Chapter V

Privacy-Sensitive Tracking of Behavior with Public Information Systems:
Moving Beyond Names in a Globalizing Mass Society

Chris C. Demchak, University of Arizona, USA

Kurt D. Fenstermacher, University of Arizona, USA

Abstract

This chapter explores the roles of names and name equivalents in social tracking and control, reviews the amount of privacy-sensitive databases accumulating today in U.S. legacy federal systems, and proposes an alternative that reduces the likelihood of new security policies violating privacy. We focus on the continuing public-authority reliance on unique identifiers, for example, names or national identity numbers, for services and security instead of dissecting a better indicator of security threats found in behavior data. We conclude with a proposed conceptual change to focusing the social-order mission on the behavior of individuals rather than their identities (behavior-identity knowledge model, BIK). It is particularly urgent to consider a different path now as increased interest in biometrics offers an insidious expansion of unique identifiers of highly personal data. E-government can be wonderful for central government's effectiveness and efficiency in delivering services while

also being a disaster for both privacy and security if not regulated legally, institutionally, and technically (with validation and appeal processes) from the outset.

Introduction

For a nation, ensuring security and acceptable social order are key missions of central governments; identifying and then restraining those who act contrary to societal rules are essential to these missions. Thus, reaching back to China's Han Dynasty or William's Domesday Book in 1086, governments have developed census and other list-making activities intended to monitor compliance. As populations grew and people moved, clan, geographic, marriage, or professional affiliations slowly became names to uniquely identify individuals. Being known to a legal system by a name, however, does not mean one's behavior is known. To know one citizen or many, nations like organizations have long used names as the key tracking device, but have needed to use local surveillance by the individual's community to monitor an individual's behavior. As long as communities were relatively immobile, the name-plus-neighbors system worked sufficiently well to allow small, local police units to supplant centuries of military-based internal social control in Europe.[1]

Today, however, the emerging global mobility of the information and terrorism age has changed the parameters of governments' roles in social control, the security needs of Westernized societies, and the privacy of citizens of democratic states. To address the first two factors, some governments have lessened the third: Privacy has routinely been sacrificed for security in a perceived privacy-security trade-off. Today, the firewall of "practical obscurity unless a criminal suspect" has been massively eroded by public authorities handing out private information in the name of public openness, inadvertent community data sharing, technological oversights in releasing data, and even commercial interests and seeking data for private market purposes. The legacy systems of most governments—including state and federal agencies in the United States—have not adapted to the new circumstances, especially the increasing shortcomings of overreliance on unique, persistent identifiers such as names and Social Security numbers (SSNs) when the goal is behavior monitoring. Public information systems need a new regime that will support the changing goals of governments while preserving the privacy that citizens expect in democratic societies.

This chapter explores the roles of names and name equivalents[2] in social control, reviews what kinds of data are being accumulated today in legacy systems, and proposes an alternative focused on the security goal that reduces the likelihood of violating the privacy of ordinary citizens. We focus on the Achilles heel in the government's efforts to both ensure social order and yet minimize the loss of privacy: the continuing reliance on unique identifiers, for example, names or national identity numbers. We conclude with a discussion about a conceptual change to focusing the social-order mission on the behavior of individuals rather than their identities. Such a system variation would be an intermediate step to a world of citizens' control of their private identities while allowing traceable public behavior. It is particularly urgent to consider a different path now as increased interest in biometrics (Alterman, 2003; Barton, Byciuk, Harris, Schumack, & Webster, 2005; Boukhonine, Krotov, & Rupert, 2005; Harris, 2003; Milone, 2001; Zorkadis & Donos, 2004) offers an insidious

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/privacy-sensitive-tracking-behavior-public/26884

Related Content

Best Practices in E-Government
Helmut Druke (2008). *Electronic Government: Concepts, Methodologies, Tools, and Applications (pp. 3487-3499).*
www.irma-international.org/chapter/best-practices-government/9941

E-Government Development in Africa: An Assessment of the Status of Sub-Regional Practice
Brendan E. Asogwa (2015). *Emerging Issues and Prospects in African E-Government (pp. 1-20).*
www.irma-international.org/chapter/e-government-development-in-africa/115661

The Evolution of Web Governance in the Federal Government
Julianne Mahlerand Priscilla M. Regan (2006). *International Journal of Electronic Government Research (pp. 21-35).*
www.irma-international.org/article/evolution-web-governance-federal-government/2010

Public Value of E-Government: The Case of Ministry of Public Administration and Home Affairs in Sri Lanka
Noor Sufnaand R. Lalitha S. Fernando (2016). *Trends, Prospects, and Challenges in Asian E-Governance (pp. 139-159).*
www.irma-international.org/chapter/public-value-of-e-government/140366

E-Government Development in the Caribbean
B. Ubaldi (2007). *Encyclopedia of Digital Government (pp. 517-522).*
www.irma-international.org/chapter/government-development-caribbean/11553