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