Chapter 13
Harm Mitigation from the Release of Personal Identity Information

Andrew S. Patrick
Office of the Privacy Commissioner of Canada & Carleton University, Canada

L. Jean Camp
Indiana University, USA

ABSTRACT

In August 2007 approximately 445,000 letters were sent to retirees who belonged to the California Public Employees' Retirement System (CalPERS). This was a routine mailing, but all or a portion of each pensioner's Social Security Number (SSN) was printed on the address panel of the envelopes, making this event all but ordinary. This massive breach of sensitive SSNs, along with names and addresses, exposed these people to potential identity theft and fraud. What are the harms associated with a data breach of this nature? How can those harms be mitigated? What are, or should be, the costs and consequences to the organization releasing the data? While it is very difficult to predict the specific consequences of a data breach of this nature, a statistical model can be used to estimate the likely financial repercussions for individuals and organizations, and the recent settlement in the TJX case provides a good model of harm mitigation that could be applied in this case and similar cases.

INTRODUCTION

In August 2007 approximately 445,000 letters were sent to retirees who belonged to the California Public Employees' Retirement System (CalPERS). This was a routine mailing, but all or a portion of each pensioner's Social Security Number (SSN) was printed on the address panel of the envelopes, making this event all but ordinary (Bosworth, 2007; Privacy Rights Clearing House, n.d.). This massive breach of sensitive SSNs, along with names and addresses, exposed all of these people to potential identity theft and

DOI: 10.4018/978-1-61350-501-4.ch013

fraud. SSNs are supposed to be kept secret from all but a select few recipients (e.g., employers, tax agencies), and yet this information was plainly printed on the outside of envelopes sent through the regular postal mail.

What are the harms associated with a data breach of this nature? How can those harms be mitigated? What are, or should be, the costs and consequences to the organization releasing the data? This chapter describes the harms caused by the release of personal identity information, and discusses the possible mitigation of financial and non-financial identity theft risks. Different harm mitigation strategies are discussed and the costs of identity protection services are described. The impacts on the releasing organization are also described. Finally, the unique characteristics of vulnerable people, such as pensioners, that might lead to more concerns about the effects of the breach are discussed.

Risk mitigation begins with risk avoidance, so this chapter begins with a discussion of best practices for data governance. Immediately following is a discussion of the consequences of data breaches, and then a classification of the most common consequences, identity theft and account fraud. Near and long-term harm mitigation is then addressed, first for the consumer whose data were exposed and then for the organization that exposed the data. Moving from more generic consequences to specific costs, the next section contains an enumeration of credit monitoring services. We then discuss issues associated with particularly vulnerable populations. We conclude by providing a proposal for harm mitigation that involves moving away from provable damages towards recognizing harm from exposure. Throughout the chapter we return to our motivating case, the large-scale release by CalPERS of personal identity information for a uniquely vulnerable population.

DATA GOVERNANCE BEST PRACTICES

"Data governance" refers to the procedures put in place to mange the collection, storage, and use of information in an organization. With the amount of information being processed by organizations increasing all the time, data governance is crucial not only for maintaining the health and effectiveness of the organization, but also for protecting any sensitive information being held. Good data governance is not optional, and it must be part of a long-term process that ensures that organizations control the data they have been entrusted with (Smith, 2007).

The State of California has recognized the importance of good data governance, and they have also emphasized the special importance of protecting the SSN:

The Social Security Number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential. (California Office of Privacy Protection, 2008)

The public disclosure of the SSN was prohibited starting in 2003 and in 2004 laws were passed banning the use of SSNs on pay stubs. California has even recognized the specific risk involved in the CalPERS case, printing SSNs on the outside of envelopes:

When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application. (California Office of Privacy Protection, 2008)