

Contents

EXECUTIVE SUMMARY	1
1 SCOPING THE ISSUE: TERRORISM, PRIVACY, AND TECHNOLOGY	7
1.1 The Nature of the Terrorist Threat to the United States, 7	
1.2 Counterterrorism and Privacy as an American Value, 8	
1.3 The Role of Information, 11	
1.4 Organizational Models for Terrorism and the Intelligence Process, 15	
1.5 Activities of the Intelligence Community and of Law Enforcement Agencies, 17	
1.6 Technologies of Interest in This Report, 19	
1.6.1 Data Mining, 20	
1.6.2 Behavioral Surveillance, 24	
1.7 The Social and Organizational Context, 26	
1.8 Key Concepts, 27	
1.8.1 The Meaning of Privacy, 27	
1.8.2 Effectiveness, 29	
1.8.3 Law and Consistency with Values, 30	
1.8.4 False Positives, False Negatives, and Data Quality, 35	
1.8.5 Oversight and Prevention of Abuse, 41	
1.9 The Need for a Rational Assessment Process, 42	

2	A FRAMEWORK FOR EVALUATING INFORMATION-BASED PROGRAMS TO FIGHT TERRORISM OR SERVE OTHER IMPORTANT NATIONAL GOALS	44
2.1	The Need for a Framework for Evaluating Information-Based Programs, 44	
2.2	Evaluating Effectiveness, 47	
2.3	Evaluating Consistency with U.S. Law and Values, 52	
2.3.1	Data, 53	
2.3.2	Programs, 54	
2.3.3	Administration and Oversight, 56	
2.4	A Note for Policy Makers: Applying the Framework in the Future, 57	
2.5	Summary of Framework Criteria, 59	
2.5.1	For Evaluating Effectiveness, 59	
2.5.2	For Evaluating Consistency with Laws and Values, 61	
2.5.3	For Developing New Laws and Policies, 63	
3	CONCLUSIONS AND RECOMMENDATIONS	67
3.1	Basic Premises, 67	
3.2	Conclusions Regarding Privacy, 71	
3.2.1	Protecting Privacy, 71	
3.2.2	Distinctions Between Capability and Intent, 75	
3.3	Conclusions Regarding the Assessment of Counterterrorism Programs, 75	
3.4	Conclusions Regarding Data Mining, 76	
3.4.1	Policy and Law Regarding Data Mining, 76	
3.4.2	The Promise and Limitations of Data Mining, 77	
3.5	Conclusions Regarding Deception Detection and Behavioral Surveillance, 82	
3.6	Conclusions Regarding Statistical Agencies, 84	
3.7	Recommendations, 86	
3.7.1	Systematic Evaluation of Every Information-Based Counterterrorism Program, 86	
3.7.2	Periodic Review of U.S. Law, Policy, and Procedures for Protection of Privacy, 95	

APPENDIXES

A	Acronyms	105
B	Terrorism and Terrorists	111
B.1	The Nature of Terrorism, 111	

B.2	Some Tactics of Terrorism, 113	
B.3	A Historical Perspective on Terrorism, 114	
B.4	Explaining Terrorism, 114	
B.5	Al Qaeda and the Terrorist Threat to the United States, 115	
B.6	Terrorists and Their Supporting Technologies, 118	
B.7	Looking to the Future, 119	
C	Information and Information Technology	120
C.1	The Information Life Cycle, 120	
C.1.1	Information Collection, 120	
C.1.2	Information Correction and Cleaning, 121	
C.1.3	Information Storage, 122	
C.1.4	Information Analysis and Use, 122	
C.1.5	Information Sharing, 122	
C.1.6	Information Monitoring, 123	
C.1.7	Information Retention, 124	
C.1.8	Issues Related to Data Linkage, 126	
C.1.9	Connecting the Information Life Cycle to the Framework, 126	
C.2	The Underlying Communications and Information Technology, 128	
C.2.1	Communications Technology, 128	
C.2.2	Information Technology, 129	
C.2.3	Managing Information Technology Systems and Programs, 131	
D	The Life Cycle of Technology, Systems, and Programs	133
E	Hypothetical and Illustrative Applications of the Framework to Various Scenarios	137
E.1	Airport Security, 137	
E.1.1	The Threat, 137	
E.1.2	A Possible Technological Approach to Addressing the Threat, 138	
E.1.3	Possible Privacy Impacts, 139	
E.1.4	Applying the Framework, 140	
E.2	Syndromic Surveillance, 141	
E.2.1	The Threat, 141	
E.2.2	A Possible Technological Approach to Addressing the Threat, 141	
E.2.3	Possible Privacy Impacts, 142	
E.2.4	Applying the Framework, 144	

F	Privacy-Related Law and Regulation: The State of the Law and Outstanding Issues	150
F.1	The Fourth Amendment, 150	
F.1.1	Basic Concepts, 150	
F.1.2	Machine-Aided Searches, 151	
F.1.3	Searches and Surveillance for National Security and Intelligence Purposes That Involve U.S. Persons Connected to a Foreign Power or That Are Conducted Wholly Outside the United States, 152	
F.1.4	The Miller-Smith Exclusion of Third-Party Records, 153	
F.2	The Electronic Communications Privacy Act, 154	
F.3	The Foreign Intelligence Surveillance Act, 155	
F.4	The Privacy Act, 156	
F.5	Executive Order 12333 (U.S. Intelligence Activities), 159	
F.6	The Adequacy of Today's Electronic Surveillance Law, 160	
F.7	Further Reflections from the Technology and Privacy Advisory Committee Report, 164	
G	The Jurisprudence of Privacy Law and the Need for Independent Oversight	166
G.1	Substantive Privacy Rules, 167	
G.1.1	Privacy Challenges Posed by Advanced Surveillance and Data Mining, 167	
G.1.2	Evolution of Regulation of New Technologies, 172	
G.1.3	New Surveillance Techniques That Raise Privacy Questions Unaddressed by Constitutional or Statutory Privacy Rules, 175	
G.1.4	New Approaches to Privacy Protection: Collection Limitation Versus Use Limitation, 175	
G.2	Procedural Privacy Rules and the Need for Oversight, 176	
G.2.1	Oversight Mechanisms of the U.S. Government, 177	
G.2.2	A Framework for Independent Oversight, 179	
G.2.3	Applying Independent Oversight for Government Agencies to Protect Privacy, 182	
G.2.4	Collateral Benefits of Oversight, 184	
H	Data Mining and Information Fusion	185
H.1	The Need for Automated Techniques for Data Analysis, 185	
H.2	Preparing the Data to Be Mined, 189	

H.3	Subject-Based Data Mining as an Extension of Standard Investigative Techniques, 192	
H.4	Pattern-Based Data Mining Techniques as Illustrations of More Sophisticated Approaches, 193	
H.5	The Evaluation of Data Mining Techniques, 198	
H.5.1	The Essential Difficulties of Evaluation, 199	
H.5.2	Evaluation Considerations, 200	
H.6	Expert Judgment and Its Role in Data Mining, 205	
H.7	Issues Concerning the Data Available for Use with Data Mining and the Implications for Counterterrorism and Privacy, 207	
H.8	Data Mining Components in an Information-Based Counterterrorist System, 208	
H.9	Information Fusion, 209	
H.10	An Operational Note, 211	
H.11	Assessment of Data Mining for Counterterrorism, 213	
I	Illustrative Government Data Mining Programs and Activity	218
I.1	Total/Terrorism Information Awareness (TIA), 219	
I.2	Computer-Assisted Passenger Prescreening System II (CAPPS II) and Secure Flight, 219	
I.3	Multistate Anti-Terrorism Information Exchange (MATRIX), 222	
I.4	Able Danger, 224	
I.5	Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE), 226	
I.6	Automated Targeting System (ATS), 228	
I.7	The Electronic Surveillance Program, 229	
I.8	Novel Intelligence from Massive Data (NIMD) Program, 230	
I.9	Enterprise Data Warehouse (EDW), 231	
I.10	Law Enforcement Analytic Data System (NETLEADS), 232	
I.11	ICE Pattern Analysis and Information Collection System (ICEPIC), 232	
I.12	Intelligence and Information Fusion (I2F), 233	
I.13	Fraud Detection and National Security Data System (FDNS-DS), 233	
I.14	National Immigration Information Sharing Office (NIISO), 234	
I.15	Financial Crimes Enforcement Network (FinCEN) and BSA Direct, 234	
I.16	Department of Justice Programs Involving Pattern-Based Data Mining, 235	

J	The Total/Terrorist Information Awareness Program	239
J.1	A Brief History, 239	
J.2	A Technical Perspective on TIA's Approach to Protecting Privacy, 243	
J.3	Assessment, 247	
K	Behavioral-Surveillance Techniques and Technologies	250
K.1	The Rationale for Behavioral Surveillance, 250	
K.2	Major Behavioral-Detection Methods, 251	
K.2.1	Facial Expression, 252	
K.2.2	Vocalization, 254	
K.2.3	Other Muscle Activity, 255	
K.2.4	Autonomic Nervous System, 255	
K.2.5	Central Nervous System, 257	
K.3	Assessing Behavioral-Surveillance Techniques, 258	
K.4	Behavioral and Data Mining Methods: Similarities and Differences, 259	
L	The Science and Technology of Privacy Protection	263
L.1	The Cybersecurity Dimension of Privacy, 263	
L.2	Privacy-Preserving Data Analysis, 266	
L.2.1	Basic Concepts, 266	
L.2.2	Some Simple Ideas That Do Not Work in Practice, 268	
L.2.3	Private Computation, 269	
L.2.4	The Need for Rigor, 270	
L.2.5	The Effect of Data Errors on Privacy, 273	
L.3	Enhancing Privacy Through Information-System Design, 275	
L.3.1	Data and Privacy, 275	
L.3.2	Information Systems and Privacy, 276	
L.4	Statistical Agency Data and Approaches, 277	
L.4.1	Confidentiality Protection and Public Data Release, 278	
L.4.2	Record Linkage and Public Use Files, 279	
M	Public Opinion Data on U.S. Attitudes Toward Government Counterterrorism Efforts	281
M.1	Introduction, 281	
M.2	Data and Methodology, 284	
M.3	Organization of This Appendix, 287	
M.4	General Privacy Attitudes, 288	
M.5	Government Surveillance, 291	

M.5.1	Trends in Attitudes Toward Surveillance Measures, 291	
M.5.2	Communications Monitoring, 294	
M.5.3	Monitoring of Financial Transactions, 300	
M.5.4	Video Surveillance, 301	
M.5.5	Travel Security, 302	
M.5.6	Biometric Identification Technologies, 303	
M.5.7	Government Use of Databases and Data Mining, 304	
M.5.8	Public Health Uses of Medical Information, 306	
M.6	The Balance Between Civil Liberties and Terrorism Investigation, 310	
M.6.1	Civil Liberties Versus Terrorism Prevention, 311	
M.6.2	Privacy Costs of Terrorism Investigation, 315	
M.6.3	Personal Willingness to Sacrifice Freedoms, 316	
M.6.4	Concerns About Uses of Expanded Powers, 317	
M.7	Conclusions, 319	
M.8	Annex, 322	
M.8.1	Details of Cited Surveys, 322	
M.8.2	Research of Organization/Sponsor Name Abbreviations, 322	
M.8.3	List of Surveys, 324	
M.8.4	References, 334	
N	Committee and Staff Biographical Information	335
O	Meeting Participants and Other Contributors	