PUBLIC ADMINISTRATION AND PUBLIC POLICY/155

HANDBOOK OF PUBLIC INFORMATION SYSTEMS

THIRD EDITION

Edited by
CHRISTOPHER M. SHEA
G. DAVID GARSON

ROUTLEDGE

HANDBOOK OF PUBLIC INFORMATION SYSTEMS

THIRD EDITION

Edited by
CHRISTOPHER M. SHEA
G. DAVID GARSON

Routledge
Taylor & Francis Group
New York London

PUBLIC ADMINISTRATION AND PUBLIC POLICY

A Comprehensive Publication Program

EDITOR-IN-CHIEF

EVAN M. BERMAN

Distinguished University Professor
J. William Fulbright Distinguished Scholar
National Chengchi University
Taipei, Taiwan

Founding Editor

JACK RABIN

1. *Public Administration as a Developing Discipline,* Robert T. Golembiewski
2. *Comparative National Policies on Health Care,* Milton I. Roemer, M.D.
3. *Exclusionary Injustice: The Problem of Illegally Obtained Evidence,* Steven R. Schlesinger
5. *Organization Development in Public Administration,* edited by Robert T. Golembiewski and William B. Eddy
7. *Approaches to Planned Change,* Robert T. Golembiewski
8. *Program Evaluation at HEW,* edited by James G. Abert
9. *The States and the Metropolis,* Patricia S. Florestano and Vincent L. Marando
11. *Changing Bureaucracies: Understanding the Organization before Selecting the Approach,* William A. Medina
12. *Handbook on Public Budgeting and Financial Management,* edited by Jack Rabin and Thomas D. Lynch
15. *Handbook on Public Personnel Administration and Labor Relations,* edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
19. *Handbook of Organization Management,* edited by William B. Eddy
22. *Politics and Administration: Woodrow Wilson and American Public Administration,* edited by Jack Rabin and James S. Bowman
23. *Making and Managing Policy: Formulation, Analysis, Evaluation,* edited by G. Ronald Gilbert
25. *Decision Making in the Public Sector,* edited by Lloyd G. Nigro
26. *Managing Administration,* edited by Jack Rabin, Samuel Humes, and Brian S. Morgan
27. *Public Personnel Update,* edited by Michael Cohen and Robert T. Golembiewski
28. *State and Local Government Administration,* edited by Jack Rabin and Don Dodd
29. *Public Administration: A Bibliographic Guide to the Literature,* Howard E. McCurdy
31. *Handbook of Information Resource Management,* edited by Jack Rabin and Edward M. Jackowski
32. *Public Administration in Developed Democracies: A Comparative Study,* edited by Donald C. Rowat
33. *The Politics of Terrorism: Third Edition,* edited by Michael Stohl
34. *Handbook on Human Services Administration,* edited by Jack Rabin and Marcia B. Steinhauer
36. *Ethics for Bureaucrats: An Essay on Law and Values, Second Edition,* John A. Rohr
37. *The Guide to the Foundations of Public Administration,* Daniel W. Martin
39. *Terrorism and Emergency Management: Policy and Administration,* William L. Waugh, Jr.

40. *Organizational Behavior and Public Management: Second Edition,* Michael L. Vasu, Debra W. Stewart, and G. David Garson
43. *Government Financial Management Theory,* Gerald J. Miller
46. *Handbook of Public Budgeting*, edited by Jack Rabin
49. *Handbook of Court Administration and Management*, edited by Steven W. Hays and Cole Blease Graham, Jr.
50. *Handbook of Comparative Public Budgeting and Financial Management*, edited by Thomas D. Lynch and Lawrence L. Martin
53. *Encyclopedia of Policy Studies: Second Edition,* edited by Stuart S. Nagel
54. *Handbook of Regulation and Administrative Law,* edited by David H. Rosenbloom and Richard D. Schwartz
55. *Handbook of Bureaucracy,* edited by Ali Farazmand
56. *Handbook of Public Sector Labor Relations*, edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
57. *Practical Public Management*, Robert T. Golembiewski
58. *Handbook of Public Personnel Administration*, edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
60. *Handbook of Debt Management*, edited by Gerald J. Miller
61. *Public Administration and Law: Second Edition*, David H. Rosenbloom and Rosemary O'Leary
62. *Handbook of Local Government Administration*, edited by John J. Gargan
63. *Handbook of Administrative Communication*, edited by James L. Garnett and Alexander Kouzmin
64. *Public Budgeting and Finance: Fourth Edition,* edited by Robert T. Golembiewski and Jack Rabin
67. *Handbook of Public Finance*, edited by Fred Thompson and Mark T. Green
68. *Organizational Behavior and Public Management: Third Edition,* Michael L. Vasu, Debra W. Stewart, and G. David Garson
69. *Handbook of Economic Development*, edited by Kuotsai Tom Liou
70. *Handbook of Health Administration and Policy*, edited by Anne Osborne Kilpatrick and James A. Johnson
72. *Handbook on Taxation*, edited by W. Bartley Hildreth and James A. Richardson
73. *Handbook of Comparative Public Administration in the Asia-Pacific Basin*, edited by Hoi-kwok Wong and Hon S. Chan
74. *Handbook of Global Environmental Policy and Administration,* edited by Dennis L. Soden and Brent S. Steel
75. *Handbook of State Government Administration,* edited by John J. Gargan
76. *Handbook of Global Legal Policy,* edited by Stuart S. Nagel
78. *Handbook of Global Economic Policy,* edited by Stuart S. Nagel
79. *Handbook of Strategic Management: Second Edition,* edited by Jack Rabin, Gerald J. Miller, and W. Bartley Hildreth
80. *Handbook of Global International Policy,* edited by Stuart S. Nagel
81. *Handbook of Organizational Consultation: Second Edition,* edited by Robert T. Golembiewski
82. *Handbook of Global Political Policy,* edited by Stuart S. Nagel
83. *Handbook of Global Technology Policy,* edited by Stuart S. Nagel
84. *Handbook of Criminal Justice Administration*, edited by M. A. DuPont-Morales, Michael K. Hooper, and Judy H. Schmidt
85. *Labor Relations in the Public Sector: Third Edition*, edited by Richard C. Kearney
86. *Handbook of Administrative Ethics: Second Edition,* edited by Terry L. Cooper
87. *Handbook of Organizational Behavior: Second Edition*, edited by Robert T. Golembiewski
88. *Handbook of Global Social Policy,* edited by Stuart S. Nagel and Amy Robb
89. *Public Administration: A Comparative Perspective, Sixth Edition,* Ferrel Heady

90. *Handbook of Public Quality Management*, edited by Ronald J. Stupak and Peter M. Leitner
91. *Handbook of Public Management Practice and Reform*, edited by Kuotsai Tom Liou
93. *Handbook of Crisis and Emergency Management*, edited by Ali Farazmand
94. *Handbook of Comparative and Development Public Administration: Second Edition,* edited by Ali Farazmand
95. *Financial Planning and Management in Public Organizations*, Alan Walter Steiss and Emeka O. Cyprian Nwagwu
96. *Handbook of International Health Care Systems,* edited by Khi V. Thai, Edward T. Wimberley, and Sharon M. McManus
97. *Handbook of Monetary Policy,* edited by Jack Rabin and Glenn L. Stevens
98. *Handbook of Fiscal Policy,* edited by Jack Rabin and Glenn L. Stevens
99. *Public Administration: An Interdisciplinary Critical Analysis,* edited by Eran Vigoda
100. *Ironies in Organizational Development: Second Edition, Revised and Expanded,* edited by Robert T. Golembiewski
101. *Science and Technology of Terrorism and Counterterrorism*, edited by Tushar K. Ghosh, Mark A. Prelas, Dabir S. Viswanath, and Sudarshan K. Loyalka
102. *Strategic Management for Public and Nonprofit Organizations*, Alan Walter Steiss
103. *Case Studies in Public Budgeting and Financial Management: Second Edition,* edited by Aman Khan and W. Bartley Hildreth
104. *Handbook of Conflict Management,* edited by William J. Pammer, Jr. and Jerri Killian
105. *Chaos Organization and Disaster Management,* Alan Kirschenbaum
106. *Handbook of Gay, Lesbian, Bisexual, and Transgender Administration and Policy,* edited by Wallace Swan
107. *Public Productivity Handbook: Second Edition,* edited by Marc Holzer
108. *Handbook of Developmental Policy Studies,* edited by Gedeon M. Mudacumura, Desta Mebratu and M. Shamsul Haque
109. *Bioterrorism in Medical and Healthcare Administration,* Laure Paquette
110. *International Public Policy and Management: Policy Learning Beyond Regional, Cultural, and Political Boundaries,* edited by David Levi-Faur and Eran Vigoda-Gadot
111. *Handbook of Public Information Systems, Second Edition,* edited by G. David Garson
112. *Handbook of Public Sector Economics,* edited by Donijo Robbins
113. *Handbook of Public Administration and Policy in the European Union,* edited by M. Peter van der Hoek
114. *Nonproliferation Issues for Weapons of Mass Destruction,* Mark A. Prelas and Michael S. Peck
115. *Common Ground, Common Future: Moral Agency in Public Administration, Professions, and Citizenship*, Charles Garofalo and Dean Geuras
116. *Handbook of Organization Theory and Management: The Philosophical Approach, Second Edition,* edited by Thomas D. Lynch and Peter L. Cruise
117. *International Development Governance,* edited by Ahmed Shafiqul Huque and Habib Zafarullah
118. *Sustainable Development Policy and Administration,* edited by Gedeon M. Mudacumura, Desta Mebratu, and M. Shamsul Haque
119. *Public Financial Management,* edited by Howard A. Frank
120. *Handbook of Juvenile Justice: Theory and Practice,* edited by Barbara Sims and Pamela Preston
121. *Emerging Infectious Diseases and the Threat to Occupational Health in the U.S. and Canada,* edited by William Charney
122. *Handbook of Technology Management in Public Administration,* edited by David Greisler and Ronald J. Stupak
123. *Handbook of Decision Making,* edited by Göktuğ Morçöl
124. *Handbook of Public Administration, Third Edition,* edited by Jack Rabin, W. Bartley Hildreth, and Gerald J. Miller
125. *Handbook of Public Policy Analysis,* edited by Frank Fischer, Gerald J. Miller, and Mara S. Sidney

126. *Elements of Effective Governance: Measurement, Accountability and Participation,* edited by Kathe Callahan
127. *American Public Service: Radical Reform and the Merit System,* edited by James S. Bowman and Jonathan P. West
128. *Handbook of Transportation Policy and Administration,* edited by Jeremy Plant
129. *The Art and Practice of Court Administration,* Alexander B. Aikman
130. *Handbook of Globalization, Governance, and Public Administration,* edited by Ali Farazmand and Jack Pinkowski
131. *Handbook of Globalization and the Environment,* edited by Khi V. Thai, Dianne Rahm, and Jerrell D. Coggburn
132. *Personnel Management in Government: Politics and Process, Sixth Edition,* Norma M. Riccucci and Katherine C. Naff
133. *Handbook of Police Administration,* edited by Jim Ruiz and Don Hummer
134. *Handbook of Research Methods in Public Administration, Second Edition,* edited by Kaifeng Yang and Gerald J. Miller
135. *Social and Economic Control of Alcohol: The 21st Amendment in the 21st Century,* edited by Carole L. Jurkiewicz and Murphy J. Painter
136. *Government Public Relations: A Reader,* edited by Mordecai Lee
137. *Handbook of Military Administration,* edited by Jeffrey A. Weber and Johan Eliasson
138. *Disaster Management Handbook,* edited by Jack Pinkowski
139. *Homeland Security Handbook,* edited by Jack Pinkowski
140. *Health Capital and Sustainable Socioeconomic Development,* edited by Patricia A. Cholewka and Mitra M. Motlagh
141. *Handbook of Administrative Reform: An International Perspective,* edited by Jerri Killian and Niklas Eklund
142. *Government Budget Forecasting: Theory and Practice,* edited by Jinping Sun and Thomas D. Lynch
143. *Handbook of Long-Term Care Administration and Policy,* edited by Cynthia Massie Mara and Laura Katz Olson
144. *Handbook of Employee Benefits and Administration,* edited by Christopher G. Reddick and Jerrell D. Coggburn
145. *Business Improvement Districts: Research, Theories, and Controversies,* edited by Göktuğ Morçöl, Lorlene Hoyt, Jack W. Meek, and Ulf Zimmermann
146. *International Handbook of Public Procurement,* edited by Khi V. Thai
147. *State and Local Pension Fund Management,* Jun Peng
148. *Contracting for Services in State and Local Government Agencies,* William Sims Curry
149. *Understanding Research Methods: A Guide for the Public and Nonprofit Manager,* Donijo Robbins
150. *Labor Relations in the Public Sector, Fourth Edition,* Richard Kearney
151. *Performance-Based Management Systems: Effective Implementation and Maintenance,* Patria de Lancer Julnes
152. *Handbook of Governmental Accounting,* edited by Frederic B. Bogui
153. *Bureaucracy and Administration,* edited by Ali Farazmand
154. *Science and Technology of Terrorism and Counterterrorism, Second Edition,* edited by Tushar K. Ghosh, Mark A. Prelas, Dabir S. Viswanath, and Sudarshan K. Loyalka
155. *Handbook of Public Information Systems, Third Edition,* edited by Christopher M. Shea and G. David Garson

Available Electronically

Principles and Practices of Public Administration, edited by Jack Rabin, Robert F. Munzenrider, and Sherrie M. Bartell

PublicADMINISTRATION*netBASE*

First published 2010 by CRC Press

Published 2019 by Routledge
711 Third Avenue, New York, NY, 10017
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

International Standard Book Number: 978-1-4398-0756-9 (Hardback)

Library of Congress Cataloging-in-Publication Data

Handbook of public information systems / editors, Christopher M. Shea, G. David Garson. -- 3rd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4398-0756-9 (alk. paper)
1. Public administration--Information technology. I. Shea, Christopher M. II. Garson, G. David. III. Title.

JF1525.A8H36 2010
352.7'4--dc22 2009034802

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

Contents

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Preface

In the relatively short amount of time that has passed since the previous edition of this book, the field of public information systems has continued to evolve. This evolution has elucidated many issues that public sector managers face as they wrestle with the information age. As we continue to learn more about e-government and e-governance issues and impacts, the more it becomes apparent that the interrelationships between political environments, organizational environments, and technological capabilities are often difficult to summarize and predict. Commonly held beliefs and understandings are called into question. In other words, as the field advances, our understanding of the complexity of the relevant issues increases, and more guidance becomes available to administrators.

We believe it is appropriate, therefore, that the study of information and communication technologies (ICT) continues to assume a central place in public administration curricula. There is good reason to study and better understand the implementation of ICT projects. While these projects often carry substantial expected benefits, many projects do not fulfill expectations, either in terms of benefits or costs. Also, it might be argued that some IT projects have potential for negative impacts. The prevalence of IT failure to deliver projects on time and within budget, and to do so while also providing for such values as privacy, security, and accountability, is as important a public management challenge as any in our time.

Given the evolution of the field and its central importance to public administrators, it may not be surprising that more than half this third edition of the *Handbook of Public Information Systems* is comprised of new material. We wish to thank all those in government service, academic institutions, and elsewhere who contributed to this edition. Without their generous contributions of time and energy, this volume would not be possible.

Christopher M. Shea
Chapel Hill, NC

G. David Garson
Raleigh, NC

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Editors

Christopher M. Shea is clinical assistant professor of health policy and management in the Gillings School of Global Public Health at the University of North Carolina at Chapel Hill, where he serves as director of the Bachelor of Science in Public Health program in health policy and management. He is currently teaching, or has taught, courses in the areas of organizational behavior and management, research methods, business communication, health information systems, and human resources management.

He is a member of the Public Health Informatics Steering Committee and the faculty advisor for the Health Information Management and Systems Society (HIMSS) student interest group, both at the University of North Carolina at Chapel Hill. He also has served as an associate editor of the journal *World Health and Population*, has co-authored a paper appearing in *Electronic Healthcare*, and completed his dissertation on electronic medical record systems (2008). He was inducted into Pi Alpha Alpha, the honor society for the National Association of Schools of Public Affairs and Administration, in 2004.

He earned a Bachelor of Business Administration in Finance and English from James Madison University (1995), a Master of Arts in English from West Virginia University (1998), a Master of Public Administration from North Carolina State University (2004), and a PhD in Public Administration from North Carolina State University (2008).

G. David Garson is full professor of public administration at North Carolina State University (NCSU), where he teaches courses on advanced research methodology, geographic information systems, information technology, e-government, and American government. In 1995, he was recipient of the Donald Campbell Award from the Policy Studies Organization, American Political Science Association, for outstanding contributions to policy research methodology, and in 1997, of the Aaron Wildavsky Book Award from the same organization. In 1999, he won the Okidata Instructional Web Award from the Computers and Multimedia Section of the American Political Science Association, in 2002, received an NCSU Award for Innovative Excellence in Teaching and Learning with Technology, and in 2003, received an award for Outstanding Teaching in Political Science from the American Political Science Association and the National Political Science Honor Society, Pi Sigma Alpha. In 2008, the NCSU Public Administration Program was named in the top 10 PA schools in the nation in information systems management.

Professor Garson is editor of and contributor to *Modern Public Information Technology Systems* (2007); *Patriotic Information Systems: Privacy, Access, and Security Issues of Bush Information Policy* (2007); and *Handbook of Research on Public Information Technology* (2008) and author of *Public Information Technology and E-Governance: Managing the Virtual State* (2006); editor of *Public*

Information Systems: Policy and Management Issues (2003); co-editor of *Digital Government: Principles and Practices* (2003); co-author of *Crime Mapping* (2003); author of *Guide to Writing Quantitative Papers, Theses, and Dissertations* (Dekker, 2001); editor of *Social Dimensions of Information Technology* (2000); *Information Technology and Computer Applications in Public Administration: Issues and Trends* (1999); and *Handbook of Public Information Systems* (1999, 2005); and is author of *Neural Network Analysis for Social Scientists* (1998); *Computer Technology and Social Issues* (1995); *Geographic Databases and Analytic Mapping* (1992); and is author, co-author, editor, or co-editor of 17 other books and author or co-author of over 50 articles. He has also created award-winning American Government computer simulations, CD-ROMs, and six Web sites for Prentice-Hall and Simon & Schuster (1995-1999).

For the last 25 years, he has also served as editor of the *Social Science Computer Review* and is on the editorial board of four additional journals.

Professor Garson received his undergraduate degree in political science from Princeton University (1965) and his doctoral degree in government from Harvard University (1969).

Contributors

Douglas Carr
Department of Public Administration
Oakland University
Rochester, Michigan

T. R. Carr
Department of Public Administration and Policy Analysis
Southern Illinois University Edwardsville
Edwardsville, Illinois

Shaoming Cheng
Department of Public Administration
Florida International University
Miami, Florida

Philip C. Christian
Florida Department of Revenue
Florida International University
Miami, Florida

Roland J. Cole
Sagamore Institute for Policy Research
Indianapolis, Indiana

David H. Coursey
The Decision Theater
Arizona State University
Phoenix, Arizona

Charles N. Davis
Missouri School of Journalism
National Freedom of Information Coalition
Columbia, Missouri

William L. Dougan
Department of Management
University of Wisconsin at Whitewater
Whitewater, Wisconsin

Ed Downey
Department of Public Administration
State University of New York College at Brockport
Brockport, New York

Mary Jane Frisby
Law Firm of Barnes & Thornburg
Indianapolis, Indiana

G. David Garson
Department of Political Science and Public Administration
North Carolina State University
Raleigh, North Carolina

Marilu Goodyear
Department of Public Administration
University of Kansas
Kansas City, Kansas

Carl Grafton
Department of Political Science and Public Administration
Auburn University Montgomery
Montgomery, Alabama

Thomas J. Greitens
Department of Public Administration
Central Michigan University
Mount Pleasant, Michigan

Stephen H. Holden
Touchstone Consulting Group of SRA International, Inc.
Washington, D.C.

Mark Curtis Hoffman
School of Public and Nonprofit Administration
Grand Valley State University
Allendale, Michigan

Sungsoo Hwang
Department of Public Administration
Yeungnam University
Kyungsan, Korea

Jennifer Killingsworth
Florida Fish and Wildlife Conservation Commission
Tallahassee, Florida

Younhee Kim
Department of Political Science
East Carolina University
Greenville, North Carolina

Jeremy R. T. Lewis
Department of Political Science
Huntingdon College
Montgomery, Alabama

Julianne Mahler
Department of Government and Politics
George Mason University
Fairfax, Virginia

Lynn M. Mulkey
Department of Social Sciences
University of South Carolina Beaufort
Bluffton, South Carolina

Patrick R. Mullen
Department of Public Administration
Center for State Policy and Leadership
University of Illinois at Springfield
Springfield, Illinois

Mark R. Nelson
EDUCAUSE Center for Applied Research
National Association of College Stores
Oberlin, Ohio

Rebecca L. Orelli
Department of Management
University of Bologna–Forlì Campus
Forlì, Italy

Emanuele Padovani
Department of Management
University of Bologna–Forlì Campus
Forlì, Italy

Anne Permaloff
Department of Political Science and Public Administration
Auburn University Montgomery
Montgomery, Alabama

Priscilla M. Regan
Department of Government and Politics
George Mason University
Fairfax, Virginia

Lee Roberson
Web Communications Office
Northwestern University
Evanston, Illinois

Carmine Scavo
Department of Political Science
East Carolina University
Greenville, North Carolina

Alicia Schatteman
Department of Public Management
John Jay College of Criminal Justice
New York, New York

Tino Schuppan
German Institute for Electronic Government
University of Potsdam
Potsdam, Germany

Eric Scorsone
Department of Agricultural Economics
Michigan State University
East Lansing, Michigan

Christopher M. Shea
Department of Health Policy and Administration
University of North Carolina at Chapel Hill
Chapel Hill, North Carolina

Michael Stonis
Prosch Consulting
Hanover Park, Illinois

Roger R. Stough
Department of Public Policy
George Mason University
Fairfax, Virginia

Gregory Streib
Department of Public Administration and Urban Studies
Georgia State University
Atlanta, Georgia

Marc A. Thibault
Department of Public Policy
George Mason University
Fairfax, Virginia

Irvin B. Vann
U.S. Census Bureau
Washington, D.C.

Peter M. Webster
Patrick Power Library
Saint Mary's University
Halifax, Nova Scotia, Canada

Linda Williams
Department of Public Administration
University of Kansas
Lawrence, Kansas

Katherine G. Willoughby
Department of Public Management and Policy
Georgia State University
Atlanta, Georgia

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

INTRODUCTION 1

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

An Introduction to Public Information Systems

Christopher M. Shea

CONTENTS

1.1 Introduction

In the previous edition of this book, it was noted that information systems in public agencies are pervasive for all levels of government [Garson 2005]. However, despite this pervasiveness (or perhaps because of it), there is much to learn about the implications these systems have for a variety of stakeholder groups, including public administrators, businesses, and citizens. Acknowledging the complexity of the roles and impacts of information systems in public agencies can be a useful first step toward reconciling the perspectives of various stakeholders.

Information systems offer both promise and challenges. Most practitioners and researchers generally would agree that information and communication technologies (ICT) can be valuable resources for public agencies. When the ICTs are well managed, they can contribute to increasing efficiency of work processes within public agencies, facilitating information exchange between citizens and government, and improving services for citizens [United Nations 2008]. Managing information systems effectively, however, is no easy task. Part of the management challenge occurs

because ICTs can alter, and be adapted to, organizational structures, power relations, and work processes [Rogers 2003]. The complex sets of relationships make predicting the impact of information systems difficult, and the complexity increases when the systems cross organizational boundaries [Fountain 2001].

The policy environment within which a public agency operates poses another challenge. Policy issues may prompt and also emerge from the use of ICTs. For example, efforts to increase efficiency or effectiveness of services through information systems may carry with them trade-offs and, therefore, raise concerns about such issues as access to the services, privacy, and security of personal data [Garson 2006]. Along these lines, there is still much to learn about the relationship between ICTs and e-governance outcomes such as citizen engagement and public discourse [Dawes 2008].

Facilitating a better understanding of public information systems issues, challenges, and strategies is the primary purpose of this book. Before embarking on this journey, however, it is necessary to acknowledge the broad scope of public information systems. Public agencies have a multitude of missions and, therefore, various information system needs. Providing due attention to each type of agency and each information system is quite difficult to accomplish in a single volume. However, we believe that many issues, challenges, and strategies apply to a range of organizational and information system contexts. In this regard, we hope that the present volume contributes to the learning process for students and current practitioners interested in ICTs in the public sector.

This volume is organized into broad sections, enabling a discussion of multiple perspectives. These sections include:

1. Policy Environments and Issues
2. Policy Research
3. Organizational Issues and Management Applications
4. Organizational Research
5. Performance Reporting

The rationale for these sections is to provide a sampling of key issues involving stakeholder interests, challenges related to leadership and management within organizations, illustrations of the intersection between policy and management, and models for further inquiry into information systems in the public sector.

1.2 Policy Environments and Issues

E-government initiatives generally aim to improve efficiency and effectiveness of the delivery of public services by improving information flows between government agencies and citizens, government agencies and businesses, and between government agencies themselves [United Nations 2008]. These aims must be strived for within certain constraints, of course, including individual privacy and information equity [Garson 2006], as well as the political climate for e-government and information sharing. The September 11th terrorist attacks, for example, amplified discussions about the tension between terrorism prevention efforts and individual rights [Nelson 2002].

The *Policy Environments and Issues* section of this book highlights several key areas in the policy domain relevant to public information systems, including the policy environment for e-government, e-government capability as a facilitator of policy implementation, access to public records, protecting intellectual property, the development of a resource infrastructure for research,

citizen participation, and individual privacy. In addition, both this section and the Organizational Issues and Management Applications section conclude with a case study chapter. These case studies illustrate the complexity of policy and organizational issues within specific contexts, allowing the reader to analyze the situation and develop lessons learned to be carried forward to future experiences.

1.3 Organizational Issues and Management Applications

From an organizational perspective, information systems have far-reaching implications. Beginning with the adoption decision-making process, the agency's leadership plays an important role in the success of a given ICT. In all types of organizations, adoption decisions should involve analysis beyond the direct financial cost of acquiring the technology. The "true cost" involves consideration of such other aspects as the need for technical support to maintain the new technologies, as well as a possible decrease in productivity for some period of time during implementation (e.g., Kuperman and Gibson 2003). It is widely documented that a substantial number of information system projects fail to be implemented within budget or successfully at all. It is also commonly believed that these failures result from failures in management, not simply failures in technology. A lack of commitment to the initiative among top management, lack of a participative approach to implementation, and inadequate planning are often cited among the causes for implementation failure [Garson 2006]. Furthermore, it is often difficult to clearly delineate between implementation process and implementation completion because the "fit" between the information system and the organizational structure, priorities, human resource capabilities, and work processes evolve over time. The *Organizational Issues and Management Applications* section of this book surveys topics related to this "fit."

1.4 Policy and Organizational Research

Empirical research demonstrates systematic analysis guided by specific research questions and aims. This volume includes two research sections: *Policy Research* and *Organizational Research*. The research chapters address a range of policy and organizational topics and employ various analytical methods, providing the reader with valuable insights into the topic of interest and the research process. The overall aim of this section of the book is to provide readers with additional exposure to policy and organizational topics, as well as models for systematically exploring some of the pressing issues that public administrators, policy makers, and researchers are facing related to public information systems.

1.5 Performance Reporting

When considering public information systems as a content area, it is sometimes difficult to identify a clear line separating the public policy domain from the organizational domain. After all, policy is implemented by organizations and often is developed or modified in an attempt to improve service delivery for citizens. The topic of performance reporting for public agencies exemplifies the blurring of this line very well due to the number of stakeholders involved and the complexity of the technical and human factors inherent in such efforts. Because the challenge of performance

reporting is so pervasive, we have included a section in this new edition dedicated to the topic. The chapters in this section provide discussions related to federal, state, and local levels of government; include a cross-country comparison; and address various stakeholder perspectives, budgetary implications, and data challenges associated with performance reporting.

1.6 Conclusion

We believe that the structure and content of the present volume offer discussions about public information systems from a variety of perspectives. In doing so we hope that it facilitates learning about the conceptual and theoretical challenges facing the field, as well as the practical implications of information systems for public agencies and the citizens they serve.

References

Dawes, S.S. (2008). The evolution and continuing challenges of e-governance. *Public Administration Review*, 68, S86–S102.

Fountain, J.E. (2001). *Building the Virtual State*. Washington, D.C.: Brookings Institution Press.

Garson, G.D. (2005). Public information systems in the 21st century. In G.D. Garson (Ed.), *Handbook of Public Information Systems,* 2nd ed. (pp. 3–10). Boca Raton: Taylor and Francis Group.

Garson, G.D. (2006). *Public Information Technology and E-Governance: Managing the Virtual State*. Sudbury, MA: Jones and Bartlett.

Kuperman, G.J. and Gibson, R.F. (2003). Computer physician order entry: Benefits, costs, and issues. *Annals of Internal Medicine*, 139(1), 31–39.

Nelson, L. (2002). Protecting the common good: technology, objectivity, and privacy. *Public Administration Review*, 62, S69–S73.

Rogers, E.M. (2003). *Diffusion of Innovations*, 5th ed. New York: Free Press.

United Nations (2008). United Nations e-government survey 2008: From e-government to connected governance. Available at http://unpangroups/p1.un.org/intradoc/ublic/documents/un/unpan028607.pdf

Chapter 2

Public Information Technology and E-Government: A Historical Timeline

G. David Garson

This chapter traces the history of public information technology from the 1895 Depository Library Program through to the Intellectual Property Act of 2008 and proposed legislation for 2009, in the form of a chronological listing of relevant events drawn from a wide variety of governmental and other sources.

1895 The Depository Library Program (44 USC 1902) is taken over by the Government Printing Office. Originating in the 1840s, the Depository Library program promotes the practice of agencies making their publications available via the U.S. Superintendent of Documents. A century later, in the 1990s, the Office of the Superintendent of Documents moved increasingly toward electronic publication formats.

1943 Colossus, used for code-breaking, is an early computer funded and run by the British government.

1944 Vannevar Bush, Director of the Office of Scientific Research and Development, authored a report at the request of President Roosevelt entitled *Science, The Endless Frontier: A Report to the President*. It called for promotion of interchange of scientific knowledge, long before NSFnet. In July, 1945, Bush published the article, "As We May Think," in the *Atlantic Monthly*, describing a desktop "memex," with functions similar to the modern Internet.

1942-1946
The ENIAC computer is developed by J. Presper Eckert and John W. Mauchly at the University of Pennsylvania for the U.S. Army, which needed it for ballistic calculations.

1946 The Administrative Procedures Act required hearings and public participation in regulatory rule-making. In the late 1990s, this became a legal basis for electronic public participation in e-rulemaking.

1950 The Federal Records Act of 1950 (amended 1964) mandated that each agency head would preserve "adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency." Combined with the 1966 Freedom of Information Act and the 1996 Electronic Freedom of Information Act, the Federal Records Act is the legal basis for the mandate that federal agencies make information available online.

1951 Remington Rand sells the first UNIVAC computer to the Census Bureau and subsequently five other clients. The first private sector purchase was General Electric, three years later, in 1954. UNIVACs weighed eight tons and had a speed of 1,000 instructions per second. The UNIVAC was phased out six years later.

1952 IBM sells the 701 computer to the U.S. government for defense purposes connected to the Korean War. The 701 marks the advent of widespread mainframe computing in the federal government.

1957 In response to the Russian launching of Sputnik-1, the earth's first artificial satellite, the U.S. government established the Advanced Research Projects Agency (ARPA) within the Department of Defense to promote defense technology. Twelve years later, ARPA-net goes online, the predecessor of the Internet.

1958 SAGE (Semi-Automatic Ground Environment) was installed at the McGuire Air Force Base in New Jersey. Used for air defense, SAGE and the related Whirlwind project involved major advances in data communications technology.

1960 President Eisenhower placed NASA in charge of communications satellite development. Echo, NASA's first satellite, was launched August 12 and functioned to reflect radio waves back to earth.

1962 The Communications Act of 1962 combined the efforts of AT&T, NASA, and the Department of Defense to create Comsat on February 1, 1963. In 1964, led by Comsat, a consortium of 19 nations formed IntelSat with the purpose of providing global satellite coverage and interconnectivity. IntelSat, in 1965, launched the Early Bird satellite, the world's first commercial communications satellite, serving the Atlantic Ocean Region. Global satellite coverage is achieved by IntelSat seven years later, in 1969.

1965 In a precursor to the Internet, ARPA sponsors a study about a "cooperative network of time-sharing computers" at MIT's Lincoln Lab and the System Development Corporation (Santa Monica, CA), directly linked via a dedicated 1,200 bps phone line. A DEC computer at ARPA was later added to form "The Experimental Network."

1966 The Freedom of Information Act of 1966 (FOIA; Public Law 89-554) established the right of public access to government information. Agencies were required to make information available through automatic channels or upon specific individual requests. The law specified certain exemptions, including classified defense and foreign policy matters; internal agency personnel rules and practices; information protected by other laws (e.g., many contractor bids); commercial trade secrets and financial information; documents; normally privileged in the civil discovery context; personal information affecting an individual's privacy; investigatory records compiled for law enforcement purposes; information that might reasonably be construed to interfere with law enforcement or deprive a person of a fair trial; information revealing the identity of a confidential source; information needed to protect

the safety of individuals; records of financial institutions; and geographical information on oil wells.

1969 ARPAnet, the predecessor of the Internet, went online with four nodes and reached 15 nodes by 1971.

1972 E-mail comes to ARPAnet.

1972 The Technology Assessment Act of 1972 created the Office of Technology Assessment (OTA), later disbanded as other information technology (IT) agencies emerged. The OTA, along with the Congressional Research Service (reconstituted and expanded by the Legislative Reorganization Act of 1970) and the Congressional Budget Office (created by the Budget Impoundment Act of 1974) became major users of FOIA to access executive agency data.

1972 The Federal Advisory Committee Act (FACA) was an elaboration of the 1966 FOIA legislation. It required timely notice in the *Federal Register* of advisory committee meetings. FACA also required agencies to allow interested parties to appear or file written statements, mandated that advisory committees keep detailed minutes (to include a record of the persons attending, documents received, documents issued, and documents approved by committees). These materials and all other advisory committee minutes, transcripts, reports, and studies were required to be available for public inspection.

1973 The first international connections were added to ARPANET, from University College of London (England) via NORSAR (Norway).

1973 Bob Kahn started the "internetting" research program at ARPAKahn, and Vint Cerf developed many of the fundamental concepts on which the Internet rests.

1974 IntelSat activated a "Hot Line" for direct telecommunication between the White House and the Kremlin.

1974 Telenet is started as the first public packet data service. As such, Telenet is the first commercial version of ARPAnet.

1974 The Privacy Act of 1974 (Public Law 93-579; 5 USC 552a) protected the privacy of individuals identified in information systems maintained by federal agencies. The collection, maintenance, use, and dissemination of information were regulated. The Privacy Act forbade disclosure of any record containing personal information, unless released with the prior written consent of the individual. Agencies were also mandated to provide individuals with access to their records.

1974 The Office of Federal Procurement Policy Act created the Office of Federal Procurement Policy (OFPP). In 1979, OFPP set up the Federal Procurement Data Center as a computerized repository of detailed information on all purchases of over $25,000 and summary details of smaller ones. OFPP came under the GSA in 1982.

1975 ARPAnet initiated online discussion lists.

1976 The Government in the Sunshine Act was an elaboration of the 1966 FOIA. It established the principle that the public is entitled to the fullest practicable information regarding the decision-making processes of federal agencies.

1977 The University of Wisconsin established TheoryNet, which provided electronic mail to over 100 researchers.

1978 The Presidential Records Act changed the legal ownership of the official records of the President from private to public, further expanding public access to federal information.

1979 USENET was established. It soon became the umbrella for hundreds of online discussion groups (lists).

1980 ARPANET suffered its first viruses, grinding the network to a complete halt on October 27 because of a status message virus that was introduced accidentally.

1980 The Paperwork Reduction Act of 1980 (PRA) mandated an Information Resources Management (IRM) approach to federal data. This represented the first unified policy framework for information resource management at the federal level. The director of the OMB was given responsibility for developing an IRM policy and for overseeing its implementation. A major revision of the PRA in 1995 mandated strategic planning for IRM.

1981 BITNET, the "Because It's Time NETwork," was initiated as a cooperative network at the City University of New York. BITNET provided electronic mail, file transfer, and listserv functionality. ARPANET, BITNET, and NSFNET were the three immediate precursors of the Internet.

1984 The domain name system (DNS) was established, allowing users to employ mnemonic Internet addresses instead of number addresses.

1986 The National Science Foundation funded NSFNet, a long-haul backbone network with a speed of 56K bps.

1986 The Computer Fraud and Abuse Act imposed fines and imprisonment of up to 20 years for various types of unauthorized computer access and fraud. A 1996 amendment extended coverage to all computers involved in interstate commerce and communications.

1986 The Rehabilitation Act Amendments of 1986 (sometimes called the Rehabilitation Act of 1986) added Section 508 to the Rehabilitation Act of 1973. Section 508 required federal agencies to establish guidelines for disability-accessible IT. Agency accessibility evaluations were mandated, and the Attorney General was charged with compliance evaluation. The deadline for agencies to have accessibility standards in place was extended to August 7, 2000.

1987 NSF signed a cooperative agreement to manage NSFNET in cooperation with IBM, MCI, and Merit Network, Inc. By the end of 1987, there were 10,000 Internet hosts.

1987 The Computer Security Act (CSA) mandated that the National Institute of Standards and Technology (NIST) develop security standards and guidelines for federal computer systems. The CSA also required that all federal agencies and their contractors establish computer security plans.

1988 The Computer Matching and Privacy Protection Act was an amendment to the Privacy Act of 1974, which extended Privacy Act protections to most forms of computer matching of individual records across agencies.

1989 The number of Internet hosts reached 100,000.

1990 ARPAnet was phased out, eclipsed by NSFNET.

1990 The Chief Financial Officers Act (CFOA) was focused on improving federal financial management and reporting practices but also called for (1) complete and timely information prepared on a uniform basis and which is responsive to the financial information needs of agency management; (2) the development and reporting of cost information; (3) the integration of accounting and budgeting information; and (4) the systematic measurement of performance. These four objectives required development of a financial information system and networked access to it, as well as a computerized performance tracking system.

1991 The High Performance Computing Act (HPCA) authorized the President to create a "National High-Performance Computing Program" for high-speed networking and established the National Research and Education Network (NREN). The OMB was given authority to review department budget requests for this program. The HPCA is sometimes called the "Gore Act" due to the activism and leadership of Vice President Al Gore.

1992 Tim Berners-Lee developed the World Wide Web, and Mosaic software was released to surf the Web. The number of Internet hosts reached one million.

1992 The first White House home page was launched on the Web.

1992 In *Quill Corporation v. North Dakota*, the Supreme Court explicitly upheld the precedent of its *Bellas Hess (1967)* case. These principles prohibited Internet sales taxation, overruling a North Dakota Supreme Court finding that technology had made the 1967 ruling obsolete. The tax prohibition applied to vendors with no physical presence in the state.

1992 Up to 1992, access to the Internet backbone was limited by the NSF's "Acceptable Use Policy." This restriction of the National Science Foundation Act prohibited commercial traffic on the Internet. Up to 1992, all Internet traffic had to be educational, scientific, or research-oriented. With the support of Congressman Rick Boucher (D-VA), Chairman of the Science Subcommittee of the House Committee on Science, Space, and Technology, legislation was passed, and in November, 1992, President Bush signed new legislation that repealed the Acceptable Use Policy, replacing it with language that permitted commercial traffic on the Internet backbone.

1992 The Information and Technology Act promoted technology development in public education, health care, and industry and called on NSF to fund efforts to connect K-12 classrooms to NSFNET.

1993 The National Information Infrastructure Act mandated funding priority in federal research and development efforts be given to accelerated development of high-performance computing and high-speed networking services.

1993 Federal funding of the Internet ended as the Internet became a private sector entity. Routing began through private providers in 1994. NSFNET reverted to being a limited research network.

1993 National Performance Review (NPR) was established on March 3. NPR represented the Clinton Administration's emphasis on IT as a tool to reform government, under the leadership of Vice President Al Gore. The NPR report, *Creating a Government that Works Better and Costs Less: Reengineering Through Information Technology,* illustrated that the reinventing government movement, originated with a focus on decentralization/devolution, had come to see e-government as a major reform thrust. NPR was later renamed the National Partnership for Reinventing Government (NPRG).

1993 The Government Information Technology Services Board was created to help implement NPR in IT areas.

1993 The Government Performance and Results Act (GPRA) required agencies to prepare multiyear strategic plans that described agency mission goals and approaches for reaching them. The act required agencies to develop annual performance plans that OMB was to use to prepare a federal performance plan that is submitted to the Congress along with the President's annual budget submission. The agency plans must establish measurable goals for program activities and describe the methods by which performance toward those goals is measured. The act also required agencies to prepare annual program performance reports to review progress toward annual performance goals, which, of course, included IT goals.

1993 Executive Order 12862: Setting Customer Service Standards. This executive order mandated that all agencies, including IT agencies, identify their customers, customer needs, and set standards and benchmarks for customer service. Customer-orientation became a keystone of e-government policy later in the decade.

1993 The Government Information Locator Service (GILS) was announced February 22. GILS was established as an Internet index to federal materials. It reflected a decision of the Clinton

administration to support direct agency release of electronic information, reversing a Reagan-era policy that mandated that release should be contracted through private third parties.

1993 The White House established public email to the president and vice-president.

1994 The Commerce Department's National Telecommunications and Information Administration's (NTIA) report, "Falling Through the Net," brought widespread public attention to the issue of the "digital divide."

1994 The Federal Acquisition Streamlining Act (FASA) required agencies to define tolerance standards for—and to monitor—cost, time schedule, and performance goals for federal acquisition programs, including IT projects. If a program fell out of tolerance, FASA required the agency head to review, take necessary actions, and, if necessary, terminate the program.

1995 The 1995 amendment to the Paperwork Reduction Act of 1980 (PRA; this amendment is sometimes called the Paperwork Reduction Act of 1995) established strategic planning principles for information resources management, including setting IT standards, applied life cycle management principles, mandating cross-agency IT initiatives, and setting technology investment guidelines. The PRA designated senior information resources manager positions in major federal agencies and created the Office of Information and Regulatory Affairs (OIRA) within OMB to provide central oversight of information management activities across the federal government. OIRA was mandated to "develop and maintain a government-wide strategic plan for information resources management." The OIRA director became, in principle, the main IT advisor to the director of the OMB. The PRA also called on agencies to "ensure that the public has timely and equitable access to the agency's public information," including electronically. Agency use of GILS (the Government Information Locator Service, an Internet index to federal information) was mandated.

1996 The Telecommunications Act of 1996 provided for a Universal Service Fund fee (a telephone tax, also known as the "E-rate" fund or fee), part of which became used on Clinton administration initiative to provide modem-based Internet access to schools, libraries, Indian reservations, and other "digital divide" target groups.

1996 The World Trade Organization, meeting in Singapore, reduced tariffs on IT trade items, thereby encouraging global ICT (information and communication technology) development.

1996 The Electronic Freedom of Information Act Amendment of 1996 (EFOIA) extended the right of citizens to access executive agency records to include access to electronic formats and online opportunities for access information. EFOIA officially defined a "record" in very broad terms. Release of information had to be in a format convenient to the user, not an agency option, as previous case law had held. Agencies were required to make "reasonable efforts" to search electronic databases for records. Electronic Reading Rooms were mandated to include "policy statements, administrative rulings and manuals, and other materials that affect members of the public."

1996 The Communications Decency Act (CDA) prohibited Internet distribution of "indecent" materials. A few months later, a three-judge panel issued an injunction against its enforcement. The Supreme Court unanimously ruled most of the CDA unconstitutional in 1997.

1996 The Federal Acquisition Reform Act (FARA) made purchasing of IT more flexible than under the prior Brooks Act. FARA gave the GSA a powerful oversight role, but it functioned more like an "IT commodities broker" than as an "IT policeman."

1996 OMB Circular A-130 implemented the Paperwork Reduction Act of 1980 and 1995 amendments by establishing government-wide uniform information resources management

practices. It mandates life cycle information management planning and work process redesign. The Department of Commerce is also mandated to improve federal telecommunications systems. Circular A-130 is revised and reissued periodically.

1996 The Federal Financial Management Improvement Act (FFMIA) required agency financial management systems to comply with federal financial management system requirements, applicable federal accounting standards, and the *U.S. Government Standard General Ledger* (SGL). To the extent that federal accounting standards specify IT aspects, the FFMIA requires uniformity of IT accounting across the federal government.

1996 The Clinger–Cohen Act of 1996 (originally named the Information Technology Management Reform Act of 1996, an amendment to the Paperwork Reduction Act of 1980) established a chief information officer (CIO) in every federal agency, making agencies responsible for developing an IT plan that relates IT planning to agency missions and goals. The Clinger–Cohen Act also mandated top management involvement in IT strategic planning, using IT portfolio management approaches. The oversight role of the director of the OMB was strengthened. The Clinger–Cohen Act also:

1. Encouraged federal agencies to evaluate and adopt best management and acquisition practices used by private and public sector organizations;
2. Required agencies to base decisions about IT investments on quantitative and qualitative factors related to costs, benefits, and risks, and to use performance data to demonstrate how well the IT expenditures support improvements to agency programs through measures like reduced costs, improved productivity, and higher client satisfaction; and
3. Streamlined the IT acquisition process by ending the General Services Administration's (GSA's) central acquisition authority. It placed procurement responsibility directly with federal agencies and encouraged adoption of smaller, more modular IT projects.

Later, when e-government became a priority, the existence of the CIO strategic planning structure was an important element facilitating e-government implementation at the federal level.

1996 President Clinton issued Executive Order 13011, a companion to the Clinger–Cohen Act. EO 13011 sought to improve management through an alignment of agency technology goals with strategic organizational goals and through interagency coordination of technology applications. EO 13011 created the CIO Council, an advisory body from 28 federal agencies plus senior OMB/OIRA personnel. The CIO Council was intended to be the central interagency forum for improving agency IT practices. EO 13011 represented the presidential "seal of approval" for e-government. In practice, the CIO Council was eclipsed by initiatives from the OMB itself and did not become a major generator of Bush administration IT initiatives.

1996 The Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA), also known as welfare reform, required interstate and intergovernmental coordination of IT systems to ensure that no individual exceeded the allotted five-year lifetime cap on assistance.

1997 The U.S. Department of Agriculture (USDA) became the first federal agency to engage in e-rulemaking, soliciting Web-based comments on rules for organic foods. This initiative won the 1998 Government Technology Leadership Award.

1998 Virginia, then Colorado became the first states to have a cabinet-level Secretary of Information Technology.

1998 The Digital Millennium Copyright Act extended copyrights to digital media, but the "Fair Use Doctrine" was retained to promote the rights of universities, libraries, and other occasional users of intellectual property. The act also prohibited removal of "copyright management information" from electronic media, outlawing the circumvention of anti-piracy access controls.

1998 The 1998 Amendments to the Rehabilitation Act of 1973, signed by President Clinton on August 7, required federal agencies to make their electronic information available to people with disabilities, including their Internet pages. This strengthened the Section 508 disability access standards mandated by the 1986 amendments to the Rehabilitation Act. Federal agencies were exempted from Section 508 implementation where the disability initiative in question would constitute an "undue burden."

1998 The Presidential Memorandum of May 14, 1998: Privacy and Personal Information in Federal Records. This memorandum directed federal agencies to review their compliance with the Privacy Act of 1974. Each agency was to designate a Senior Official for Privacy Policy. Each agency was required to conduct a Privacy Act compliance review.

1998 Presidential Decision Directive 63: Protecting America's Critical Infrastructures. Based on recommendations of the President's Commission on Critical Infrastructure Protection, this directive set the goal of establishing an integrated, secure IT infrastructure by 2003. A national center to warn of infrastructure attacks was established in the National Infrastructure Protection Center. Agencies were required to establish performance measures of Web site security.

1998 The Government Paperwork Elimination Act of 1998 (GPEA, signed into law on October 21) authorized the OMB to acquire alternative information technologies for use by executive agencies (Sec. 1702); provided support for electronic signatures (Secs. 1703–1707); and provided for the electronic filing of employment forms (Sec. 1705). Electronic filing of most forms had to be in place by October 21, 2003. The GPEA was the legal framework for accepting electronic records and electronic signatures as legally valid and enforceable, and it also represented Congressional endorsement of the e-government strategy.

1998 The Federal Activities Inventory Reform (FAIR) Act required agencies to inventory and report all of their commercial activities to the OMB. The FAIR Act then established a two-step administrative challenge and appeals process under which an interested party may challenge the omission or the inclusion of a particular activity on the inventory as a "commercial activity." While the FAIR Act did not require agencies to privatize, outsource, or complete their commercial activities, subsequent OMB guidelines required that nonexempt commercial activities undergo a cost evaluation for a "make or buy" decision. Each time a federal agency head considers outsourcing to the private sector, a competitive process is required. FAIR put pressure on agencies to outsource IT operations. Though "core operations" were not to be outsourced, CIOs sometimes felt that the core was encroached upon and that it was difficult to establish effective performance standards with vendors.

1998 IRS Restructuring and Reform Act of 1998 (RRA). Section 2001c promoted electronic filing of tax returns. Section 2003d required the IRS to establish that all forms, instructions, publications, and other guidance be available via the Internet. Section 2003e provided for tax return preparers to be authorized electronically to communicate with the IRS. Section 2005 provided taxpayer electronic access to their account by 2006.

1998 The National Archives and Records Administration (NARA) Bulletin 98-02: Disposition of Electronic Records, reminded agencies of their obligations under federal law to provide documentation of agency activities, including Web site pages and records.

1998 The Postal Service launched e-commerce, selling stamps via the Web.

1998 The Internet Tax Freedom Act of 1998 (ITFA) imposed a three-year moratorium on state and local taxation on Internet access.

1999 The Presidential Memo of December 17: Electronic Government reflected Clinton's endorsement of the concept of a federal government-wide portal (http://www.FirstGov.gov). Clinton announced 12 steps agencies can take including getting forms online by December 2000, posting online privacy policies, posting email contact information, identifying e-gov "best practices," and more.

1999 The Trademark Cyberpiracy Prevention Act outlawed "cybersquatting," giving businesses protection against those who register well-known domain names as a means of extorting fees from the true owners of existing trademarks.

1999 Fiscal year (FY) 1999 National Defense Authorization Act required the Department of Defense to establish a single electronic mall system for procurement.

2000 The President's Management Council adopted digital government as one of its top three priorities.

2000 On June 24, President Clinton made the first presidential Internet address to the nation, calling for the establishment of the FirstGov.gov portal.

2000 FirstGov.gov was launched September 22 as a Clinton management initiative. It was the official U.S. government portal, designed to be a trusted one-stop gateway to federal services for citizens, businesses, and agencies. At launch, it was a gateway to 47 million federal government Web pages. FirstGov.gov also linked state, local, District of Columbia, and tribal government pages in an attempt to provide integrated service information in particular areas, such as travel. It was managed by the Office of Citizen Services and Communications within the GSA.

2000 President Clinton asked Congress for $50 million to provide computers and Internet access to the poor, and requested $2 billion in tax incentives for the same purpose. The Universal Service Fund Fee, a telephone tax created in 1996, paid for these incentives.

2000 In Election 2000, both candidates (Gore and Bush) advocated digital government expansion.

2000 The Electronic Signatures in Global and National Commerce Act (ESIGN) made digital signatures legal in all 50 states, essential for the expansion of e-commerce.

2000 The OMB revised Circular A-130 to include a mandate for IT Portfolio Management, a management which requires a strategic approach to IT investment and risk.

2000 The Government Information Security Reform Act (GISRA; located within the FY 2001 Defense Authorization Act) amended the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." Sometimes called the "Security Act," this legislation required the establishment of agency-wide information security programs, annual agency program reviews, annual independent evaluations of agency programs and practices, agency reporting to OMB, and OMB reporting to Congress. GISRA covered programs for both unclassified and national security systems but exempted agencies operating national security systems from OMB oversight. The Security Act is to be implemented consistently with the Computer Security Act of 1987.

2001 *The President's Management Agenda*, issued in August, committed the Bush administration to five major management objectives, one of which was electronic government.

2001 The Congressional Federal Telework Mandate of 2001 (part of the Department of Transportation Appropriations Act of 2001) stated, "each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the maximum extent possible without diminished employee performance."

2001 In June, the OMB created the position of Associate Director for Information Technology and E-Government. This gave the OMB a "point man" to give higher priority to IT initiatives, particularly the goal of creating a "citizen-centric government." In essence, this position was given a mandate to provide leadership to all federal IT implementation, including a special emphasis on e-government. The Associate Director also directed the activities of the CIO Council. Mark Forman was the first incumbent.

2001 Information Quality Act (IQA) is Section 515 of the Treasury and General Government Appropriations Act for FY 2001, passed as a "rider." Section 515 charged OMB with the task of developing government-wide guidelines to ensure and maximize the quality of information disseminated by agencies. These guidelines were published in October, 2002. Under the guidelines, agencies must have a data quality control policy; quality control procedures must be applied before information can be disseminated; and each agency must develop an administrative mechanism whereby affected parties can request that agencies correct poor quality information (that is, an appeals process was mandated).

2001 Executive Order 13231: Critical Infrastructure Protection in the Information Age was issued in October, following 9/11, creating the President's Critical Infrastructure Protection Board. The Board is the central focus in the Executive Branch for cyberspace security. It is composed of senior officials from more than 20 departments and agencies.

2001 The USA Patriot Act became law on October 26. It gave government investigators greater authority to track e-mail and to eavesdrop on telecommunications. In September 2002, the Court of Review interpreted the USA Patriot Act to mean that surveillance orders under the Foreign Intelligence Surveillance Act could apply to criminal as well as terrorist cases.

2001 President Bush signed the Internet Access Taxation Moratorium on November 28, extending the 1998 ITFA to November 1, 2003. At this point, online spending was expected to account for 15% of holiday 2001 spending. The moratorium on Internet taxation was seen by the Bush administration as an economic stimulus as well as in promotion of Internet industries, but state governments feared significant revenue losses.

2002 The first Chief Technology Officer (CTO) for the federal government was appointed. This officer was to oversee the implementation of e-government initiatives. Casey Coleman, heading up the GSA's Office of Citizen Services, was appointed July 25.

2002 The OMB issued the document *E-Government Strategy* on February 27. This document set forth Bush administration e-government principles: citizen-centric, results-oriented, market-based. It also called for increased cross-agency data sharing. Some 34 specific projects are identified for funding, including the 22 initially announced in the "Quicksilver Initiative" in October, 2001:

GOVERNMENT TO CITIZEN

1. USA Service (GSA)
2. EZ Tax Filing (Treasury)
3. Online Access for Loans (DoEd)
4. Recreation One Stop (Interior)
5. Eligibility Assistance Online (Labor)

GOVERNMENT TO BUSINESS

1. Federal Asset Sales (GSA)
2. Online Rulemaking Management (DOT)
3. Simplified and Unified Tax and Wage Reporting (Treasury)

4. Consolidated Health Informatics (HHS)
5. Business Compliance One Stop (SBA)
6. International Trade Process Streamlining (Commerce)

GOVERNMENT TO GOVERNMENT
1. E-Vital (SSA)
2. E-Grants (HHS)
3. Disaster Assistance and Crisis Response (FEMA)
4. Geospatial Information One Stop (Interior)
5. Wireless Networks (Justice)

INTERNAL EFFECTIVENESS/EFFICIENCY
1. E-Training (OPM)
2. Recruitment One Stop (OPM)
3. Enterprise HR Integration (OPM)
4. Integrated Acquisition (GSA)
5. E-Records Management (NARA)
6. Enterprise Case Management (Justice)

2002 The Homeland Security Act established a CIO for the new Department of Homeland Security. The CIO was to oversee the largest consolidation of federal databases in U.S. history. Other provisions of Title 2 (the Information Analysis and Infrastructure Protection title) included:

- Section 201. The Office of Under Secretary for Information Analysis and Infrastructure Protection was created to receive and integrate security information; design and protect the security of data; issue security advisories to the public.
- Section 202. Transferred these units: the National Infrastructure Protection Center of the FBI (other than the Computer Investigations and Operations Section), the National Communications System of the Department of Defense, the Critical Infrastructure Assurance Office of the Department of Commerce, the Computer Security Division of the National Institute of Standards and Technology, the National Infrastructure Simulation and Analysis Center of the Department of Energy, and the Federal Computer Incident Response Center of the GSA.
- Section 203. Access to information. This section established the Secretary of Homeland Security's entitlement to receive intelligence and other information from agencies.
- Section 204 of the Homeland Security Act allowed the federal government to deny FOIA requests regarding information voluntarily provided by non-federal parties to the Department of Homeland Security.

2002 Acting on a February 2002 recommendation from the Federal CIO Council, the OMB established the Federal Enterprise Architecture Program Management Office (FEAPMO) on February 6, 2002. In 2002 FEAPMO issued "The Business Reference Model Version 1.0," which created a functional (not department-based) classification of all government services with a view to its use by OMB for cross-agency reviews to eliminate redundant IT investments and promote re-usable IT components. A Performance Reference Model (Fall 2002) set general performance measurement metrics. Data and Information Reference Model data needed to support Enterprise Architecture. Overall, this was reminiscent of the

1960s PPB: functional, not line item budgeting; emphasis on empirical measurement of performance; and strengthening top management oversight capabilities.

2002 The OMB called for a uniform protocol for e-rulemaking by the end of 2003.

2002 The GSA and the Office of Federal Procurement Policy (OFPP), with involvement from DOD, NASA, and NIH, advanced e-procurement by establishing the PPIRS (Past Performance Information Retrieval System) to give online access to past vendor performance records.

2002 President Bush issued a "Presidential Memo on the Importance of E-Government" in July, stating, "My administration's vision for government reform is guided by three principles. Government should be citizen-centered, results-oriented, and market-based."

2002 The OMB issued a revision of OMB Circular A-16 in August, setting guidelines for standardizing GIS data collection records. This laid the basis for its Geospatial One Stop portal, one of the eventually 24 OMB e-government "Quicksilver" initiatives. Circular A-16 was originally issued in 1953 to give OMB authority over surveying and mapping.

2002 The OMB issued a revision of OMB Circular A-76 in October, replacing lowest-cost acquisition with best-value acquisition, a goal long sought by CIOs. The circular also encouraged outsourcing in line with the Bush administration's goal to outsource 15% of "noninherently governmental jobs."

2002 The Cyber Security Research and Development Act (CSRDA) passed as part of the Homeland Security Act, enacted November 27, and authorized funding for new computer and network security research and grant programs. It also shielded Internet service providers (ISPs) from customer lawsuits when they revealed customer information to law enforcement authorities.

2002 The Enhanced Border Security and Visa Entry Reform Act of 2002 mandated that the 27 Visa Waiver Program countries would have to establish biometric passport plans by 2004. This deadline was later extended to 2006. In essence, it pressured other countries to follow the lead of the Department of Homeland Security and the State Department in adopting e-passports with embedded RFID technology.

2002 The Federal Information Security Management Act (FISMA), enacted December 17, permanently authorized and strengthened the information security program, evaluation, and reporting requirements of federal agencies.

2002 The Dot Kids Implementation and Efficiency Act, passed December 4, created a new domain similar to .com and .edu. The .kids domain was to be a child-friendly space within the Internet. Every site designated .kids would be a safe zone for children and would be monitored for content, for safety, and all objectionable material would be removed. Online chat rooms and instant messaging were prohibited unless they could be certified as safe. The Web sites under this new domain would not connect a child to other online sites outside the child-friendly zone.

2002 The Electronic Government Act of 2002 was passed by Congress on November 15 and signed by the President on December 16. The act was sponsored by Senator Joe Lieberman (D-CT) and was intended to promote e-government in all federal agencies. In essence, the EGA formalized much of what had been done by the OMB's Associate Director for IT and E-Government.

- The EGA established an Office of Electronic Government within the Office of Management and Budget. The head of this office was to be appointed by the president and report to the OMB director. In essence, this formalized the administrative setup established by the OMB, in 2001, under Mark Forman, making the OEG head the federal CIO and

the new Office of Electronic Government the overseer of setting cross-agency standards, including privacy standards, and assuring new e-government initiatives were cross-agency in nature. As such, the EGA represented a direct attack on the agency-centric "stovepipe" approach to IT of prior years.

- The EGA required regulatory agencies to publish all proposed rules on the Internet and to accept public comments via e-mail as part of "e-rulemaking."
- All information published in the *Federal Register* was now to be published on the Web also.
- The federal courts were required to publish rulings and other information on the Web.
- Privacy protections were added, prohibiting posting of personally identifiable information. Privacy notices are required, codifying a three year old OMB directive to agencies.
- The EGA also promoted better recruiting and training of federal IT officers. Each agency head was required to establish an IT training program. Public-private employee exchange programs were also authorized.
- Share-in-savings IT contracting was authorized and Federal Acquisition Regulations (FAR) was changed accordingly.
- Common standards for GIS information were mandated.
- The OMB's prime role in overseeing IT security was reaffirmed to be coordinated with the NIST's role in setting security technical standards.
- The EGA authorized $45 million available to the OMB for e-government projects in the current FY 2003, $50 million in FY 2004, and $250 million in each of FY 2005 and 2006. However, actual appropriations deleted $40 million of the authorized $45 million, forcing the OMB to implement e-gov strategy from mostly departmental budgets. Subsequent appropriations were also far lower than originally planned.
- The GSA was also authorized $8 million for digital signatures and $15 million for maintenance and improvement of FirstGov.gov and other portals. FirstGov.gov will be improved by adding a subject directory so pages can be accessed by topic rather than by agency.

2002 Regulation.gov was launched as a new one-stop Web portal in late 2002 as part of Bush administration e-government initiatives. It was designed to encourage citizens to participate in Federal rulemaking. On this site, one can find, review, and submit comments on Federal documents that are open for comment and published in the Federal Register. The uniform resource locator (URL) is http://www.regulations.gov.

2003 President Bush dissolved the Critical Infrastructure Protection Board on February 28, placing its function in the new Homeland Security Council, which is charged with coordinating cybersecurity policy. Early strategy emphasized public and private sector best practices and downplayed enforcement of security policies.

2003 The OMB announced "Round 2" of its e-government initiatives in March, looking beyond the earlier 24 "Quicksilver" initiatives. Round 2 focused on data and statistics, criminal investigations, financial management, public health monitoring, and monetary benefits to individuals. The OMB sought to force joint projects (e.g., Justice, Treasury, and EPA to have one criminal investigation system instead of three separate ones).

2003 The OMB required privacy assessments as part of the FY 2005 budget process for the first time. Agencies were required to submit privacy assessments of major IT systems as part of their annual business case submissions. This implemented privacy provisions detailed in the E-Government Act of 2002, which included privacy assessments and Web site privacy statements.

2003 Funding of e-government initiatives for FY 2004 was cut to $1 million, far short of the $50 million over five years as initially announced. OMB's head of the Office of Electronic Government, Mark Forman, quit, departing for the private sector. Future growth of e-government was called into question, at least temporarily.

2003 The Check Clearing for the 21st Century Act passed in October, allowing the substitutability of electronic images of checks for physical transfer of printed checks among banks. It did not mandate electronic check clearance but made it legally equivalent.

2003 The 2003 Amendment to the Fair Credit Reporting Act strengthened laws to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes.

2003 The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) was passed in December, giving the Federal Trade Commission, state attorneys general, and ISPs the power to enforce rules requiring senders of marketing e-mail to include pornography warnings, to offer opt-out methods, and to not use false or deceptive information in e-mail subject lines. The law became effective January 1, 2004, and authorized the FTC to impose fines up to $250 per e-mail, with a cap of $2 million for initial violations and $6 million for repeat violations (these caps do not apply to e-mail using false/deceptive subject lines). There were also criminal penalties including up to five years of prison. The FTC was mandated to develop a plan for a national do-not-spam registry and is authorized to launch the list after filing its report. Although CAN-SPAM led to some high-profile convictions of spammers, by 2008 the level of Internet spam had grown ten-fold and was estimated to cost ISPs and corporations over $40 billion annually, leading many observers to judge the act a relative failure.

2003 The Medicare Prescription Drug Improvement and Modernization Act of 2003 established a prescription benefit for Medicare to start January 1, 2006, which in turn required a massive IT effort to administer since millions of senior citizens were to be served. Led by CMS (Centers for Medicare and Medicaid Services), the government worked with 10,000 partners to establish a drug card based on over a hundred privately provided plans. The IT component had to collect data on drug claims, reconcile them for appropriateness, and manage fraud and abuse. A single vendor, AT&T Global Networking Services, was used for data connectivity.

When implemented in 2005–2006, there were major transitional problems including glitches in the software for plan selection and enrollment, rejecting coverage of medicines needed by elderly patients, and the lack of reimbursement for purchases. By January, 2006, Pennsylvania and eight other states had felt compelled to mount efforts to assure their citizens were not overcharged or deprived of Medicare benefits.

2005 The Real ID Act of 2005 was a Bush- and Republican-sponsored bill passed largely along party lines and largely without debate in Congress or much attention from the media. It was embedded in an emergency military appropriations bill for Iraq to make it hard for opponents to vote against it. Its purpose was to establish and rapidly implement regulations for state driver's license and identification document security standards. It compelled states to design their driver's licenses by 2008 to comply with federal antiterrorist standards. Federal employees would then reject licenses or identity cards that did not comply, which could curb Americans' access to airplanes, national parks, federal courthouses, Social Security,

and even opening bank accounts. The act came close to being a national ID card and to taking effect in 2008, but soon gave rise to strong state resistance over cost and implementation issues, eventually raising questions about whether it would be implemented in whole or part by the new Obama administration. The original legislation gave HSD authority to specify standards, which could include biometrics (fingerprint, iris scans), RFID tags, and DNA information in addition to basic identity information and a digital photo. State DMVs were to require much more identification than in the past (another unfunded mandate to the states). The Real ID Act could engender creation of a massive national database on individuals, though there is still a chance the Real ID cards will only be checked locally on an individual basis (e.g., does the cardholder have the fingerprints the card says they have). If there is to be such a database, and who will have access to it, including commercial access, was not spelled out.

2005 The Family Entertainment and Copyright Act of 2005 provided further protection for intellectual property, criminalized having pre-release media files on one's computer, strengthened law enforcement powers over Internet bootlegging of counterfeit media and sharing of pirated media, banned using camcorders in movie theaters, but specifically did not include any new criminal penalties for file sharers, meaning that publishers must still prove "willful intent to violate copyright" in order to obtain convictions. This left consumers still free to use devices like ClearPlay to make movies "family friendly" by automatically skipping over violence, sexual situations, and advertisements.

2005 The Junk Fax Prevention Act of 2005 legalized spam faxes and put the burden on consumers to get off of spam lists; the act exempted businesses from previous FCC regulations barring unsolicited fax messages if they had prior business relationship with the recipient (FCC rules had required expressed written consent). Recipients were guaranteed "a clear and conspicuous notice on the first page" explaining how to get off the fax mailing list.

2005 The Patient Safety and Quality Improvement Act of 2005 created a national database on patient safety, including doctor errors. The act gave legal protection to health professionals who reported their practices to patient safety organizations. The Act had been introduced in response to the Institute of Medicine's 1999 report, "To Err is Human." In that report, it was disclosed that approximately 98,000 patients die each year as a result of medical errors. Under privacy protections of the bill, patient safety databases were exempted from federal, state, or local civil, criminal or administrative subpoena; would not be subject to discovery in federal, state or local civil, criminal or administrative proceedings; and could not be disclosed under the Freedom of Information Act or any other similar law.

2005 The National All Schedule Prescription Electronic Reporting Act of 2005 (NASPER) followed a model from Idaho under which grants were given to states to establish a uniform electronic database for reporting controlled substances. Some 20 states already had prescription monitoring plans (PMP) at the time of passage of NASPER, which took a state-based approach, authorizing $60 million for FY 2006–2010. NASPER's purpose was to curtail prescription drug abuse by users who go "doctor shopping" to get drugs from multiple doctors. Medical lobbies were successful in rejecting language, which would have required law enforcement access without a court finding of probable cause.

2006 The USA Patriot Act Amendments of 2006 (Public Law 109-178) clarified that individuals who receive FISA orders (e.g., librarians) can challenge nondisclosure requirements, that individuals who receive national security letters are not required to disclose the name of their attorney, and that libraries are not wire or electronic communication service providers unless they provide specific services and for other purposes. Introduced by Senator John

Sununu (R-NH), the bill defended the position of the American Library Association and civil libertarians.

2006 The red-green-blue rating system employed by the OMB to rate federal agencies on e-government and the other four initiatives of the President's Management Agenda of 2001, mentioned on page 52 of the first edition, was deemphasized by the OMB in 2006. Among the reasons cited was that this rating system distracted both agencies and decision-makers, including the president, from a focus on achieving agencies' goals and missions. Lower ratings (red and yellow) also called attention to administration shortcomings and failures and created morale problems in the agencies affected, which often disagreed with the meaningfulness of the ratings.

2006 The GSA Modernization Act of 2006 merged the Federal Technology and Federal Supply services into the Federal Acquisition Service and merged the Information Technology Fund and General Supply Fund into the Acquisition Services Fund. A major objective of the mergers was to remove acquisition obstacles for departments wishing to buy IT "solutions," such as enterprise systems consisting of a mix of hardware, software, and support services, rather than simply purchase computer hardware or other discrete items, toward which the old form of GSA organization was oriented.

2006 The Federal Funding Accountability and Transparency Act of 2006 mandated that the Office of Management and Budget establish a Web site gateway to a searchable online database of all federal grants, subgrants, loans, contracts, awards, cooperative agreements, and other forms of financial assistance. Passed with bipartisan support, the legislation was designed to make federal spending transparent and accessible. Previously, there had been no single way to search for the disposition of federal spending.

2006 The USA Safe Web Act of 2006 (Public Law 109-455) was an amendment to the Federal Trade Commission Act of 1914. It increased the powers of the FTC to pursue distributors of spyware, spam, and other Internet threats to consumers.

2006 The Adam Walsh Child Protection and Safety Act of 2006, while not limited to online issues, established a searchable Internet-based national database of sex offenders and offenders against children; gave social service agencies online access to national databases on sex crimes against children; increased penalties for child pornography; increased record-keeping requirements for digital images of actual or simulated sexual acts, with penalties for noncompliance; funded online child safety programs; and in Title VII (the "Internet Safety Act"), increased criminal penalties for participation in an enterprise involving child exploitation and prohibited the embedding of deceptive words or images on a Web site to deceive an individual, including a minor, into viewing obscene material. Other provisions significantly increased the number of federal agents devoted to enforcement of child pornography and other crimes against children. In January, 2007, it was announced that states which did not bring themselves into compliance with the act would face cuts in federal funding.

2006 The Unlawful Internet Gambling Enforcement Act of 2006 made it illegal and imposed penalties for financial institutions and credit card companies to process payments related to settling Internet bets.

2006 The Tax Relief and Health Care Act of 2006 included research and development tax credit allowing companies to deduct a portion of money they invest in technology and innovation.

2006 The National Integrated Drought Information System Act of 2006 established the National Integrated Drought Information System to collect data as part of a drought early warning system.

2006 The Health Information Technology Promotion Act of 2006 created the position of the National Coordinator Office for Health IT, and mandated the development and implementation of a national interoperable health IT infrastructure.

2006 The Veterans Benefits, Health Care and Information Technology Act of 2006 required that the Veterans Affairs Department protect the privacy of veterans' personal information, including fraud alerts, data breach notification and analysis, reports to Congress, credit monitoring, and identity theft insurance. The act also funded the Information Security Education Assistance program to provide incentives allowing Veterans Affairs to recruit skilled IT personnel.

2006 The Telephone Records and Privacy Protection Act of 2006 created penalties to attempt to stop the public disclosure of personal phone records. Such disclosure had been widespread, based on professional "pretexters" who obtain commercially available personal information (address, mother's maiden name, Social Security numbers, etc.) and use these data to impersonate an individual and request a copy of phone records from telephone companies for resale to clients who request it. A secondary method of disclosure has been profiteering by telephone company employees who sell telephone records for personal gain. The bill imposed up to 10 years in jail and up to half a million dollars in fines for knowingly transferring private phone records to unauthorized persons.

2006 In 2006, states began passing identity theft/data breach protection laws. Among the first was Hawaii, which passed three acts for respectively providing notification of consumers regarding security breaches, requiring those businesses and government agencies responsible to have "reasonable" protections against data theft, and allowing victims of identity theft to place a security freeze on their credit reports so as to prevent thieves from taking out loans in their names.

2007 In January 2007, FirstGov.gov announced that it had changed its name to USA.gov. The change came after the GSA, which administers the nation's premiere portal, found that in the previous year, some 600,000 Americans had entered "usa.gov" when looking for federal information while not having been aware of the "FirstGov.gov" address.

2007 The Legislative Transparency and Accountability Act of 2007 (Public Law 110-81) was passed overwhelmingly (96:2) in the U.S. Senate in January, 2007. It mandated creation of a searchable Web site for data on congressional travel and also called for expanded Internet publication of Senate proceedings, conference reports, committee hearings, and proposed text of legislation.

2007 The Open Government Act of 2007 (Public Law 110-175) strengthened the Freedom of Information Act by requiring agencies to make information available online more fully. Agencies were required to establish individualized tracking systems for FOIA requests. The act also defined "members of the news media" more broadly to include blogs and similar news Web sites, at least for blogs of established news organizations. Also, the act clarified that when information services and databases are contracted out, FOIA still applies. Finally, Section 10 of the act established the Office of Government Information Services within the National Archives and Records Administration to function as ombudsman and to review agency FOIA policies and procedures, and recommend changes. Unfortunately, NARA was not given implementation funding for the new office.

2008 The KIDS Act of 2008 (Public Law No: 110-400, also known as "Keeping the Internet Devoid of Sexual Predators Act of 2008"), introduced in January, 2007, by Senators Charles E. Schumer and John McCain, required all registered sex offenders to submit their active e-mail addresses to law enforcement so that they may be entered into a registry which social e-networking and other organizations may check in order to protect their members.

2008 The Prioritizing Resources and Organization for Intellectual Property Act of 2008, introduced in the Senate (S. 3325) by Sen. Patrick Leahy (D-VT), became Public Law 110-403. In addition to numerous provisions broadly applicable to all types of intellectual property, whether or not computer-based, its Section 403 specifically authorized additional funding for the Department of Justice "to investigate and prosecute intellectual property crimes and other criminal activity involving computers." The bill also created an "Intellectual Property Czar" ("Intellectual Property Enforcement Coordinator"), whom critics feared would exercise a heavy hand in restricting Internet freedom through lawsuits the "czar" was authorized to initiate on behalf of the government.

2009 As this article is written in the first two weeks of the 111th Congress, these computer- and Internet-related bills have already been introduced:

- The Permanent Internet Tax Freedom Act of 2009, introduced in Senate (S43) by Sen. John Ensign (R-NV) , was intended to make the federal moratorium on Internet access taxes and multiple and discriminatory taxes on electronic commerce permanent.
- The Online Job Training Act of 2009, introduced in House (HR 145) by Rep. Rush Holt (D-NJ), was proposed to amend the Workforce Investment Act of 1998 to include workforce investment programs on the Internet.
- The Prescription Drug Affordability Act of 2009 (HR 163), introduced in the House by Rep. Ron Paul (R-TX), would amend the Internal Revenue Code and the Federal Food, Drug, and Cosmetic Act to remove barriers for and reduce taxes on retired individuals who import prescription drugs via Internet sites. Similarly, the Pharmaceutical Market Access Act of 2009, introduced in the Senate (S 80) by Sen. David Vitter (R-LA), also sought to reduce barriers to importation of prescription drugs via the Internet.
- The Transparency in Corporate Filings Act, introduced in the House (HR 281) by Rep. Peter Roskam (R-IL), would authorize the Securities and Exchange Commission (SEC) to permit or require persons securities filing information to be made available on internet Web sites and not just written filings to the SEC.
- The Voting Opportunity and Technology Enhancement Rights Act of 2009 was introduced in the House (HR 105) by Rep. John Conyers (D-MI), and it would mandate each State to establish a program under which individuals may access and submit voter registration forms electronically through the Internet. In addition, the bill would set standards for electronic voting software.
- The Notify Americans Before Outsourcing Personal Information Act of 2009, introduced in the House (HR 427) by Rep. Ted Poe (R-TX), would prohibit the transfer of personal information to any person or business outside the United States without notice.
- HR 230 was a bill "to require certain warning labels to be placed on video games that are given certain ratings due to violent content" and was introduced in the House by Rep. Joe Baca (D-CA).
- The Health Information Technology Act of 2009 was introduced in the Senate (S.179) by Senator Debbie Stabenow (D-MI) and was intended to improve quality in health care by providing incentives for adoption of modern IT.

2009 In addition, some bills, which died in the 110th Congress (2007–2008) without being enacted into law, may still be taken up by the 111th Congress (2009–2010) and the Obama administration. These include:

- The Voter Confidence and Increased Accessibility Act of 2007 would have required electronic voting systems to be designed to provide a paper trail of recorded votes and more.

- The Global Online Freedom Act of 2007, sponsored by Rep. Chris Smith, would have prohibited Internet companies from cooperating with repressive regimes that restrict Internet access to information about human rights and democracy and that use IP addresses or other personally identifiable information to punish pro-democracy activists. Specifically, Internet companies would have been prohibited from turning over personally identifiable information to such regimes.
- The Internet Freedom Preservation Act of 2007 was introduced to prohibit Internet and broadband service providers from offering preferential treatment to certain classes of customers. It reflected the goal of maintaining "net neutrality," which presently makes the Web site of a small organization about as accessible as the Web site of a large corporation.
- The Deleting Online Predators Act (DOPA), first approved in the House in 2006, would have banned children from using or viewing blogs and social networking sites in schools and libraries. DOPA was again proposed in 2007. The Center for Democracy and Technology is among those opposing DOPA, calling it unconstitutional and ineffective, and urging instead to educate children about safe Internet use. Another provision of DOPA would have required mandatory labeling of certain Web sites as containing "sexually explicit" content. The Center for Democracy and Technology has noted that such legislation has repeatedly been voided in the courts as unconstitutional.
- The NSA Oversight Act of 2007 reiterated that chapters 119 and 121 of title 18, United States Code, and the Foreign Intelligence Surveillance Act of 1978 are the exclusive means by which domestic electronic surveillances may be conducted, as well as for other purposes. That is, the act sought to reaffirm the exclusive role of the FISA courts in approving wiretaps. Other proposed reforms included requiring similar court approval for National Security Letters, which can also compel disclosure of sensitive information. Sponsored by Rep. Adam Schiff (D-CA), the bill was a repudiation of aspects of the Bush administration information policy.
- The Federal Agency Data Mining Reporting Act of 2007, also known as the Feingold-Sununu bill, would have increased the role of Congress in overseeing information sharing and data mining in the federal government
- The Congressional Research Accessibility Act of 2007 would have mandated the Congressional Research Service to make its reports available on the Web.
- The Identification Security Enhancement Act of 2007 would have repealed the Real ID Act in favor of a more limited approach to standardizing state drivers' licenses without creating centralized, national ID databases.
- The Free Internet Filing Act of 2007 would have provided for direct access to electronic tax return filing, a potential IRS service opposed by the private tax preparation industry.
- The Telework Enhancement Act of 2007, introduced by Senator Ted Stevens (R-AK) and Senator Mary Landrieu (D-LA), would have required all federal agencies to appoint a full-time senior-level employee as a telework managing officer.
- S.2661, sponsored by Senator Olympia Snowe (R-ME), sought to prohibit the collection of identifying information of individuals by false, fraudulent, or deceptive means through the Internet, a practice known as "phishing," and to provide the Federal Trade Commission the necessary enforcement authority.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

II

POLICY ENVIRONMENTS AND ISSUES

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 3

Tide of Security Secrecy, Tide of Transparency: The G.W. Bush and Obama Administrations, 2001–2009

Jeremy R. T. Lewis

CONTENTS

3.1 Introduction

George W. Bush's two administrations were characterized by national security issues, intertwined with issues of invasions of privacy and partial restrictions of open government legislation. His vice president, Richard Cheney, a leader in both of these policy areas, is considered the most influential vice president in U.S. history. G.W. Bush can claim to have directed the most information-conservative administration of the past 60 years, exceeding those of previous Republicans Eisenhower, Nixon, Reagan, and G.H.W. Bush. The Obama administration immediately laid its claim to being the most information-liberal administration, exceeding in its first months those of previous Democrats Kennedy, (a reluctant) Johnson, Carter, and Clinton. Therefore, at first sight, this was the sharpest, most polarized transition between official information regimes since the first agitation for freedom of information in the United States in the 1950s. We shall briefly examine the actions affecting the official information policy of both administrations along with reactions to them from the open government community. But first, we shall briefly summarize the history of the development of the freedom of information movement in the United States, occurring in decade-long policy cycles from 1955–2000 [see Lewis 1995, 2000a, and 2000b].

3.2 A Brief Survey of Federal Information Policy before 2000

Federal official information policy has developed primarily since the Administrative Procedures Act of 1946 (which mandates public notice and comment periods, appellate, and other quasi-judicial forms of administration). Amending its section 3 is the Freedom of Information Act (FOIA), primarily known for requiring the release of records once they are requested by the public, with extension by other, lesser legislations such as the Privacy Act, Sunshine Act, and Advisory Committee Act. The Copyright Act bars the U.S. government (unusually among developed states) from copyrighting documents prepared at public expense. Despite codification, these statutes do not harmonize in language, nor are they limited to narrow categories of records. This area of policy, therefore, has been highly litigious. The FOIA alone accounted for 3,000 lawsuits by 1990, two dozen Supreme Court opinions by 2000, and currently 400 lawsuits a year. (Other information

statutes have produced few requests or lawsuits.) Overall, the history of FOIA and of other lesser legislation on information policy provides the setting for public information systems at the start of the twenty-first century.

The FOIA was conceived in the mid-1950s by a loose coalition of the press and academics with the Moss committee, chaired by a young Representative from California and Sens. Hennings and Long of Missouri. The first policy cycle culminated in the 1966 FOIA, passed by the Democratic majority with Republican help over the resistance of President Johnson, which established the principle (in 5 USC 552 section (a)) of publishing all law and regulations and releasing records upon request from "any person." Section (b) listed nine exemptions, primarily involving national security classified documents and law enforcement documents, plus confidential commercial material and internal deliberative material. Privacy would be protected by segregating portions of records that would have identified individuals.

Initiating a second policy cycle, 1972 House hearings found that, lacking procedural language, the FOIA had had little effect beyond the symbolic. This was remedied in the post-Watergate 1974 amendments, passed by a super-majority over the veto of President Ford on November 21, 1974. These primarily tightened the language of exemptions, particularly for law enforcement, and added procedural requirements. In the late 1970s, President Carter's Attorney General issued a supportive memo, agencies ramped up their FOIA programs, and the first law suits were heard by the courts. It became evident that, while the press lobbied for the FOIA, most of the requests came from businesses contracted with or regulated by federal agencies.

The third policy cycle occurred in the environment of a balance of power between the Republican administration, Republican Senate, and Democratic House. The Reagan administration stepped in during 1982 to obtain a bill protecting the identities of covert intelligence officers, then the 1986 amendments, which compromised over setting fees for businesses at a higher rate than for those disseminating official information to the public (the press and academics, but more contentiously, public interest groups). A minor exemption clause permitted the CIA to also disguise whether it held any records that it was denying.

In the fourth cycle, 1986–1996, the issue of electronic records was explored by subunits of the U.S. House Government Operations Committee and the U.S. Office of Management and Budget, leading to the 1996 EFOIA [Lewis, 2000b]. In 1980–1986, the Senate's policy on public records depended on tension between a subcommittee (of judiciary) on the Constitution chaired by Sen. Orrin Hatch (R-Utah) and that on Technology and the Law chaired by Sen. Patrick Leahy (D-VT). The 1985 U.S. House hearings and report (1986a) combined with OMB Circular A-130 to raise the central questions of electronic information policy for the 1990s. OMB's Office of Information and Regulatory Affairs (OIRA) was granted extraordinary control over executive regulations through the 1980 Paperwork Reduction Act and a Reagan administration mandate to review (as a tight bottleneck) all proposed regulations. OMB's 1985 Circular A-130, The Management of Federal Information Resources, argued for avoiding monopolies of information, for giving value-added resellers a role in the private sector, for the contracting out of databases, and for continuance of inexpensive public access to official records [Sprehe, 1987 and 1988].

The judicial branch gradually was requiring electronic records to be released under the FOIA, giving some prospect of EFOIA without amending the law [Lewis, 1995, pp. 434–435]. The Supreme Court had let stand a decision in *Long v. IRS* [1979] that computer-stored records are still records under the FOIA. Then, in 1980, the Supreme Court had found in *Forsham v. Harris* that records include machine readable materials. Another court in *Yeager v. DEA* [1982] had maintained no distinction between manual and computer storage systems. In 1989, a district court in *Armstrong v. Bush* decided that National Security Council e-mail records were distinct from

telephone conversations, and on remand [sub nom. *Armstrong v. EOP*], it found that digital files contained information not held by hard copy.

In contrast to the Reagan and Bush (41) administrations, the Clinton administration reasserted the principle of open government being tied to new access technology. On February 22, 1993, the Vice President announced creation of the Government Information Locator System (GILS), an Internet index to materials publicly available at agencies. On June 25, 1993, Sally Katzen, of OMB's OIRA, in a revised Circular A-130, announced a policy reversing the Reagan administration's and favoring agency release of electronic information over having private sector contractors do the job. Agencies were requested to integrate CD-ROM and online indexing and publication with hard-copy processes, and to charge only for dissemination, not acquisition cost.

In an October 4, 1993 memo to agency heads, President Clinton encouraged agencies to release more records and in electronic form where available. The Justice Department also revised its guidance toward a more open policy. Janet Reno, Attorney General, in an October 4, 1993 circular rescinding the 1981 Justice guidelines, called for agencies to use broader discretion in releasing records, particularly those falling under the FOIA's exemption for internal memoranda. By 2000, despite efforts to resist the uncovering of a series of corruption and sexual scandal issues involving the Clintons, the open government community was relatively comfortable with the state of official information policy.

3.3 Information Policy in the G.W. Bush Administration, 2001–2005

G.W. Bush's first administration was a play in three acts: the first eight months, a prelude; then two years of reacting to a national security crisis; then a re-election campaign based heavily on a theme of a national security presidency. In the crisis act, there was a widespread support for, or acquiescence in, measures for national security secrecy.

3.3.1 Vice President Cheney's Energy Task Force

From February to May 2001, Vice President Cheney chaired a task force to develop a new energy policy, a situation reminiscent of the controversy over First Lady Hillary Clinton's task force on health care in 1993. For two members of Congress, the GAO routinely requested the roster and minutes of the group. Cheney's counsel, David Addington, denied the request, claiming the GAO lacked authority. Subsequently, public interest groups filed a lawsuit under the FOIA and another (rare) under the FACA; three years later, federal courts upheld the Vice President's office in withholding the records—and rejected the challenge under the FACA. The Supreme Court and District of Columbia Circuit Court both issued opinions, *In Re: Cheney*, 2004–2005. The Vice President argued that they were a special case outside the provisions of the FACA that required balanced membership and public records [Hammitt, 2005a]. The Supreme Court remanded the case to the D.C. Circuit, and, although the groups (Judicial Watch, the Natural Resources Defense Council, and the Sierra Club) obtained most of the records via FOIA requests to the Energy Department, the courts had almost destroyed the FACA [Hendler, 2009a; and Hammitt, 2009].

The political environment was drastically altered on September 11, 2001, by terrorist attacks using passenger aircraft on the World Trade Center towers in New York and on the Pentagon in Washington, D.C. The Bush administration, hitherto little interested in global treaties or foreign policy, was transformed into a national security presidency. With enormous support in Congress,

a war was initiated within weeks against the Al Qaeda and Taliban groups in Afghanistan, and a covert war that embraced many countries. The USA PATRIOT Act (2001) was passed overwhelmingly, giving carte blanche for the anti-terrorist war. Intelligence services and special operators were unleashed, electronic eavesdropping was allowed far more broadly (including domestically, [Risen and Lichtblau, 2005]), and suspected enemy combatants abroad (the exact terminology became contentious) were captured and taken by "extraordinary rendition" to third countries (or Guantanamo naval base) for interrogation as detainees. Videotapes of those interrogations were destroyed after FOIA requests from the ACLU. Roving eavesdropping on telecommunications was permitted to track individuals using multiple connections; "sneak and peek" searches were allowed without prior or post notice; and National Security Letters were used more frequently for FBI searches of records without a court order and with a gag rule on the subjects. Despite some district court opinions striking down particular searches and seizure provisions on Fourth amendment grounds, and attempts in the Senate to moderate some provisions in favor of civil liberties, the Act was reauthorized in 2006.

Although privacy was more directly at issue, this indirectly affected public records policy in many ways. Classified records (exempted from the FOIA, and never ordered released by a court) increased massively. In a minor but symbolic policy change, images of the ceremonial return of servicemen's coffins to Dover Air Force base were no longer released.

While there was almost universal support for this war, the administration soon planned a second war, an invasion and occupation of Iraq, whose dictatorial regime had proven irritating, wealthy from oil, and aggressive toward neighbors. From 2003, this occupation of a large and divided nation proved immensely challenging, and it gradually divided U.S. public opinion. Although it was a successful theme for re-election in 2004, public opinion turned against the war strongly by 2006, and Republicans lost seats in Congress.

The administration was soon entangled in more scandals over secrecy than usual. In the Valerie Plame (2007) affair, the Vice President's assistant, Lewis "Scooter" Libby, was penalized for leaking, in 2003, that the wife of an ambassador who the administration found critical and wished to discredit was a CIA officer. Because she had been an undercover spy, it ended her 20-year career, endangered her agents, and (if intentional) was a potential violation of the 1982 Intelligence Identities Protection Act. Libby's sentence (for a procedural offense) was commuted to a fine by President Bush on July 2, 2007, though he was not pardoned. A pardon [Plame Wilson, 2007, 306 and 388] would have removed the Fifth Amendment rationale for his not testifying to Congress about the affair.

Soon there were more official information issues: the secret legal memos from the Office of Legal Counsel, Department of Justice, that had supported "enhanced interrogation techniques" (allegedly defined as torture under international law and conventions) to be applied to irregular enemy combatants. Secret flights were tracked among eastern European and Middle Eastern countries as suspects were taken for interrogation [Priest, 2005] in places beyond the reach of U.S. constitutional restraints. The justifications for the invasion of Iraq, a program of the imminent development of weapons of mass destruction and links to Al Qaeda, were without foundation. The Supreme Court, with a Republican-appointed majority, ruled against detention without adequate legal rights. As in the contentious Vietnam War period that begat the 1966 FOIA and the Pentagon papers and Watergate era that stimulated the 1974 FOIA, national security secrecy and false official information created demands for more open government.

A center of gravity in the Bush administration was the Attorney General's Office of Legal Counsel, responsible for several memoranda justifying both a reduction of open government and a harsh detention regime for captured enemy combatants.

3.3.2 Attorney General Ashcroft's Memo, October 2001

Attorney General John Ashcroft (2001) continued the tradition of issuing a memo to federal agencies, setting a direction for FOIA processing. The memo removed the "foreseeable harm" test introduced by Attorney General Griffin Bell (in the Carter administration, 1976) and reintroduced by Attorney General Janet Reno (in the Clinton administration, 1993). It also committed the administration to the "fundamental values" of the *exemptions* to the FOIA, and to defending agencies withholding records whenever they found a "sound legal basis." This encouraged agencies [Hammitt, 2003] to withhold records where discretion permitted. The General Accounting office issued a report on September 19, 2003, on FOIA processing under the Ashcroft memo, reckoning that about one-quarter of agencies had made some changes in response to the order [Hammitt, 2003].

3.3.3 Andrew Card's 2002 Memorandum on Protecting Homeland Security Records

Reorganization and creation of the unified Department of Homeland Security, plus a widespread drive to remove any information from official Web sites that could facilitate poisoning water supplies or air with weapons of mass destruction, brought attention to the inability to declare most of this material classified. Posting of records on environmental dangers of many kinds, like other safety data, had been thought beneficial to public health. In spring 2002, the White House Chief of Staff, Andrew Card, issued a memo to agency heads, with advice from the Justice Department and ISOO, to protect Sensitive But Unclassified Homeland Security records via the FOIA's little-used exemption (b)(2) for internal personnel rules and practices, and exemption (b)(4) for confidential commercial information and trade secrets. (Neither one is really suitable for the purpose.)

3.3.4 Bush's Executive Order Restricting the Presidential Records Act

The 1978 Presidential Records Act treated presidents' records as public property, though court challenges and executive orders have reduced the scope of the statute. In 1995, however, a court opinion declared—against counsel for both presidents George H. W. Bush and William J. Clinton—that former presidents yielded control over their papers 12 years after leaving office. In early 2001, White House counsel Alberto Gonzales instructed the Archivist to delay release of President Reagan's files, let alone those of Bush and Clinton. A subsequent November 1, 2001 Executive Order (EO) 13233 revoked President Reagan's 1989 EO 12667 and required approval from the current president for the release of former presidents' records. (President G.W. Bush would therefore be able to protect his father's records.) Furthermore, past presidents and vice presidents could hand down their privileges indefinitely. "It was essentially overturning the Presidential Records Act," said Thomas Blanton, of the National Security Archive [Hendler, 2009a].

3.3.5 The National Security Classification System

Since 2001, more agencies and more officials have been authorized to classify records. By 2007, the Information Security Oversight Office (ISOO) found more than twenty-three million classification actions government-wide—the number having more than doubled since 2000. President G.W. Bush then laid down, by the 2003 executive order, a three-year moratorium on many automatic declassifications, authorized the Director of Central Intelligence to overrule declassifications