launches Street View Germany, Spiegel Online International, 11/18, 2010. http://www.spiegel.de/international/business/0,1518,729793,00.html

[7] M.E. Johnson, E. Goetz, Embedding Information Security into the Organization. IEEE Security & Privacy, 16-24, 2007.

[8] Q. Ma, A.C. Johnston, J.M. Pearson, Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security, 16, 251-270, 2008.

[9] M. Siponen, R. Willison, Information security management standards: Problems and solutions. Information & Mgmt., 46, 267–270, 2009.

[10] Merriam-Webster, 11th Collegiate Dictionary, 2004.

[11] E.L. Bertino, D. Lin, W. Jiang, A Survey of Quantification of Privacy Preserving Data Mining Algorithms. In: AGGARWAL, C. C. Y., PHILIP S. (ed.) Privacy-Preserving Data Mining: Models and Algorithms. Ney York: Springer, 2008.

[12] D. Takahashi, Web users will trade privacy for security and convenience, VentureBeat, September 2009. http://digital.venturebeat.com/2009/09/15/web-users-will-trade-off-privacy-for-security-and-convenience/

[13] A.I. Antón, J.B. Earp, J.D. Young, How Internet Users' Privacy Concerns Have Evolved since 2002, IEEE Security & Privacy, Vol. 8, No. 1, pp. 21-27, Jan/Feb 2010. http://doi.ieeecomputersociety.org/10.1109/MSP.2010.38

[14] A.I. Antón, J.B. Earp, A Requirements Taxonomy for Reducing Web Site Privacy Vulnerabilities, Requirements Eng. J., Vol. 9, No. 3, pp. 169–185, 2004.

[15] T. Weber, Will convenience beat privacy? BBC News, January 2006. http://news.bbc.co.uk/2/hi/business/4649292.stm

[16] R. Clarke, Privacy impact assessment: Its origins and development, Computer Law & Security Review, Vol. 25, Issue 2, 123-135, 2009. doi:10.1016/j.clsr.2009.02.002

[17] S. Kaplan, B.J. Garrick, On the quantitative definition of risk. Risk Analysis, 1, 11-27, 1981.

[18] R.R. Gallati. Risk mgmt. and capital adequacy, NY, McGraw-Hill, 2003.

[19] C.A. Archbold, Managing the bottom line: risk management in policing. Policing: An International Journal of Police Strategies & Management, 28, 30-48, 2005.

[20] J. Jordan, J. Lowe, Protecting Strategic Knowledge: Insights from Collaborative Agreements in the Aerospace Sector. Technology Analysis and Strategic Management, 16, 241-259, 2004.

[21] K.C. Desouza, G.K. Vanapalli, Securing Knowledge in Organizations. In: DESOUZA, K. C. (ed.) New frontiers of knowledge management. Basingstoke: Palgrave Macmillan, 2005.

[22] D. Baccarini, G. Salm, P.E.D. Love, Identification and Management of Risks in Information Technology Projects. 14th Australasian Conference on Information Systems. Perth, Australia, 2003.

[23] H. Zhi, Risk management for overseas construction projects. International Journal of Project Management, 13, 231-237, 1995.

[24] MindGems, BossKey, http://www.mindgems.com/products/Boss-Key/boss-key.htm