Achieving Effective Information Privacy: A Review of Outcome Measures Used By National Data Protection Authorities

Peter Mameli, Associate Professor
Department of Public Management
John Jay College of Criminal Justice, USA
pmameli@jjay.cuny.edu

KAPA/ASPA International Conference October 28-29, 2011
Pursuing Government Performance and Recovering Public Trust
The National Library of Korea
Seoul, South Korea

ABSTRACT

Scholarly literature on performance management systems, performance measures and results driven research for National Data Protection Authorities (NDPAs) is limited. However, an evidence-based analysis of NDPA results is necessary to determine their effectiveness. It is also needed to maintain public trust in the work carried out, as the milieu they operate within continues to shift. This paper examines original survey results, NDPA Annual Reports and secondary sources in order to assess how outcome measures can be best utilized and presented to the public when evaluating organizational performance. It then builds on these findings to recommend effective practices that all NDPAs can consider employing within their performance management systems.

---

1 Some elements of this paper were presented at the Northeast Political Science Association Annual Conference, Boston, Massachusetts, November 11-13, 2010.
“The essence of the present situation is that we are over our heads in complexity.”
Dwight Waldo (1980)

Introduction

Building and maintaining public trust in government requires the ability to see problems before they arise, and then competently construct policies to manage the ensuing environment. It also requires accountability and transparency after implementation of plans takes place. Current growth in social networking usage, and ongoing improvements in surveillance technology employed by public agencies and private organizations, has consumers, citizens and civil society calling for improved and credible data protection by governments.

The importance of focusing on the effectiveness of information privacy protections continues to accompany the refinement of legal instruments and governance structures for realizing this end (Hustinx, 2011). Understanding how to achieve effective information privacy at a national level in issue areas such as data collection, data matching, and data analysis is essential to securing the trust of citizens. Braman defines information policy as:

“Information policy is comprised of laws, regulations, and doctrinal positions – and other decision making and practices with society-wide constitutive effects – involving information creation, processing, flows, access, and use.” (2011, p. 3)

The niche that information privacy falls into involves all the above, but from the specific perspective of individual rights to protection for the personal material that is captured and transmitted within these processes. It is seen as one of the defining social challenges accompanying the growth of information technology in the 21st century (O’Leary and Van Slyke, 2010a: p. S7), and is complicated by the growing capabilities of performance measurement systems used by government agencies (Hatry, 2010: p. S209).

The need to clarify values surrounding these issues, and then design policies to guarantee those values are adhered to, represents an ongoing effort to achieve equilibrium in a consistently shifting landscape between security and privacy. The meaning of these values must be addressed by each country individually first to begin such a process fruitfully. After values have been settled upon, there must then be an attempt to answer policy questions. But these efforts should not be expected to yield “one size fits all” solutions. What will be uniform, however, is the need to address the importance of the governance problems appearing so as to build trust with the citizenries in question (see EdriGram, 2011, for an example of recent failures by the Irish police to ensure protection of confidential data that impact specifically on the notion of public trust).

While the multi-faceted impact of these technologies has become clear politically in the Middle East of late, it has also become of increasing significance in Western liberal democracies. Recent revelations of how the New York Police Department’s Intelligence Division has worked with the United States Central Intelligence Agency to engage in