Digital Identity and Access Management:

Technologies and Frameworks

Raj Sharman
State University of New York at Buffalo, USA

Sanjukta Das Smith
State University of New York at Buffalo, USA

Manish Gupta
State University of New York at Buffalo, USA

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Senior Editorial Director: Heather Probst
Book Production Manager: Sean Woznicki
Development Manager: Joel Gamon
Development Editor: Joel Gamon
Acquisitions Editor: Erika Gallagher
Typesetters: Mackenzie Snader
Print Coordinator: Jamie Snavely
Cover Design: Nick Newcomer, Greg Snader

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Digital identity and access management: technologies and frameworks / Raj Sharman, Sanjukta Das Smith and Manish Gupta, editors.
p. cm.
Includes bibliographical references and index.
Summary: “This book explores important and emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes”--Provided by publisher.
ISBN 978-1-61350-498-7 (hbk.) -- ISBN 978-1-61350-499-4 (ebook) -- ISBN 978-1-61350-500-7 (print & perpetual access) 1. Computer networks--Security measures. 2. Computer networks--Access control. 3. Computer security. 4. Online identities. 5. Online identity theft--Prevention. I. Sharman, Raj. II. Smith, Sanjukta Das, 1978- III. Gupta, Manish, 1978-
TK5105.59.D54 2012
005.8--dc23

2011036891

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 7
Separating Private and Business Identities

Gábor György Gulyás
Budapest University of Technology and Economics, Hungary

Róbert Schulcz
Budapest University of Technology and Economics, Hungary

Sándor Imre
Budapest University of Technology and Economics, Hungary

ABSTRACT

As various information technologies are penetrating everyday life, private and business matters inevitably mingle. Separating private and business past records, public information, actions or identities may, however, be crucial for an employee in certain situations. In this chapter we review the interrelated areas of employee privacy, and analyze in detail two areas of special importance from the viewpoint of the separation: web and social network privacy. In relation to these areas we discuss threats and solutions in parallel, and besides surveying the relevant literature, we also present current Privacy Enhancing Technologies applicable in each area. Additionally, we briefly review other means of workplace surveillance, providing some insight into the world of smartphones, where we expect the rise of new privacy-protecting technologies as these devices are getting capable of taking over the functions of personal computers.

INTRODUCTION

The workplace is an area where the employee devotes his time and expertise to achieving goals designated by the employer; however, it is not possible to reach the total absence of private life in a workplace (Szabó & Székely, 2005). There are two typical cases where the employee's privacy may be violated by the employer; at labor recruitment and during employment, but there may be other cases as well (e.g. when the employee is forced to submit herself to personality tests). During these encounters the employer may collect information about the employee's private life, for instance, by searching for public records before conducting a job interview (Microsoft Research,

DOI: 10.4018/978-1-61350-498-7.ch007

2009), or pursuing surveillance during work time activities referring to security or other reasons.

Setting aside the legal aspects – as they vary in many countries (Privacy International, 2011) – we analyze how Privacy Enhancing Technologies (PETs) can be used to hide one's private life from the prying eyes of an employer. The purpose of the paper is to present possible technologies and techniques involving some theoretical solutions suitable for assembling a privacy protective portfolio that can be adjusted to the local legal aspects in any country. Therefore we intend to present a practical solutions with some theoretical background, focusing primarily on the technical side of the problem.

The outline of the paper is as follows. Since the selection of categories of breeching employees privacy is based on the work of Szabó & Székely (2005) we briefly present the relevant aspects of their analysis first. The focal point of our work is the discussion of three areas from the viewpoint of employee privacy. First, web privacy issues are discussed, including the analysis of the importance of information superpowers, but focusing on how privacy can be demolished by tracking user activities on the web and by using public Web 2.0 data sources. Then the significance of social networks is presented, and before concluding our work, other means of privacy violation are also briefly discussed.

BACKGROUND: ANALYSIS OF SCENARIOS IN HUNGARY

Szabó & Székely (2005) analyzed numerous complaints that were filed to the Hungarian Data Protection Commissioner from a non-technical, legal point of view in the context of Hungarian law. Their work includes a classification of the cases based on the purpose of the employer and determines four categories such as labor recruitment, work control and supervision, personality tests and other cases of unreasonable privacy violation.

During labor recruitment, the employer's goal is to learn about the applicants' personality, medical status and past records in order to choose the most adequate candidate for the job. This inevitably includes privacy-related issues, such as various kinds of (unnecessary) medical examinations, personality tests, using of lie detectors or exaggerated data inquiry. However, the internet can be also used as a data source for such investigations, since the purpose of many web services (e.g., social networks) is to gather and provide information on individuals.

Personality tests are usually conducted offline, and should be avoided by legal means if possible. Some of the issues reported in the work of Szabó & Székely, under the category of other cases of unreasonable privacy violation can be avoided by using PETs, but some do not even need them. For instance, the authors mentioned employers who were investigating the political background or the religious beliefs of applicants. These issues should be hindered by using PETs related to the first two categories, and if this is not possible, these issues need to be solved by other means, e.g. through legal redress or involving commissioners.

In case of successful recruitment, it is important for the employer to ensure that the employee devotes his time and expertise to the designated tasks. This can lead to work control and supervision over the concerned services, software or hardware provided by the employer, which does not necessarily imply the violation of the employee's privacy; however, some actions in the employee's personal life will inevitably take place during the working hours. This is even more likely to happen if corporate access is provided to public services like phone networks or the internet. Therefore, it is important to separate private and business actions in these cases as well.

In accordance with the work of Szabó & Székely, we selected web and social network privacy as these can be involved during the application

process and employment alike. Besides, there are many less relevant, but existing problems, some of which are also analyzed – these are discussed under the category of other issues.

PRIVACY ON THE WEB

Tracking users on the web has a long history. At the beginning of the web it was possible to identify users by their IP addresses, later by the identifiers stored on their computers (Gulyás et al., 2008). Over time, these techniques became more and more sophisticated as the business value of uniquely identified users and profiling had been recognized. As companies with extensive service portfolios and services based on voluntarily submitted personal data appeared, new data sources became available. From the viewpoint of separating private identities from business ones, all areas should be considered, but probably the latter seems to be the most sensitive: companies can also search for previous blog posts, web pages, or other kinds of small pieces of information containing personal information about the applicant or the employee.

Information Superpowers

Today, there are several companies on the web offering a wide scale of services with single sign-on (e.g., search services, mail, and calendar). These companies usually offer their services for free, but in return they analyze the uploaded content and display advertisements. Besides allowing an insight into the uploaded private information, meta-data about the user are also revealed (e.g., first and last time of reading mails, daily routine, relaxation habits, interests) leading to extensive inter-application surveillance, as the content of different applications can be easily linked by the host.

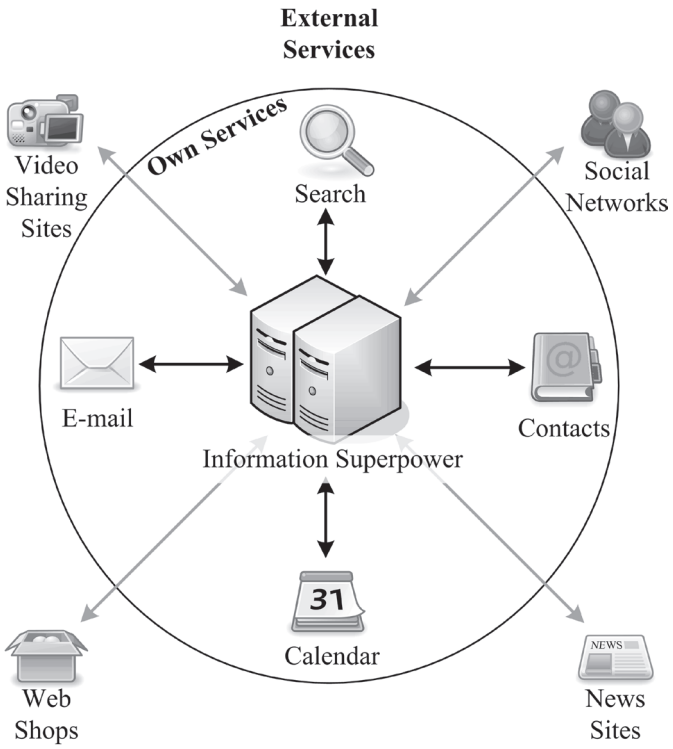
These companies do not necessarily need to remain within the border of their services. For instance, by offering web analytic services, they can monitor how visitors browse across websites, and some of these tracked visitors can even be identified by their login name (Krishnamurthy & Wills, 2009). As the majority of web analytic services are provided by only a handful of companies that also serve a vast number of users with their applications, and therefore manage a huge amount of personal information, we call these information superpowers. Figure 1. illustrates the nature of information superpowers and some typical services they can access.

Usually, these services do not publish content by default, but some may have built-in social networking functionality. However, the related options should be revised from time to time, since new privacy settings may appear and new defaults can be set. The Privacy Policy changes committed over time by Facebook are good examples for that (McKeon, 2010). New functions or related services that publish private information can also appear, as was the case with Google Buzz (Wood, 2010). Therefore, an employee (or a job applicant) should consider managing the privacy settings carefully, and should avoid publishing sensitive material (e.g., via Google Reader) – self-consciousness might be even more important if the employer is the same company as the one running the concerned services.

Separating workflows is a powerful way of enhancing privacy. For services requiring logins, multiple unlinkable registrations can separate personal and business identities if they are accessed with anonymous web browsers (discussed in the next section). If logging in is not mandatory, then service specific PETs can be used to avoid profiling. For example, GoogleSharing is a Google-specific PET allowing access the public Google services anonymously (Marlinspike, 2010). As GoogleSharing provides anonymity, sequentially entered search queries sent by the same user are unlinkable for Google.

Open source alternatives can substitute some services of information superpowers. For example,

Figure 1. Information superpower inside the border of its services, and the outer world



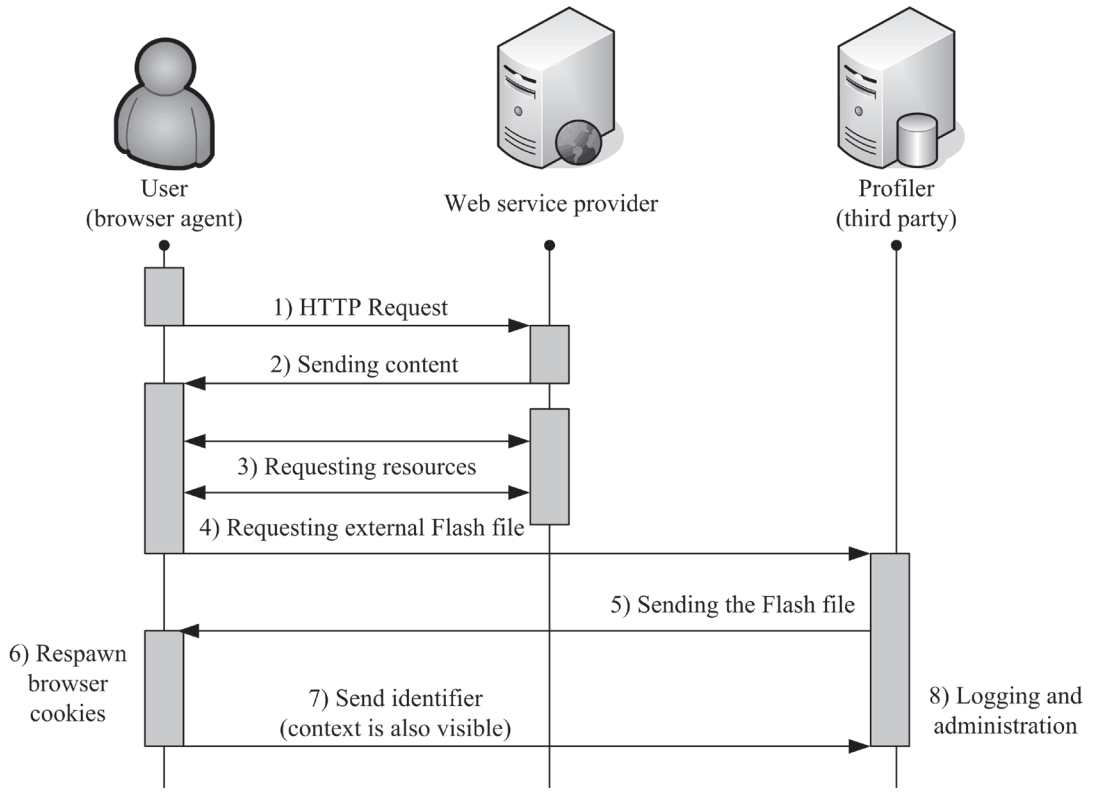
FengOffice (FengOffice, 2010) offers a web based calendar and task manager besides the regular web office suite (the latter can manage documents and presentations). As this is open source software, it can be freely installed on the employee's computer to allow her exercising total control over the uploaded data.

Tracking Users on the Web

The overall goal of tracking users on the web is to link user activity to a pseudonymous or a personal profile (Gulyás et al., 2008). Profiles can be created for various reasons, such as behavioral profiling, profiling for targeted advertising, or dynamic pricing. Large and complex profiles are more useful for these purposes, but creating such profiles requires users to be identified and recognized across websites. This kind of profiling is also relevant from the viewpoint of an employee who intends to separate her business and private life even if she is not working for a company, which is trying to track her activities. Local databases (e.g., cookies, history databases and cache, and other client-side storages) on her working computer can contain private information, which makes it possible to rebuild a complex behavioral profile on her.

Nowadays, there exist numerous techniques for online profiling and surveillance, and many of the leading web services are using them (What They Know, 2010). Initially IP addresses were used as user identifiers when IP changes and multiple users on personal computers were rare. As IP addresses became dynamic over time, this technique was not accurate enough anymore, and tracking cookies have replaced them. These identifiers are stored in the user's profile by the web browser application. Besides identifying returning visitors, tracking cookies can also be used to track user

Figure 2. The operation of Flash PIEs and cookie recreation



activities across different websites by embedding "detectors" into the content of the cooperating websites. For instance, web bugs (typically small 1x1 pixel transparent GIF images) specifically used for tracking, are still in use on many popular websites (Carver et al., 2009).

In addition to tracking cookies, "detectors" of other media types became also widespread for cross-domain user tracking. Adobe Flash (Adobe Systems Incorporated, 2010) is a popular extension for animation and interactive graphics used on many websites. Similarly to web browsers, the Flash player also provides its own cookies that can be used for storing identifiers. Soltani et al. (2009) found that a significant number of websites used Flash cookies to recreate deleted web browser tracking cookies. However, Flash cookies are also available as tracking cookies called Persistent Identification Elements, or PIEs for short (Gulyás et al., 2008). Figure 2. illustrates how Flash cookies can be used for tracking and restoring web browser cookies.

There are techniques that do not need to store additional data on the client-side: history stealing attacks aim to read the history of the web browser via web scripts. As browser history should be unique for most users, it can even be used to identify the user by determining her social networking profile (Wondracek et al., 2010). However, the fate of history stealing attacks is already sealed, as the API deficiency that allows history stealing attacks is going to be patched in Firefox 4 (Stamm, 2010), and other browsers are also expected to do the same in the near future. When direct monitoring of the local network is not possible, or for some reason the employee's computer is inaccessible for the company, history

stealing can be used on the local corporate intranet to sniff what employees are browsing on the web.

There is a novel method combining all available local storage methods and flaws that can be exploited for storage, called evercookies (Kamkar, 2010). Evercookies use almost a dozen storage methods, and therefore they are quite resistant against attempts to clear browsing history and local storages. However, web browser vendors and plugin developers recognized these flaws, and the revision of local storage management can be expected as a response (Huang, 2011).

As a reaction to tracking issues, a novel feature called private mode has been implemented in modern browsers, aiming to provide protection against local observers (e.g., other users, administrator) by hiding traces of the user's activity, and also by making sessions unlinkable for service providers. Recent research has shown that private mode implementations failed their objectives in several browsers, and in addition, different plug-ins and extensions also allow the profiling of users (Aggarwal et al., 2010). Moreover, passive fingerprinting techniques can also be used to identify users (Eckersley, 2010). By comparing the fingerprints of modern web browsers in private mode, we found that the fingerprints were the same in normal and private mode (e.g., the font list, same settings, plug-ins are still visible to the visited site). According to Eckersley (2010), these fingerprinting techniques, together with IP addresses can also be used to restore tracking cookies; therefore, web browsers in private mode are also vulnerable to being tracked.

Although IP addresses allow imprecise identification only, hiding these addresses seems to be important, as the latter example emphasizes. For IP hiding, anonymous proxies are the simplest solutions; however, their architectural simplicity is also their weakness: the user has to place confidence in a single server (Gulyás et al., 2008). Mixes (Chaum, 1981) provide a better network level protection against both the unreliable servers in the network and the remote target. Additionally, MIXes provide extra protection against local observers. For example, in order to use the popular service called Tor (Dingledine et al., 2004), users need to install a local proxy on their computer that connects them to the anonymizing network. For employees, this is favorable: their connection is protected on the local company network against surveillance and censorship, and the visited websites cannot determine their IP addresses either.

The most complex PETs offering protection against all the aforementioned techniques of tracking user activities on the web are called anonymous web browsers (Gulyás et al., 2008). Modern anonymous web browsers, such as JondoFox (JonDos GmbH, 2010), are portable, offer tools for maintaining local databases (e.g., Flash cookie filtering), filter malicious content (e.g., web bugs, untrusted JavaScript) and apply network level anonymizing services for hiding the user's IP address. Considering their functionality, it can be stated that anonymous web browsers offer the most powerful privacy protection for users. The necessary level of protection is also guaranteed for privacy-aware employees for local databases and against possible network observers.

Profiling by Collecting Information from Public Sources

Numerous web services, especially Web 2.0 sites, are specialized in user contribution, and encourage their users to submit large amount of personal data, which often get published worldwide without any access control provided. These services include, but are not limited to social networking sites, content sharing sites, blogs, micro-blogs, forums, etc. Besides the lack of control over data publication, the evolution of search engines also played an important role in this process by organizing content and enhancing ease of access. For some Web 2.0 services, real time search is also provided (Singhal, 2009), which raises further privacy issues: as published data are immediately accessible

via search engines, the revocation of information becomes very difficult or even impossible.

There are other, more alarming ways–completely disregarding the data subjects' approval–for service providers to access private data, which can also be used for abuses. For instance, tagging people on images is a popular feature on Facebook which allows tagging people either by their names and a link to their profiles or only by their names. The latter can be abused as it requires no confirmation from the tagged user, and removing such tags by others than their poster is not possible (Boutin, 2009). Allowing the website to access and search through one's email account is another popular feature that helps people build up their social network. However, as we pointed out earlier, even errors in privacy policies can lead to these kinds of breaches (Wood, 2010), and ownership issues or the difficulties around data revocation are just additional factors complicating the situation (Schroeder, 2009).

These issues should be considered both by applicants and employees. During the application process, a company can search for past records on the applicant (Microsoft Research, 2009), and, even during employment, the company can keep employees under control by collecting information from public sources (Matyszczyk, 2009). Therefore, besides raising the employees' own privacy-awareness on publishing content, it is important to technically separate sensitive information by means of access control. (Nevertheless, in cases where data publication is not voluntary, there is not much a user can do technically.)

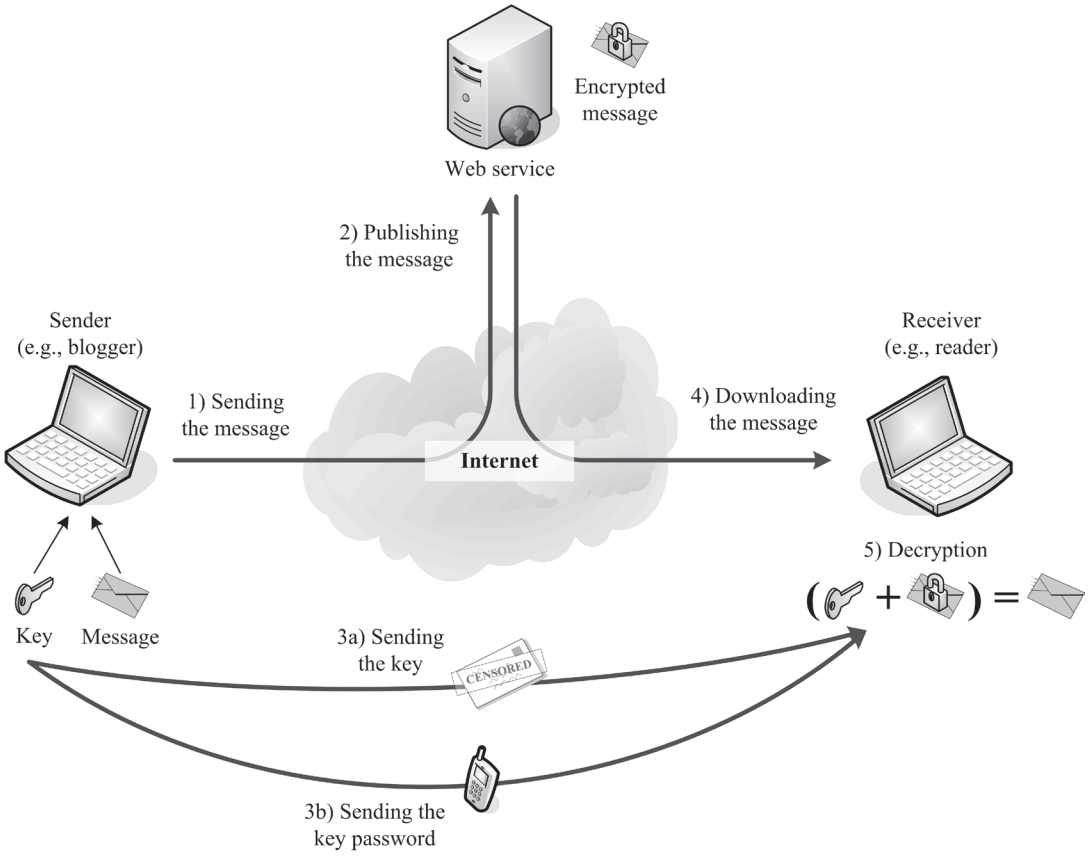
There are several solutions for managing access control, but small, client-side applications using cryptography are the best practical choices (Paulik et al., 2010). These solutions provide strong confidentiality over the encrypted data due to strong encryption, and require no trust in the service provider or any third parties. However, Paulik et al. (2010) defined further requirements to be considered while choosing the proper software. Such an application should be gradually deployable for clients using the same service, and universal in order to be compatible with most popular services. The authors also emphasize usability without compromises and easy installation as the use of such software is intended for non-technically oriented people, too.

The FireGPG Firefox extension is a piece of generic encryption software allowing symmetric and public key encryption, also capable of encrypting messages posted on the web (Cuony, 2010). Although it is available as a Firefox extension, one of its main drawbacks is that it is not standalone: the user must have the GNU Privacy Guard installed to use it. This may be a convenient software for professional users, but the installation can be quite cumbersome for an average user, and its rich functionality can also be confusing.

The BlogCrypt Firefox extension allows only symmetric encryption, but it is more user-friendly, as it was specifically designed for web encryption (Paulik et al., 2010). The key management of BlogCrypt was designed for the structure of the web, since keys are identified by the domain name and a locally unique key identifier. Encrypted text appears on sites as a Base64 coded string, starting with a header tag including the related key identifier–the extension automatically tries to decrypt these content blocks if the key identifier is stored in its database. The operation of BlogCrypt is illustrated on Figure 3.

While BlogCrypt was primarily designed for regular web pages (though manual decryption works with AJAX-based software also), it is also possible to insert a cryptographic layer between the client-side software and the service provider in Web 2.0 applications. SeGoDoc is a client-side cryptographic solution designed this way: it demonstrates this functionality for Web 2.0 services using the AJAX technology by cooperating with Google Docs (D'Angelo et al., 2010). There are even further alternatives, and more software will be cited in the next section relating to social networking. Some of these tools can also be used for the web in general. For a more comprehensive

Figure 3. The operation of the BlogCrypt Firefox extension

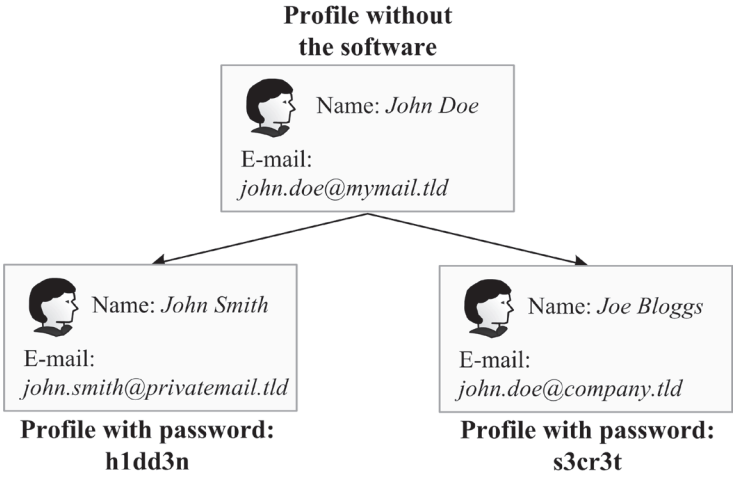


comparison of related software see the work of Paulik et al. (2010).

According to Paulik et al. (2010), the ideal PET for providing access control applies steganography. Here we give an insight into how such software could operate on social networking profiles–describing the generic solution in detail is beyond the scope of this article, and we leave that for future work. The core concept is as follows: after detecting that a password is assigned to the profile (e.g., after storing a local database of user ID and password pairs) the software retrieves real attributes by using the password and replaces them with the originals. This concept is visualized on Figure 4. by introducing an identity management-like scenario.

The retrieval can be realized by using random addresses identified by the password at an arbitrarily selected third party service (e.g., the hash value of the password can be used as the address identifier). Thus, different passwords would produce different address and content. As the content would be encrypted with the password, and the address would not contain the password itself, the third party service could not jeopardize revealing the real content, and backward linkability would not be possible. We note that as the retrieval process is based on the password, identity management can also be realized based on these principles (e.g., simply by assigning different passwords for distinct groups).

Figure 4. Different keys used to reveal different sets of data (i.e., profiles)



SEPARATING IDENTITIES IN SOCIAL NETWORKS

Social networks are getting more and more integrated into our private life, and therefore the use of these services at the workplace is nearly unavoidable. The result of the FaceTime (2008) survey shows that 51% of employees use these services every day; however, social networks raise several privacy issues concerning the relation of the employer and the employee, for instance, the separation of private and business identities (e.g., separation of registrations for the current and job seeking identities), separation of contacts (e.g., friends and colleagues), contact lists, group memberships, limiting access to events (e.g., personal activities) or hiding sensitive profile information (e.g., state of pregnancy). There are a few additional privacy issues derived from these, such as information flow control (Chew et al., 2008). These features are often unavailable or control possibilities are ineffective.

Due to the nature of social networking, these services involve several participating roles. Wang & Kobsa (2009) defined three roles representing privacy threat to employees: other users, the employer (represented by users) and the service operator. From the technical aspect of privacy protection, there are no differences between other users and employers (registration of bosses, managers, etc.), since all users are equal in regular social networking services. Company services are open only for employees (e.g., IBM Beehive; DiMicco et al., 2009), and since these services may fall under special regulations, the service provider being the company itself (e.g., use of PETs can be forbidden), these services should only be used with raised privacy awareness, or be avoided totally.

In addition to the work of Wang & Kobsa (2009), we note that third parties, as an additional role beside other users and the service provider, also pose a threat to user privacy. Structural analysis shows that social networks are vulnerable to active (Backstrom et al., 2007) and passive attacks (Narayanan & Shmatikov, 2009) aiming to re-identify nodes in anonymized data exports. As the latter algorithm only considers structural properties of the export, it can reveal hidden relationships between identities present in different networks; for example, this algorithm can reveal that a business and a private identity belong to the same user.

Cryptography-Based Access Control

Relating to web privacy, we have discussed several PETs that can be used to post encrypted messages on the web by allowing client-side access control. These access control techniques are useful for controlling other users' and the service provider's access to the uploaded content alike. Some of this software can also be used for social networks, such as FireGPG (Cuony, 2010) or BlogCrypt (Paulik et al., 2010), but there are other PETs specifically designed for social networking, providing similar functionality.

The main goal of these PETs is to hide profile attributes or to separate identities by presenting false names (Luo et al., 2009); however, link hiding can also be possible (Anderson et al., 2009). We emphasize that for proper identity separation, the use of anonymous web browsers is necessary, since the service provider can easily link profiles by identifying the user between different logins (e.g., using browser descriptor information and IP address for identification; see Eckersley, 2010).

We propose the use of client-side software for social networks, concerning that the same requirements apply here as to PETs that are used for access management of web content. Nevertheless, there is a significant number of software tools that have some unfortunate compromises while trying to achieve enhanced privacy in social networks. For example, FlyByNight (Lucas & Borisov, 2008) is a Facebook application offering symmetric and public key encryption, but stores data encrypted on Facebook servers and has the service provider involved in the key management as well. Although it is a browser and operating system independent solution (it uses JavaScript technology on the client-side), it works only for Facebook, and requires the permission of the service provider to operate.

Some PETs are more than applications created for a single social network; however, they still only work with a single service. NOYB (Guha et al., 2008) and FaceCloak (Luo et al., 2009) are both Firefox extensions, although they are implemented to work only with Facebook. Both applications replace fake data with the original to avoid the appearance of ciphertexts in profiles; due to the substitution, these methods resemble steganography. The most serious disadvantage of these solutions is that fake data are provided by the software, and the user cannot suggest alternatives: NOYB substitutes attributes by creating dictionaries compiled from real data sets where the key determines the secret assignment, while FaceCloak uses relatively small pre-compiled dictionaries. Both tools use third party servers: NOYB for storing dictionaries, FaceCloak for storing the original data in an encrypted form.

Beato et al. (2009) define their work as an extension to NOYB by allowing sophisticated access control management for Facebook users. Their Firefox extension uses an external binary for encryption that originates from FireGPG. In this application, users can define groups of users (called connection classes) and folders of documents (called content classes), and can set access rights respectively. An employee may find this useful for separating access of colleagues and friends easily, while this kind of separation is not possible with the previously analyzed software tools. We note that this access management resembles privacy-enhancing identity management (Clauß et al., 2005) discussed in the next section.

Furthermore, comparison of most of these solutions can be found in the work of Paulik et al. (2010). To sum it up, one should consider the following before choosing the proper software. A practical solution should not necessitate trust in the service provider, should nor reliance on third parties (if possible), and it should be service independent and should not require the collaboration of the service operator. Further requirements, such as browser and operating system independency, the comfort of use, external software independency, are mostly up to the user's decision (for instance, BlogCrypt meets these requirements). We also

note that the concept of PETs using steganography suggested previously, could also be used here.

Using Privacy-Enhancing Identity Management

Gürses et al. (2008) put access control issues in a more generic context, and state the need for internal and external separation of digital identities. Internal separation means that users share different profile data with a selected group of their contacts, and external separation signifies that even the user herself runs under a different identifier (such as another registration). Both are quite useful functionalities for separating private and business life. For example, internal separation can allow an employee to share information on private and business events with her friends and boss respectively, and external separation can allow an employee to maintain different, unlinkable profiles for her private and business identities. Here, unlinkability should include the unlinkability of profile information.

For internal separation, the authors propose that the service providers should allow their users using group-based access control mechanisms, similarly to the techniques analyzed in the previous section. However, the client-sided cryptography-based solutions may not only provide more flexible access control management, but also protect the confidentiality of the data against the service provider. In addition, using these software tools does not require the consent of the service provider and can be changed any time, even by the user herself. Therefore, we propose using a client-side application providing the appropriate level of key management, supposing that it meets the presented requirements.

For external separation Gürses et al. propose the using of identity partitioning tools, for example partial identities, which is a privacy-enhancing identity management technique (Clauß et al., 2005). Other researchers have also concluded that current social networks are flat from an access control point of view, while real-life social networks have a partitioned structure (Adams, 2010). Since identity separation supports the partitioning of one's contacts, identity partitioning, in our opinion, is an excellent solution for internal separation.

The core concept of partial identities means that a user can partition her set of attributes (i.e., her profile) into smaller sets, which may be accessed under different pseudonyms. These pseudonyms with their attribute set are the partial identities. Sometimes it can also be important for a pseudonym to be unlinkable with the other pseudonyms of the users; therefore, random pseudonyms should be used with a client-side solution that fixes readability and management of identities (Borcea-Pfitzmann et al., 2005). Identities can be changed as the context or communication partners change (Brocea et al., 2005), thereby allowing the user to context-dependently present information on herself.

Both internal and external separation could be solved by introducing a novel model to social networks that applies the principles of privacy-enhancing identity management; for example, Nexus-Identity Networks (NIN) is such a model (Gulyás et al., 2009). Instead of offering a single profile, the NIN model allows users to have several profiles that are stored in a tree hierarchy, where leaves can refer to groups of users having access to that specific profile. An example for the comparison of regular and identity partitioning enabling social networks is provided on Figure 5.

Figure 5. Today's social networks with their flat structure (left), and social networks extended with identity partitioning (right) including a node that applies external separation

For providing identity separation, the NIN model allows three levels of anonymity. Pseudonymous identification refers to internal identity separation according to the terminology of Gürses et al. (2008). Identities running under pseudonymous identification are linkable for a global observer, but local observers (e.g., contacts) may

receive different information. In case of unlinkable pseudonymity, the identities are not trivially linkable by a global or by a local observer (i.e., they have different pseudonyms, and unlinkability is further enhanced by profile attributes). The highest level is total anonymity, which means the total absence of identifiers for the identity.

Social networks providing these levels of anonymity and access control with high granularity are able to support internal and external identity separation. These services provide the strongest level of privacy if the service provider cannot act as a global observer and cannot access all user content. However, if profile crawling is permitted, it may be a threat.

Threats Posed by Large Datasets Exported from Social Networks

Datasets can be exported from a social network for various reasons. For example, it can be provided by the social network operator for business partners or researchers, or it can be crawled by other third parties. However, these copies can endanger user privacy, as third parties that can access anonymized network data are able to learn additional private information. Backstrom et al. (2007) showed that an attacker who can modify the structure prior to anonymization can execute targeted attacks in order to learn hidden profile information or hidden connections between some users. Narayanan & Shmatikov (2009) argued the viability of such active attacks, and showed that passive attacks can de-anonymize users by simply using data crawled from a public network as auxiliary source.

Companies do not need anonymized exports to pose a privacy threat to employees. For instance, the passive attack presented by Narayanan & Shmatikov, can also be run on two datasets crawled from a personal and a business-oriented social network to match private and official identities. Today there are no proven techniques to avoid such attacks, but using these networks with raised privacy awareness can still be useful. The employee should consider separating her contacts in these networks, and should carefully avoid business contacts on the personal social networking site and friends on the business social networking site (to achieve different neighborhood structure). Besides the separation, one should also use different names on these networks, and should access the services via anonymous web browsers.

Other Issues in Social Networks

We highlight, for the sake of the completeness, that a distributed network architecture is also a good solution for providing privacy against the service provider; although, this is not the user's choice. However, these types of services are yet to spread in the future. For example, Cutillo et al. (2009) propose a three-layered social networking service including a social networking, and a peer-to-peer layer, both above the internet layer. Their model also provides protection against mapping one's neighborhood due to the structure and encryption in the social networking system.

OTHER MEANS OF WORKPLACE SURVEILLANCE

The employer may provide hardware (e.g., computer, smartphone), software (e.g., operating system, utilities), or services (e.g., company email service, intranet) to the employee, and therefore perform further surveillance to ensure that these resources are used for the right purpose, and the employee is spending his time properly – not considering that private actions may also take place. There might be many services involved; here we just mention some of the most frequently used ones: web browsing (discussed previously), e-mailing, internet usage, telephone calls, smartphones.

Problems related to most of these areas are technically much less complicated than the ones

discussed earlier, and therefore involving PETs is not always necessary. In most cases an agreement and a clear statement on the conditions of use are enough. For example, instead of asking for a detailed call list on a company phone, an employer may simply calculate with a slightly higher budget that includes a certain amount of private use (Szabó & Székely, 2005). Beyond the budget limit the employee should be responsible for the invoice. This kind of problem management can be used in many of these previously mentioned areas.

However, for some areas, there are PETs designed for solving these issues. There are application-related PETs like anonymous remailers providing e-mail sender anonymity (Danezis et al., 2003), but there are service specific PETs, too. For instance, to prevent network monitoring, anonymous VPNs (e.g., VPN Privacy, 2010) can be used, which hide all traffic and protect against traffic analysis attacks. The employer may also want to observe what the employee uses her computer for (including hardware and software-related issues). Malicious software, such as key loggers, can be removed by scanning the computer with regular security software, e.g., anti-malware applications that are the proper tools for removing key loggers and other malware.

If it is not possible to separate the hardware used both for work and free time activities, there exist other solutions. Many PETs are portable, meaning that it is possible to carry them on USB sticks, and to use them without leaving traces on the host computer. This is not possible for all programs, especially for regular software (e.g., some instant messaging software); therefore, it would be desirable instead to carry the digital workspace with all programs included (i.e., the operating system and applications). There are existing PETs that can run from a USB stick or drive, and, after being connected, they rebuild the user's private (or corporate) workspace, even allowing to install and remove programs, while the hosting system cannot access the hosted one. This kind of private computer-in-the-computer solution is supported by MojoPac (Rinocube, 2010).

This type of solution is more likely to be favorable for the employee who wants to build up a private workspace on a corporate computer. However, this may even work the other way around, when an employee wants to set up a corporate operating system on her own computer. For instance, the IronClad USB drive (Lockheed Martin, 2010) is such a solution including a standalone operating system. The IronClad drive offers enhanced control for the company: the employer can remotely observe what happens on the drive and can even control what the user may install or remove (e.g., the user cannot remove pre-installed spyware). Thus, this solution offers practically no privacy, but, by separating the disks via storing private content in an encrypted form with TrueCrypt (TrueCrypt, 2010), this solution can work well (even without the IronClad drive). The company can have the desired level of control, but the employee can switch to her private operating system any time, while her employer cannot access private information due to the encryption.

Today there are numerous brands of smartphones, which are taking over some of the functionalities of regular computers. These devices are equipped with applications that have been only used on personal computers before (e.g., web browsing, emailing, and even new apps can be installed on most of the phones), and as these accompany their user almost all the time, their integration into personal life is a serious threat to privacy. We expect the same or similar PETs to appear on these platforms in the near future, although a few are already available. For example, there are anonymous web browsers that use an implementation of the Tor anonymizing service adapted to smartphones (Gauld et al., 2009; The Guardian Project, 2010). There is also a software providing confidentiality for calls and text messages through encryption (Whisper Systems, 2010).

CONCLUSION

From the viewpoint of separating private and business life, our paper discussed numerous threats against user privacy due to the integration of online services into everyday life. By neglecting any legal support provided, we seek technical solutions for the separation. Based on the work of Szabó & Székely (2005) we focused on analyzing the privacy threats posed by the web and social networks, but also gave some insight into other means of workplace surveillance. Besides discussing the related literature, we have also proposed several PETs related to each of the areas; however, we drew the conclusion that it is not the technological solutions that are the most important, but awareness of data protection and privacy. We emphasize that with the necessary level of awareness, users are able to protect their privacy in the long run, by adjusting the set of chosen PETs to the local legal possibilities.

ACKNOWLEDGMENT

We are grateful for the comments, remarks and suggestions of Ádám Máté Földes, and we thank him for reviewing several versions of this article. We also thank Iván Székely for reviewing the final version, and for his useful comments.

REFERENCES

Adams, P. (2010). *Closing the gap between people's online and real life social network*. Paul Adams Presentations. Retrieved August 31, 2010, from http://www.slideshare.net/padday/the-real-life-social-network-v2

Adobe Systems Incorporated. (2010). *Adobe Flash player*. Retrieved August 31, 2010, from http://www.adobe.com/products/flashplayer/

Aggarwal, G., Burzstein, E., Jackson, C., & Boneh, D. (2010). *An analysis of private browsing modes in modern browsers*. Proc. of Usenix Security.

Anderson, J., Diaz, C., Bonneau, J., & Stajano, F. (2009). Privacy-enabling social networking over untrusted networks. In *Proc. of the 2nd ACM Workshop on Online Social Networks* (pp. 1-6). Barcelona, Spain: ACM Press. doi:10.1145/1592665.1592667

Backstrom, L., Dwork, C., & Kleinberg, J. (2007). Wherefore art thou R3579X? Anonymized social networks, hidden patterns, and structural steganography. In *Proc. of the 16th International Conference on World Wide Web* (pp. 181-190). Banff, Canada: ACM Press. doi:10.1145/1242572.1242598

Beato, F., Kohlweiss, M., & Wouters, K. (2009). *Enforcing access control in social network sites*. Paper presented at the HotPET section of the 9th PET Symposium.

Borcea, K., Donker, H., Franz, E., Liesebach, K., Pfitzmann, A., & Wahrig, H. (2005). Intra-application partitioning of personal data. In *Proc. of Workshop on Privacy-Enhanced Personalization*.

Borcea-Pfitzmann, K., Franz, E., & Pfitzmann, A. (2005). Usable presentation of secure pseudonyms. In *Proc. of the Workshop on Digital Identity Management, 2005* (pp. 70-76). Fairfax, VA: ACM Press. doi:10.1145/1102486.1102498

Boutin, P. (2009). How to block Facebook photos of yourself. *Gadgetwise Blog – NYTimes.com*. Retrieved August 31, 2010, from http://gadgetwise.blogs.nytimes.com/2009/05/05/how-to-block-facebook-photos-of-yourself/

Carver, B., Gomez, J., Pinnick, T., Soltani, A., Makker, S., & McCans, M. (2009). Know privacy, full report. *Know Privacy*. Retrieved August 31, 2010, from http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *24*(2), 84–88. doi:10.1145/358549.358563

Chew, M., Balfanz, D., & Laurie, B. (2008). (Under)mining privacy in social networks. In *Proc. of Web 2.0 Security and Privacy 2008*.

Clauß, S., Kesgodan, D., & Kölsch, T. (2005). Privacy enhancing identity management: Protection against re-identification and profiling. In *Proc. of the Workshop on Digital Identity Management, 2005* (pp. 84-93). Fairfax, VA: ACM Press. doi:10.1.1.101.2196

Cuony, M. (2010). Install FireGPG. *FireGPG*. Retrieved August 31, 2010, from http://en.getfiregpg.org/s/install

Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, *47*(12), 94–101. doi:10.1109/MCOM.2009.5350374

D'Angelo, G., Vitali, F., & Zacchiroli, S. (2010). Content cloaking: Preserving privacy with Google Docs and other web applications. In *Proc. of the 25th Annual ACM Symposium on Applied Computing* (pp. 826-830). Sierre, Switzerland: ACM Press. doi:10.1145/1774088.1774259

Danezis, G., Dingledine, R., & Mathewson, N. (2003). Mixminion: Design of a Type III anonymous remailer protocol. In *Proc. of Symposium on Security and Privacy, 2003* (pp. 2-15). Berkeley, CA: IEEE Computer Society.

DiMicco, J., Geyer, W., Millen, D., Dugan, C., & Brownholtz, B. (2009). People sensemaking and relationship building on an enterprise social network site. In *Proc. of the 42nd Hawaii International Conference on System Sciences* (pp. 1-10). Big Island, HI: IEEE Computer Society. doi:10.1109/HICSS.2009.343

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: the second-generation onion router. In *Proc. of the 13th USENIX Security Symposium*.

Eckersley, P. (2010). How unique is your web browser? *Panopticlick*. Retrieved August 31, 2010, from http://panopticlick.eff.org/browser-uniqueness.pdf

FaceTime. (2008). *The collaborative internet: Usage trends, end user attitudes and IT impact*. Security, Management & Compliance for Unified Communications, Web 2.0 and Social Networks. Retrieved August 31, 2010, from http://www3.facetime.com/forms/survey08_request.aspx

FengOffice. (2010). *Feng Office*. Retrieved August 31, 2010, from http://fengoffice.com/web/index.php

Gauld, C., Beresford, A., & Rice, A. (2009). *Shadow and TorProxy*. Computer Laboratory: Digital Technology Group. Retrieved August 31, 2010, from http://www.cl.cam.ac.uk/research/dtg/android/tor/

Guha, S., Tang, K., & Francis, P. (2008). NOYB: Privacy in online social networks. In *Proc. of the First Workshop on Online Social Networks* (pp. 49–54). Seattle, WA: ACM Press. doi:10.1145/1397735.1397747.

Gulyás, G. Gy., Schulcz, R., & Imre, S. (2008). Comprehensive analysis of web privacy and anonymous web browsers: Are next generation services based on collaborative filtering? In *Proceedings of the Joint SPACE and TIME Workshops 2008* (pp. 17-32). Trondheim, Norway: CEUR-WS.

Gulyás, G., Schulcz, R., & Imre, S. (2009). Modeling role-based privacy in social networking services. In *Proc. of Third International Conference on Emerging Security Information, Systems and Technologies, 2009, SECURWARE '09* (pp. 173-178). Athens, Greece: IEEE. *Computers & Society*. doi:.doi:10.1109/SECURWARE.2009.34

Gürses, S., Rizk, R., & Günther, O. (2008). Privacy design in online social networks: Learning from privacy breaches and community feedback. In *Proc of International Conference on Information Systems*.

Huang, E. (2011). On improving privacy: Managing local storage in Flash player. *Adobe Flash Platform Blog*. Retrieved February 15, 2011, from http://blogs.adobe.com/flashplatform/2011/01/on-improving-privacy-managing-local-storage-in-flash-player.html

JonDos GmbH. (2010). JondoFox. *JondoNym*. Retrieved August 31, 2010, from http://anonymous-proxy-servers.net/en/jondofox/

Krishnamurthy, B., & Wills, C. (2009). Privacy diffusion on the Web: A longitudinal perspective. In *Proc. of the 18th International Conference on World Wide Web* (pp. 541-550). Madrid, Spain: ACM Press. doi:10.1145/1526709.1526782

Lockheed Martin. (2010). *IronClads USB drive*. Lockheed Martin. Retrieved August 31, 2010, from http://lockheedmartinengineering.com/products/ironclad/index.html

Lucas, M. M., & Borisov, N. (2008). FlyByNight: Mitigating the privacy risks of social networking. In *Proc. of the 7th ACM Workshop on Privacy in the Electronic Society* (pp. 1-8). Mountain View, CA: ACM Press. doi:10.1145/1456403.1456405.

Luo, W., Xie, Q., & Hengartner, U. (2009). FaceCloak: An architecture for user privacy on social networking sites. In *Proc. International Conference on Computational Science and Engineering, 2009* (pp. 26-33). Washington, DC: IEEE Computer Society. doi:10.1109/CSE.2009.387.

Marlinspike, M. (2010). *GoogleSharing*. Retrieved August 31, 2010, from http://www.googlesharing.net

Matyszczyk, C. (2009). Facebook entry gets office worker fired. *CNet News.* Retrieved August 31, 2010, from http://news.cnet.com/8301-17852_3-10172931-71.html

McKeon, M. (2010). *The evolution of privacy on Facebook.* Matt McKeon. Retrieved August 31, 2010, from http://mattmckeon.com/facebook-privacy/

Microsoft Research. (2009). *Online reputation in a connected world*. Online Reputation Research. Retrieved August 31, 2010, from http://www.microsoft.com/privacy/dpd/research.aspx

Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. In *Proc. of the 30th IEEE Symposium on Security and Privacy, 2009* (pp. 173-187). Washington, DC: IEEE Computer Society. doi:10.1109/SP.2009.22

Paulik, T., Földes, Á. M., & Gulyás, G. (2010). BlogCrypt: Private content publishing on the Web. In *Proc. of the Fourth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2010*, Venice, Italy.

Privacy, V. P. N. (2010). *VPN privacy*. VPN Privacy Service. Retrieved August 31, 2010, from http://vpnprivacy.com

Privacy International. (2011). *European privacy and human rights*. Privacy International. Retrieved February 15, 2011, from https://www.privacyinternational.org/ephr

Rinocube. (2010). *MojoPac.* Retrieved August 31, 2010, from http://www.mojopac.com

Samy Kamkar. (2010). Evercookie -- Never forget. *Evercookie - virtually irrevocable persistent cookies*. Retrieved February 15, 2011, from http://samy.pl/evercookie/

Schroeder, S. (2009). Are you sure those photos have really been deleted? *Mashable – The Social Media Guide.* Retrieved August 31, 2010, from http://mashable.com/2009/05/21/photos-deleted-facebook/

Singhal, A. (2009). Relevance meets the real-time web. *Official Google Blog.* Retrieved August 31, 2010, from http://googleblog.blogspot.com/2009/12/relevance-meets-real-time-web.html

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). *Flash cookies and privacy.* Social Science Research Network. Retrieved August 31, 2010, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

Stamm, S. (2010). Plugging the CSS history leak. *The Mozilla Blog*. Retrieved August 31, 2010, from http://blog.mozilla.com/security/2010/03/31/plugging-the-css-history-leak/

Szabó, M. D., & Székely, I. (2005). Privacy and data protection at the workplace in Hungary. In Nouwt, S., & de Vries, B. R. (Eds.), *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy* (pp. 249–284). The Hague, The Netherlands: T. M. C. Asser Press, IT & Law Series. doi:10.1007/978-90-6704-589-6_10

The Guardian Project. (2010). Open-source mobile security. *The Guardian Project*. Retrieved February 15, 2011, from https://guardianproject.info

TrueCrypt Foundation. (2010). *TrueCrypt downloads*. TrueCrypt – Free Open-Source On-The-Fly Disk Encryption Software. Retrieved August 31, 2010, from http://www.truecrypt.org/downloads

Wang, Y., & Kobsa, A. (2009). Privacy in online social networking at workplace. In *Proc. of International Conference on Computational Science and Engineering, 2009, CSE '09* (pp. 975-978). Washington, DC: IEEE Computer Society. doi:10.1109/CSE.2009.438

What They Know. (2010). What They Know. *WSJ Blogs*. Retrieved February 15, 2011, from http://blogs.wsj.com/wtk/

Whisper Systems. (2010). *RedPhone, TextSecure*. Whisper Systems. Retrieved August 31, 2010, from http://whispersys.com

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010). A practical attack to de-anonymize social network users. In *Proc. of IEEE Symposium on Security and Privacy, 2010* (pp. 223-238). Washington, DC: IEEE Computer Society.

Wood, M. (2010). Google Buzz: Privacy nightmare. *CNet News*. Retrieved August 31, 2010, from http://news.cnet.com/8301-31322_3-10451428-256.html

ADDITIONAL READING

Besmer, A., & Lipford, H. (2009). Tagged photos: concerns, perceptions, and protections. In *Proc. of the 27th international conference extended abstracts on Human factors in computing systems* (pp. 4585-4590), Boston, MA, USA: ACM Press.

Blacksheep (2010). BlackSheep – Firefox Add-on. *Zscaler Cloud Security*. Retrieved February 15, 2011, from http://www.zscaler.com/blacksheep.html

Bonneau, J., Anderson, J., & Danezis, G. (2009). Prying Data out of a Social Network. In *Proc. of the International Conference on Advances in Social Network Analysis and Mining, 2009* (pp. 249-254), Washington, DC, USA: IEEE Computer Society.

DiMicco, J. M., & Millen, D. R. (2007). Identity management: multiple presentations of self in facebook. In *Proc. of the International ACM conference on Supporting group work, 2007* (pp. 383-386), Sanibel Island, Florida, USA: ACM Press.

Duffy, M. K., Ganster, D. C., & Pagon, M. (2002). Social Undermining in the Workplace. *Academy of Management Journal*, *45*(2), 331–351. doi:10.2307/3069350

Firesheep (2010). Firesheep. *Firesheep*. Retrieved February 15, 2011, from http://codebutler.github.com/firesheep/

Franz, E., Groba, C., Springer, T., & Bergmann, M. (2008). A Comprehensive Approach for Context-dependent Privacy Management. In *Proc. of Third International Conference on Availability, Reliability and Security* (pp. 903-910), Washington, DC, USA: IEEE Computer Society.

Franz, E., & Liesebach, K. (2009). Supporting Local Aliases as Usable Presentation of Secure Pseudonyms. In *Proc. of the 6th International Conference on Trust, Privacy and Security in Digital Business TrustBus* (pp. 22-31), Linz, Austria: Springer-Verlag, 2009.

Goldberg, I. (2002). Privacy-enhancing technologies for the Internet, II: Five years later. In *Proc. of Privacy Enhancing Technologies workshop*.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proc. of the ACM workshop on Privacy in the electronic society, 2005* (pp. 71-80), Alexandria, VA, USA: ACM Press.

Guha, S., Francis, P., & Tang, K. (2009). The NYOB official site. *NOYB: Posting Secret Messages on the Web*. Retrieved August 31, 2010, from http://adresearch.mpi-sws.org/noyb.html

Gulyás, G. Gy. (2009), Design of an Anonymous Instant Messaging Service. In *Proc. of the Fourth Privacy Enhancing Technologies Convention* (pp. 34-40), Dresden, Germany: Technical University of Dresden.

Hakkila, J., & Kansala, I. (2004). Role based privacy applied to context-aware mobile applications. In *Proc. of IEEE International Conference on Systems, Man and Cybernetics, 2004*, Washington, DC, USA: IEEE Computer Society.

Hansen, M., Schwartz, A., & Cooper, A. (2008). Privacy and Identity Management. *IEEE Security and Privacy*, *6*(2), 38–45. doi:10.1109/MSP.2008.41

Irani, D., Webb, S., Li, K., & Pu, C. (2009). Large Online Social Footprints – An Emerging Threat. In *Proc. of the International Conference on Computational Science and Engineering – Volume 03, 2009* (pp. 271-276), Washington, DC, USA: IEEE Computer Society.

Jendricke, U., & Gerd tom Markotten, D. (2000). Usability meets security – The Identity-Manager as your Personal Security Assistant for the Internet. In *Proc. of the 16th Annual Computer Security Applications Conference* (pp. 334-344), New Orleans, USA: IEEE Computer Society.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review (Seattle, Wash.)*, *79*(1), 2004.

Oreilly, T. (2007). What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications & Strategies*, (1), 17-38.

Patil, S., & Kobsa, A. (2004). *Instant Messaging and Privacy* (pp. 85–88). Leeds, U.K.: Proc. of The Human-Computer Interaction.

Reichenbach, M., Damker, H., Federrath, H., & Rannenberg, K. (1997). Individual Management of Personal Reachability in Mobile Communication. In *Proc. of IFIP/SEC'97 13th International Information Security Conference*, Copenhagen, Denmark.

Rezgui, A., Bouguettaya, A., & Eltoweissy, M. Y. (2003). Privacy on the Web: Facts, Challenges, and Solutions. *IEEE Security and Privacy*, *6*(1), 40–49.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty. Fuzziness and Knowledge-Based Systems*, *10*(5), 557–570. doi:10.1142/S0218488502001648

Tootoonchian, A., Saroiu, S., Ganjali, Y., & Wolman, A. (2009). Lockr: better privacy for social networks. In *Proc. 5th International Conference on emerging Network Experiments and Technologies (CoNEXT)* (pp. 169–180). Rome, Italy: ACM Press. doi:10.1145/1658939.1658959

Zheleva, E., & Getoor, L. (2008). *How friendship links and group memberships affect the privacy of individuals in social networks*. Technical report.

Zheleva, E., & Getoor, L. (2009). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proc. of the 18th international conference on World wide web* (pp. 531-540), Madrid, Spain: ACM Press.

KEY TERMS AND DEFINITIONS

Anonymizing Network: It works as a chain of proxies sitting between two communicating parties to provide anonymity for the sender, the receiver, or both. On the web, the purpose of these networks is to provide anonymity towards the service provider (or some other third parties) by hiding their users' IP addresses.

Anonymous Web Browser: A complex application or a web service that enables the user to access web pages anonymously. Anonymized users cannot be identified, tracked, profiled on web pages, and their presence cannot be linked to previous sessions.

Identity Separation: A single user creating two or more virtual identities with unlinkable attribute sets. In practice, the user relates her actions to these identities respectively by considering maintaining unlinkability.

Privacy-Enhancing Identity Management or PIDM: Its goal is to provide flexible control over the related data and meta data of the user's identities.

Privacy Enhancing Technologies or PETs: Computer applications, services or technologies that allow their users to protect their privacy, and provide access control and management on the data provided to the different actors they get involved with. PETs should especially provide protection over confidential and personally identifiable information.

Profiling: Collecting information on individuals. Its purpose is chiefly pursuing business benefits (e.g., through targeted advertising or dynamic pricing).

Pseudonymous Identification: An entity (i.e., a user) that has an identifier like a series of numbers, or a hexadecimal code is said to be identified with pseudonymous identifiers.

Social Network: An online service that allows individuals to build networks by creating relationship links toward each other, and also to interact with the community through these links.