**Comparative Policy Evaluation Series**
Ray C. Rist, series editor

*Program Evaluation and the Management of Government*
edited by Ray C. Rist

*Budgeting, Auditing, and Evaluation*
edited by Andrew Gray, Bill Jenkins, and Bob Segsworth

*Can Governments Learn?*
edited by Frans L. Leeuw, Ray C. Rist, and Richard C. Sonnichsen

*Politics and Practices of Intergovernmental Evaluation*
edited by Olaf Rieper and Jacques Toulemonde

*Monitoring Performance in the Public Sector*
edited by John Mayne and Eduardo Zapico-Goñi

*Public Policy and Program Evaluation*
by Evert Vedung

*Carrots, Sticks, and Sermons: Policy Instruments and Their Evaluation*
edited by Marie-Louise Bemelmans-Videc, Ray C. Rist, and Evert Vedung

*Building Effective Evaluation Capacity*
edited by Richard Boyle and Donald Lemaire

*International Atlas of Evaluation*
edited by Jan-Eric Furubo, Ray C. Rist, and Rolf Sandahl

*Collaboration in Public Services: The Challenge for Evaluation*
edited by Andrew Gray, Bill Jenkins, Frans Leeuw, and John Mayne

*Quality Matters: Seeking Confidence in Evaluation, Auditing, and Performance Reporting*
edited by Robert Schwartz and John Mayne

*From Studies to Streams: Managing Evaluation Services*
edited by Ray C. Rist and Nicoletts Stame

*Open to the Public: Evaluation in the Public Arena*
edited by Richard Boyle, Jonathan D. Breul, and Peter Dahler-Larsen

# Making Accountability Work

## Dilemmas for Evaluation and for Audit

## Comparative Policy Evaluation, Vol. 14

**Edited by**
**Marie-Louise Bemelmans-Videc, Jeremy Lonsdale and Burt Perrin**

**With a foreword by Amitai Etzioni**

**Transaction Publishers**
New Brunswick (U.S.A.) and London (U.K.)

This book is printed on acid-free paper that meets the American National Standard for Permanence of Paper for Printed Library Materials.

Library of Congress Catalog Number: 2007017718
ISBN: 978-0-7658-0399-3
Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

Making accountability work : dilemmas for evaluation and for audit / Marie-Louise Bemelmans-Videc, Jeremy Lonsdale, and Burt Perrin, editors.
p. cm.—(Comparative policy evaluation series)
Includes index.
ISBN 978-0-7658-0399-3
1. Policy sciences—Evaluation. 2. Auditing—Evaluation. 3. Auditing—Law and legislation 4. Public administration—Evaluation. 5. Evaluation. I. Bemelmans-Videc, Marie-Louise. II. Perrin, Burt. III. Lonsdale, Jeremy.

H97.M363 2007
352.3'5—dc22 2007017718

# Contents

# Foreword

*Amitai Etzioni*

Accountability deserves much more attention than it has been getting; the book before us makes a major contribution to highlight its importance. It sounds like a dull subject, something having to do with annual reports and accountants. Actually at the heart of the matter is ensuring that actions are carried out in line with legitimate policies, those set by law, in line with ethical precepts, and properly authorized by a legislature or corporate board and executive.

The importance of accountability can be highlighted by paying mind to the frequent attention paid to the need for balance between individual rights and public safety and health. I use this key area to illustrate the importance and ways of accountability, public accountability, for the rest of this foreword. The book itself provides numerous other areas in which accountability is or ought to be studied and expanded.

When the polity tilts too far toward either safety or rights, the imbalance should be corrected. Accordingly, we must determine how the balance is affected by new technologies. Liberalizing technologies have greatly hindered the work of public authorities in the area of communications surveillance. On the other hand, new protective technologies have offset these difficulties to some extent. New legislation that adapted old laws to the new technologies has further lessened these obstacles. Finally the September 11th attack on America changed the point or zone[1] of balance by posing a new, credible threat to public safety and health. The question remains whether the new technological and legal measures enhance public safety to the extent needed or excessively intrude into individual rights.

In turn, this raises the question of how to determine whether the polity is in the zone of balance. It would take volumes to begin to do justice to this issue, but I have dedicated some text to it elsewhere.[2] Briefly, I concluded that the course of a nation's laws should not be corrected unless (1) there is a compelling reason, a concept akin to "clear and present danger" although not necessarily as strict; (2) the matter cannot be addressed by non-legal, voluntary means; and (3) one can make the intrusion small and the gain—either in safety or in rights—considerable. These criteria can be applied to the issues discussed here.

For example, after September 11th, the government should have greater powers to decrypt e-mail because (1) terrorism does pose a major threat; (2) voluntary means to fight encrypted terrorist messages have not sufficed; and (3) decrypting e-mail messages is not more intrusive than tapping a phone. Some other new measures, such as roving wiretaps, may also pass the same test.

To judge whether a new measure that enhances the powers of public authorities is called for, I suggest a second, perhaps more decisive, form of balancing. Its concern is not whether the government should be accorded new powers, but how closely it is held accountable regarding the ways it uses these powers. From this viewpoint, the key issue is not whether certain powers, like the ability to decrypt email, should be available to public authorities, but whether these powers are used legitimately and whether mechanisms are in place to ensure proper usage. This is similar to passing over the question of whether there is too much money in a vault in favor of asking how strong the locks are.

Although the two forms of balance have some similarities and points of overlap, they are quite distinct. The cyber-libertarians' argument that the government should not be able to decrypt encoded messages is different from recognizing that such powers are justified as long as they are properly circumscribed and their use is duly supervised. The balance sought here is not between the public interest and rights, but between the supervised and the supervisors. Deficient accountability opens the door to government abuses of power, and excessively tight controls make agents reluctant to act. Thus, a case can be made that under most of Hoover's reign, the FBI was insufficiently accountable. One could also argue that under the new rules adopted following the Church Commission report, the FBI was excessively limited in its ability to conduct communications surveillance. Agents, fearing reprimands and damage to their careers, may have been too reluctant to act.

## Layers of Accountability

### *Limitations Built into the Law*

Limitations on the use of new powers are written into the laws governing them and limitations on protective technologies are often built into the technologies themselves. Roving and other types of intercepts are not granted without limits. Title III lays out a requirement for "minimization." It states that "[e]very order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."[3] Such built-in guidelines are intended to limit the ability of public authorities to gather and use information not directly related to their investigations.[4] Practically, this means that agents are not allowed to record conversations unrelated to the subject of the investigation and should stop listening when irrelevant matters are being



discussed. If agents are unsure whether a seemingly innocent conversation might touch on a relevant subject at some point, agents are to conduct "spot monitoring," in which they tune in every few minutes to check but only begin to record when appropriate.[5]

In Scott v. United States,[6] the Supreme Court found that an agent's implementation of minimization guidelines must be evaluated under a "standard of objective reasonableness," so that if circumstances make minimization difficult, an agent's failure to attempt it does not constitute an illegal violation.[7] In addition, if investigators have reason to suspect a conspiracy involving a large number of people, they are justified in recording and listening to all conversations until they are certain who is innocent and who is not.[8] Any critics point out that under any circumstances, minimization is voluntary and we must rely on our trust in law enforcement officers to do it properly,[9] highlighting the importance of further layers of accountability, such as the exclusionary rule.[10]

Although telephone wiretaps require human judgment to implement minimization, new public protective technologies, if properly used, carry out much of the minimization function automatically. Carnivore's filters, if set properly, act as a built-in minimization process, intercepting only what is appropriate. Although it might be capable of collecting all content that passes through it, it can and should be set to capture only data sent to and from a specific user in compliance with court orders.[11] As mentioned before, data that does not fit the filter settings merely passes through without being saved by Carnivore and is not seen by public authorities.[12]

### *Supervision Within Executive Agencies*

Numerous accountability mechanisms are built into the executive agencies of the government. Of course, numerous FBI guidelines exist, and supervisors are to ensure that field agents abide by these guidelines.[13] Moreover, when agents cross the line, they face internal reviews. In addition, the Attorney General's office supervises the FBI to some extent. For instance, as already mentioned, requests by the FBI to conduct communications surveillance under FISA must be approved by the Attorney General's office before they are submitted to the FISC. In some cases, court order or warrant requests never get past internal FBI approval procedures. For example, before September 11th, Zacarias Moussaoui, the possible "20th hijacker," was arrested on immigration charges, and field agents wanted to search his computer, but their request never made it past FBI attorneys, who found insufficient evidence to justify it.[14]

### *Courts*

Once surveillance technology makes it possible to scan e-mail or decrypt messages and once it is established in principle that the government will have

access to such technology, the question for both sides becomes: under what conditions should the government be allowed to use it? The contest on this second-level issue often centers on the issuance of warrants and court orders.

Civil libertarians contend that courts issue search orders too liberally, without due scrutiny.[15] In fact, around 10,000 intercept orders have been granted under FISA since its creation in 1979,[16] amounting to under 1,000 per year. Civil libertarians point to the fact that the FISC has only denied one request for surveillance in its entire history[17] as evidence that the standards for receiving a FISA intercept order are lower than for receiving a Title III order.[18]

Though applications for intercept orders are rarely turned down by the FISC, public safety advocates point out that it is embarrassing and damaging to agents' records and careers to be turned down by the FISC, and as a result, they are reluctant to request warrants even when they seem justified.[19] Moreover, if the FISC finds insufficient justification, it tends to return the request, and attorneys either submit further documentation or abandon the application before receiving an official rejection, which accounts for there being next to no outright refusals.[20] Furthermore, some requests never get past the Attorney General's office.[21] Lastly, FISA applications need to meet preset guidelines and must include a statement of the means by which the surveillance will be conducted as well as a statement of proposed minimization procedures.[22]

Although civil libertarians typically prefer courts to administrative agencies,[23] they fear that judges might be unable or disinclined to curb law enforcement agents.[24] First, judges are either elected or politically appointed, making them subject to the influence of public opinion.[25] In addition, they might be less cautious in granting warrants and court orders that apply to other jurisdictions, which the USA PATRIOT Act allows. Judge Meskill, in his concurrence in United States v. Rodriguez,[26] warned:

> [J]udges may be more hesitant to authorize excessive interceptions within their territorial jurisdiction, in their own back yard so to speak, than in some distant, perhaps unfamiliar, part of the country. Congress determined that the best method of administering wiretap authorizations included territorial limitation on the power of judges to make such authorizations.[27]

As a result, courts would be a relatively weak accountability mechanism for nationwide warrants. In addition to the requirements that must be met to get a warrant or court order in the first place, courts ensure that law enforcement agents act within the limits of their power by suppressing illegally collected evidence. The exclusionary rule, established in Boyd v. United States[28] and reaffirmed in Weeks v. United States,[29] states that evidence collected in violation of the Fourth Amendment must be excluded in a trial against the suspect.[30] This serves not only to protect the suspect after a violation occurs but also to deter inappropriate searches because agents know that if they do not follow the correct procedures, the culprits might go free.



*Congress*

Under our system of checks and balances, Congress is supposed to oversee the work of the executive branch and its agencies. It has many instruments for doing so. It can require heads of agencies and other high-ranking officials to respond to written questions, testify before congressional committees, and turn over documents. It may order the General Accounting Office to perform a study. In addition, Congress can conduct committee hearings in which interested parties can voice their concerns.

Civil libertarians argue that many of the measures included in the USA PATRIOT Act were enacted in a great rush without the usual hearings and deliberations.[31] Supporters of the public authorities point out that after September 11th it was assumed that there were other "sleeper" terrorist agents in the United States and that other attacks were imminent, which justified the rush. Indeed, they held that expanded powers should have been given well before September 11th.[32] Moreover, Congress had begun to address these issues before September 11th by holding hearings on Carnivore.[33]

*The Public*

The ultimate source of oversight is the citizenry, informed and alerted by a free press and by civil liberties advocates and briefed by public authorities. To be fully effective in overseeing the issues at hand, civil libertarians argue that the public must be informed about the inner workings of the protective technologies, while public authorities claim that such disclosures would inform terrorists and other criminals about how to circumvent the technologies, thus rendering them useless. Specifically, since the existence of Carnivore was made public, numerous parties have demanded access to information about how it works. The ACLU filed a Freedom of Information Act ("FOIA") request to get its source code,[34] which reveals the technical commands and internal structure of a program. EPIC filed a FOIA request to gain a copy of all documents relating to Carnivore.[35] In addition, numerous ISPs who might be asked to cooperate in installing Carnivore have called for guarantees that the program works as claimed and that there are sufficient controls to keep law enforcement agents from capturing more than what is covered by a court order.[36] In Scarfo, the judge joined civil liberties groups in demanding that the FBI release information on how KLS works, stating that he could not rule on whether its use was legal without knowing how the technology worked. The judge said he would review the technology secretly.[37] This solution satisfied neither the civil libertarians nor the FBI. David Sobel of EPIC said the matter raised "very basic questions of accountability. The suggestion that the use of high-tech law enforcement investigative techniques should result in a departure from our tradition of open judicial proceedings is very troubling."[38] Donald Kerr, Director of the FBI's

Laboratory Division, stated that the disclosure of certain information about KLS would "compromise the use of this technology ... and jeopardize the safety of law enforcement personnel."[39]

Secrecy also remains one of the key objections to the use of roving intercepts under FISA. FISA was established in the mid-1970s after the public was alarmed to learn of the activities of President Nixon and the NSA's illegal interception of telegraph and telephone calls.[40] A congressional committee was created to investigate and found that nearly every president had authorized warrantless communications surveillance, often for political purposes.[41] Essentially, agencies such as the FBI, CIA, and NSA were able to conduct surveillance without going through normal criminal procedures. The Department of Justice launched its own in-house investigation, resulting in new guidelines for both domestic and foreign intelligence investigations.[42] To prevent future abuses, Congress passed FISA in 1978 to spell out what intelligence agencies could and could not do.[43] The NSA had insisted that its activities—especially regarding its methods and technologies—would be severely compromised if discussed in open court. In response, FISA authorized the formation of a special federal court whose proceedings could be completely secret.[44] In short, while the public cannot be informed about all the workings of all the protective technologies, such as Carnivore, because this would impair the usefulness of the technologies, the public can act as the ultimate enforcer of accountability. Ultimately, this is a question of whom we trust.

*Trust*

Accountability is ultimately a matter of trust. Plato is said to have raised the issue in asking *quis custodiet ipsos custodes*, or who will guard the guardians.[45] Others attribute the question to the Roman satirist Juvenal, who wrote around 2000 years ago.[46] The issue, though, is very much with us today. If we do not trust the cops on the beat, we may ask their captains to keep them under closer supervision. If we do not trust the captains, we may call on the mayor to scrutinize the police. We may call on the other branches of government, especially the courts, to serve as checks and balances. However, if we believe that the mayors are corrupt and the judges cannot be trusted, we have little to fall back on other than the press. Yet the media, too, is often distrusted.[47]

The question, then, is whom we should distrust and how much. If no authority or media figure is trustworthy and "The System" is corrupt, we face a much larger problem than if, in a few instances, public authorities intercept more e-mail than they are supposed to or tap phones they should not. If someone believes the entire system is untrustworthy, she should either move to another country or fight for an entirely new political system. However, if the problem is only some individuals in positions of authority, we have good reason to watch out for those individuals but not to doubt the entire political system. We ought,



then, to work to improve the various layers of accountability but also realize that the fact that critics can always come up with some horror stories does not necessarily mean that those stories are typical of the system.

In total, determining whether a specific public policy measure is legitimate entails more than establishing whether it significantly enhances public safety and minimally intrudes on individual rights. It also requires assessing whether those granted new powers are sufficiently accountable to the various overseers—ultimately to the citizenry. Some powers are inappropriate no matter what oversight is provided.

However, others are appropriate given sufficient accountability. If accountability is deficient, the remedy is to adjust accountability, not to deny the measure altogether.[48] Whether the specific powers given to the government sustain or undermine the balance between rights and safety depends on how strong each layer of accountability is, whether higher layers enforce lower ones, and whether there are enough layers of accountability. I suggest that we should ignore both public authorities' claims that no strengthening of accountability is needed and the shrillest civil libertarian outcries that no one is to be trusted. Instead, we should promote reforms that will enhance accountability rather than deny public authorities the tools they need to do their work. This does not necessarily mean granting them all the powers they request, but in a world where new technologies have made the government's duties more difficult and in which the threat to public safety has vastly increased, we should focus more on accountability before denying powers to law enforcement.

Professor Amitai Etzioni is University Professor and Director of the Institute of Communitarian Policy Studies at The George Washington University in Washington, DC. He has held a number of academic posts in a distinguished career stretching back almost fifty years. He is the author of more than twenty books and numerous articles. In 2001 he was named amongst the top 100 American intellectuals.

## Notes

1. I refer to a zone because I do not claim that there is a precise point of balance that one can identify at which the government tilts clearly too far in one direction or the other.
2. See *The New Golden Rule: Community and Morality in a Democratic Society,* New York: Basic Books, 1997; and *How Patriotic is the Patriot Act?* New York: Routledge, 2004.
3. 18V .S.C.§ 2518(5)( 2000).
4. *Id.*
5. See, e.g., United States v. Clerkley, 556 F.2d 709 (4th Cir. 1977); United States v. Losing, 539 F.2d 1174, 1180 (8th Cir. 1976); United States v. Costello, 610 F. Supp. 1450, 1477 (N.D. III. 1985); United States v. Clemente 4, 82 F. Supp. 102, 108-10 (S.D.N.Y. 1979).
6. 436 U.S. 128 (1978).
7. *Id.* at 137-39.

8. *See Id.* at 142.
9. See Rep. Bob Barr, *A Tyrant's Toolbox: Technology and Privacy in America*, 26 J. LEGIS 71, 74 (2000).
10. *See Id.* at 85.
11. *See* ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, INDEPENDENT REVIEW OF CARNIVORE SYSTEM -- FINAL REPORT http://www.epic.org/privacy/carnivore/camiv_final.pdf (Dec. 8, 2000) [hereinafter IITRI Report] at §§ ES.5, 3.4.4.1.6.
12. *See Id.* § 3.4.4.1.3.
13. *See Id.* §§ 3.2-3.3; see also Orin Kerr, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001) (on file with Computer Crime and Intellectual Property Section, United States Dep't of Justice).
14. *See* Dan Eggen & Brook A. Masters, *US. Indicts Suspect in September 11 Attacks*, WASH. POST, Dec. 12, 2001, at A1.
15. See William Carlsen, Secretive U.S. Court May Add to Power, S.F. CHRON., Oct. 6, 2001, atA3.
16. *See Id.*
17. *See Id.*
18. Carnivore's Challenge to Privacy and Security Online: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 107th Cong. (2001) (statement of Alan Davidson, Staff Counsel, Center for Democracy and Technology), available at http://www.cdt.org/testimony/000724davidson.shtml ("Finding the addressee of an email or the name of a web site being visited -- if that is what law enforcement is seeking -- will often require analysis of the content of packets, not just the header information.") [hereinafter Davidson statement].
19. Interview with Orin Kerr, Associate Professor of Law, George Washington University, and former trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Dept. of Justice, in Washington, D.C. (Dec. 14, 2001).
20. Victoria Toensing, Remarks at the Communitarian Dialogue on Privacy vs. Public Safety (Nov. 26, 2001), *at* http://www.gwu.edu/-ccps/privtrans.htm [hereinafter Toensing remarks].
21. See Carlsen, supra note 15.
22. See 50 U .S.C. § 1804(a)(2000).
23. ACLU, *USA PATRIOT Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances*, at http://www.aclu.org/congress/l110101a.html (Nov. 1, 2001).
24. See ACLU, *More Detail on ACLU Objections to Selected Provisions of Proposed Anti-Terrorism Legislation* (2001) ("Law enforcement, rather than a Court, will decide what is 'content' and systems like Carnivore will be used without any real judicial supervision."), at http://www.aclu.org/congresslPatriot_Links. (last visited Mar. 4, 2002).
25. See William Mishler and Reginald S. Sheehan, Public Opinion, the Attitudinal Model, and Supreme Court Decision Making: A Micro-Analytic Perspective 5, 8 J.POL: 169, 169-200 (1996); Beverly B. Cook, Public Opinion and Federal Judicial Policy, 21 AM. J. POL. SCI. 567, 567-600 (1977).
26. 968 F.2d 130 (2d Cir. 1992).
27. *Id.* at 135.
28. 116 U.S. 616 (1886).
29. 232 U.S. 383 (1914).



30. Although the rule has been diluted somewhat, it is still controlling law. See, e.g., United States v. Leon, 468 U.S. 897 (1984) (establishing a "good faith" exception to the exclusionary rule); Nix v. Williams, 467 U.S. 431, 444 (1984) (creating the "inevitable discovery" exception to the exclusionary rule); Massachusetts v. Sheppard, 468 U.S. 981 (1984) (upholding the "good faith" exception); United States v. Calandra, 414 U.S. 338, 348 (1974) (establishing that the exclusionary rule does not proscribe use of all illegally obtained evidence). For further discussion, see Leslie-Ann Marshall and Shelby W ebb, Jr., Constitutional Law -The Burger Court's Warm Embrace of an Impermissibly Designed Interference with the Sixth Amendment Right to the Assistance of Counsel – The Adoption of the Inevitable Discovery Exception to the Exclusionary Rule: Nix v. Williams, 28 How. L.J. 945 (1985); Christopher A. Harkins, The Pinocchio Defense Witness Impeachment Exception to the Exclusionary Rule: Combating a Defendant's Right to Use with Impunity the Perjurious Testimony of Defense Witnesses, 1990 U. ILL. L. Rev. 375, 389-412 (1990).
31. Representatives of the ACLU have stated:

> The process that brought you this bill is terribly flawed. After bypassing a Judiciary Committee mark-up, a few Senators and their staffs met behind closed doors, on October 12, 2001 to craft a bill. The full Senate was presented with anti-terrorism legislation in a take-it-or-leave-it fashion with little opportunity for input or review. No conference committee met to reconcile the differences between the House and Senate versions of the bill. We find it deeply disturbing that once again the full Senate will be forced to vote on legislation that it has not had the opportunity to read. Senate offices are closed and staff cannot even access their papers to fully prepare you for this important vote. Regular order is being rejected and it is an offense to the thoughtful legislative procedures necessary to protect the Constitution and Bill of Rights at a time when the rights of so many Americans are being jeopardized.

*See* Letter from Laura W. Murphy, Director, ACLU Washington Office and Gregory T. Nojeim, Associate Director and Chief Legislative Counsel, ACLU, to Senate (Oct. 23, 2001) (urging rejection of the final version of the USA PATRIOT Act), http://www.aclu.org/congress/l102301k.html (last visited Mar. 26, 2002) [hereinafter Murphy letter].
32. Senator Hatch remarked:

> We can never know whether these tools would have prevented the attack on America, but, as the Attorney General has said, it is certain that without these tools we did not stop the vicious acts of last month. I personally believe that if these tools had been in law—and we have been trying to get them there for years—we would have caught those terrorists. If these tools could help us now to track down the perpetrators—if they will help us in our continued pursuit of terrorists—then we should not hesitate to enact these measures into law. God willing, the legislation we pass today will enhance our abilities to protect and prevent the American people from ever again being violated as we were on September 11.

147 Congo Rec. S10,990 (2001) (statement of Sen. Hatch).
33. *See, e.g., Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution, House Comm. on the Judiciary*, 106th Congo (2000), available at http://www.house.gov/judiciary/con07241.htm (last visited Mar. 4, 2002); *The "Carnivore" Controversy: Electronic Surveillance*

*and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong., available at http://www.senate.gov/-judiciary/oldsite/wI96200f.htm (last visited Mar. 4, 2002).

34. *See* Press Release, ACLU, In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Programs (July 14, 2000), http://www.aclu.org/news/2000/n071400a.html (last visited Mar. 4, 2002).
35. *See* Press Release, EPIC, Lawsuit Seeks Immediate Release of FBI Carnivore Documents (Aug. 2, 2000), http://~.epic.org/privacy/carnivore/8_02_release.html (last visited Mar. 4, 2002).
36. *See* Nick Wingfield & Don Clark, *Internet Companies decry FBI's E-mail Wiretap Plan*, WALL ST. J., July 12,2000, at B11A.
37. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 575 (D.N.I. 2001).
38. John Schwartz, *U.S. Refuses to Disclose PC Tracking*, *The New York Times*, Aug. 25, 2001, at C1.
39. Jonathan Krim, *High-Tech FBI Tactics Raise Privacy Questions*, WASH. POST, Aug. 14, 2001, at A1.
40. *See* Jim McGee, The Rise of the FBI, WASH. POST MAG., July 20, 1997, at W10.
41. *See* FBI's "*Political Abuses*," U.S. NEWS & WORLD REP., Dec. IS, 1975, at 61.
42. *See THE* FBI: A COMPREHENSIVE REFERENCE GUIDE 38 (Athan G. Theoharis ed., 1999) [hereinafter Theoharis].
43. *See* McGee, supra note 40.
44. 50 U.S.C. § 1803(c) (2000).
45. *See* Robert O. Keohane, *Governance in a Partially Globalized World*, 95 AM. POL. SCI. REV. 1 (2001).
46. *See* Martin Edmonds, *Politics, Law, Economics and Social*, 62 INT'L AFFAIRS 290 (1986) (reviewing MILITARY INTERVENTION IN DEMOCRATIC SOCIETIES (Peter J. Rowe and Christopher J. Whelan eds., 1985)).
47. *See generally* SEYMOUR MARTIN LIPSET & WILLIAM SCHNEIDER, THE CONFIDENCE GAP: BUSINESS, LABOR, & GOVERNMENT IN THE PUBLIC MIND (rev. ed., Johns Hopkins U. Press 1987) (1983) (studying trends, causes, and consequences of public confidence in U.S. institutions).
48. It is true that accountability can be excessive and that law enforcement agents can be reluctant to act due to fear that they will be penalized by superiors, courts, or Congress, or be skewered by the press. However, there have been no signs of this since September 11th.

# Part One

# Modern-Day Accountability: Evaluation and Audit Challenged