some studies that seem to support the suggestion "that more information can have the effect of changing attitudes towards a pro-abolitionist position." He maintains that "governments have a duty to make sure that all their citizens have the opportunity to base their views about the death penalty on a rational appreciation of the facts." They should also "encourage properly independent research on the operation of the system at all levels and upon its effects on capital crimes."

At the same time, he is clearly aware that more is involved in both support and opposition to the death penalty than "rational appreciation of the facts." He notes, for example, that a 1985 survey of 600 United States lawyers found two-thirds to be in favor of executing those persons currently on death row. And he says "while empirical evidence may shed light on the reality of homicide, on the way the death penalty is applied, and its effects on the level of the crime it is meant to deter, the way in which these findings will be interpreted, the weight attached to them, and the inferences drawn from them will all inevitably be coloured by broader moral and political judgements."

Here he comes close to the heart of the matter. As Hans Zeisel pointed out some years ago, the worldwide decline of the death penalty has nowhere been significantly connected with arguments about the empirical evidence. It may be that there are social policy issues which can be settled simply by reference to empirical data but the issue whether or not the death penalty should be prescribed by law for any crime is not one of them. It is preeminently a political and moral question, not an empirical one.

ADMINISTRATIVE LAW
THE OVERSIGHT OF DATA PROTECTION LAW

PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA AND THE UNITED STATES. By David H. Flaherty. Chapel Hill: University of North Carolina Press, 1989. Pp. 483.

*Reviewed by Paul Schwartz**

In the data banks of the state are boundless amounts of information that relate to identifiable persons. This information is monitored, processed, and stored within the government in order to administer services and to control the individual who appears before the state's administrative apparatus. Private organizations employ

* Assistant Professor of Law, University of Arkansas, Fayetteville. Member, Board of Editors, American Journal of Comparative Law.

their own extensive collections of personal data for similar purposes. Sometimes the state and private organizations even share data with one another. Widespread use of computers has encouraged and strengthened this sharing and processing of personal information. Today, the control of the individual described in George Orwell's *Nineteen-Eighty Four* is perfectable beyond that book's nightmare vision: computers are now used to carry out an intense, on-going monitoring of personal data.

The legal response to this situation in most Western nations has been the creation of "data protection law." The goal of this field of law is to preserve individual liberties and to guard against the Orwellian danger of absolute control of the individual. Meeting this goal requires the structuring of a compromise between concealment and exposure of personal data. An important component of this compromise has been the organization of an oversight agency whose task is to observe the effects of data use and of its regulation. A government agency with oversight responsibilities has been an almost inevitable accompaniment to the rise of data protection law.

In *Protecting Privacy in Surveillance Societies*, David H. Flaherty undertakes a successful comparative study of the phenomenon of data protection oversight.[1] His ambitious work examines the administration of data protection law in five nations: the Federal Republic of Germany, Sweden, France, Canada, and the United States. He concentrates on oversight of the government's data banks, but makes some comments about oversight of the private sector as well. Rich in detail, Flaherty's book illuminates both broad and fine distinctions in the responses of five legal cultures to a similar problem. The author's conclusion is that the "advisory model" of oversight of the Federal Republic of Germany and Canada has been far more effective than either the "licensing model" of France and Sweden or the approach of the United States, which I will call the "dispersed responsibility model." This book has particular relevancy for an American audience: currently before the Congress is a bill to change the American system by creating a Data Protection Board that would follow the "advisory model."[2]

I

Under the licensing approach, Sweden's Data Inspection Board (DIB) and France's Commission Nationale de l'Informatique et des Libertés (CNIL) have the responsibility of granting authorization for public and private data processing systems. This task is an enormous one; and, according to Flaherty, neither of these boards has the resources to carry out this job. The shared response to this situation has been to adopt simplified forms and practices that allow ap-

1. David H. Flaherty, *Protecting Privacy in Surveillance Societies* 17, 93, 183 (1989) (hereinafter cited as Flaherty).

2. H.R. 685, 102nd Cong., 1st Sess., 137 Cong. Rec. 755 (1991) (hereinafter cited as "American Data Protection Bill").

proval of many data systems without formal screening.[3]

Most of the licensing in these two countries is now carried out through such pro forma methods. In the latest year for which data are available from France, for example, the CNIL received 1,763 requests for a formal opinion, 3,928 "ordinary declarations" (which generally require staff but not commission action), and 24,184 simplified and model declarations, which automatically receive approval after a certain number of days unless the CNIL takes some action.[4] These figures indicate that a considerable burden remains on the CNIL even after the attempt to lighten its workload. Of the Swedish and French approach, Flaherty observes, "a very bureaucratic approach to data protection for the public *and* private sectors bogs down in paperwork and the registration of data banks to the neglect of audits, the investigation of complaints, and the conduct of meaningful public relations."[5]

The licensing model suffers not only from bureaucratic gridlock, but also from the organization of the Swedish and French boards as "miniparliaments."[6] In both countries, the data protection boards are deliberative bodies whose members come from the legislature and important interest groups. Within the model shared by these two countries, the Swedish Board is distinguished by the greater power of its head, the Director General. Groups represented on the Swedish DIB include "the legislature, the major trade unions, industry, the public administration, and the research community."[7] France's CNIL has a similar makeup. It is a commission of seventeen members, of whom twelve are chosen by "(v)arious major public bodies."[8] These kinds of miniparliaments are intended to lead to a diversity of opinion and a broad basis of support. But, according to Flaherty, although these boards should have a great deal of direct authority because of their ability to approve or deny licenses, their close links to existing power structures and their lack of clout limit their desire and ability to carry out their administrative mission. Instead of vigorously articulating support for personal liberties, the licensing boards tend to strike a balance between competing interests that accommodates almost all proposals for data processing systems.[9]

On the limitations of the licensing approach, Flaherty is convincing. Despite formalistic assurances of authority, these agencies often resort to less than fruitful accommodations. Questions remain, however, as to why this approach was adopted and whether it remains attractive in Sweden and France. The extent to which pro forma practices and standardized forms have altered the "pure" li-

3. Flaherty, supra n. 1 at 131, 201.

4. Commission nationale de l'informatique et des libertés, 10e rapport d'activité 54 (1989) (hereinafter cited as "CNIL Report").

5. Flaherty, supra n. 1 at 165-66 (emphasis in original).

6. Id. at 99, 193-196.

7. Id. at 101.

8. Id. at 169, 172.

9. Id. at 185, 187.

censing model indicates that some kind of compromise approach is now employed in Sweden and France. Moreover, while Flaherty does make some sensible general comments about the roots of the French and Swedish boards,[10] he does not locate these systems in a significant way within the political, legal, and social cultures of which they are a part. In the case study of the French commission, this lack of a detailed contextual analysis is made worse by a failure of authorial sympathy.

The French case study is, to be sure, the most interesting of the five in *Protecting Privacy in Surveillance Societies*. Researched with Flaherty's usual thoroughness and care, these chapters are also written with exceptional verve. Quite clearly, Flaherty is disappointed by the CNIL and the French system of data protection. In his view, "French data protection illustrates a preoccupation with grandiose principles and rhetoric to the neglect of effective implementation, a situation exacerbated by part-time commissioners, weak leadership, and inexperienced staff at the CNIL, especially in the first years."[11] Flaherty characterizes the French board as an elite organization in a highly politicized government and in a society run by elites. But Flaherty is also somewhat irritated by the French approach to data protection. He writes, "[t]he reality of CNIL's 'independence' is that almost all its members are politicians in the sense of being well aware, in good French tradition, of the current direction of the political winds."[12] This characterization is less than fair.

A relation between politics and administration, on the one hand, and elite groups and government, on the other, is unique neither to France nor to data protection. To take just the area of politics and administration, no course in American administrative law is complete without consideration of the infamous saga of the National Highway Traffic Safety Administration's imposition and suspension of seat-belt and air bag requirements in the 1970's and 1980's.[13] This shifting of standards accompanied changes in the views of successive occupants of the White House and in the relative lobbying power of the American automobile industry.[14]

French administrators are not the only ones who pay attention

---

10. Id. at 96-101, 166-72.
11. Id. at 165.
12. Id. at 185.
13. See Motor Vehicle Manufacturers Association of the United States Inc. v. State Farm Mutual Automobile Insurance Co., 463 U.S. 29, 34 (1983) ("The regulation whose rescission is at issue bears a complex and convulated history. Over the course of approximately 60 rulemaking notices, the requirement has been imposed, amended, rescinded, reimposed, and now rescinded again.").
14. See id. at 59 (Rehnquist, J., concurring in part and dissenting in part) ("The agency's changed view of the standard seems to be related to the election of a new President of a different political party."). See also J. Mashaw & D. Harfst, *The Struggle for Auto Safety* 247-48 (1990) ("Regulatory agencies are in politics. They must pursue their objectives by political means, that is, by developing and employing political resources.").

to the current direction of the political wind. Indeed, Flaherty's own study of American data protection law, as we shall see, shows that politics have a great influence on the behavior of another land's data protection administrators.[15] In his account of the French administration of data protection law, Flaherty needed to explore more deeply how the CNIL both follows and deviates from French traditions. The question is how the CNIL functions in a French context and how it might be made more effective within this framework. But Flaherty has, in fact, spoken to at least one aspect of the issue of effectiveness. He believes that the CNIL would do a better job if it carried out more audits.[16] In recent years, the CNIL has started such a "politique de contrôle" by increasing the number of visits that it makes to data processors throughout France.[17]

II

Flaherty's great contrast with the limitations of the licensing model is offered by his case studies of the merits of the advisory model of Canada and the Federal Republic of Germany. In Canada, a privacy commission, headed by a single figure who is responsible to the Parliament, acts as an ombudsman for citizen complaints and as an auditor of the federal government's handling of personal information.[18] In Germany, the federal data protection commission is also headed by a single figure, but it is located within the Federal Ministry of the Interior. Flaherty notes that this administrative attachment "creates some diversion of loyalties and interests."[19] In part, the problem is that "an ambitious person must pay attention to his or her career prospects within the ministry."[20]

Some German states, such as Hesse, have made clearer provisions for independence of their data protection entities. The Hesse Data Protection Commission, like the Canadian, is not placed within a ministry. In the case of Hesse, the State Data Protection Commissioner is elected by the Hesse Parliament, must report to Parliament, and is part of the administrative apparatus of Parliament.[21] Yet despite the location of the German Federal Commission, it does have, as Flaherty makes clear, the freedom "to set its own priorities and create its own agenda"—a freedom made greater by an absence of the licensing burden given to Swedish and French boards.[22] The 1990 amendments to the German Federal Data Protection Law have

15. See Flaherty, supra n. 1 at 306 ("OMB's lack of political will to act on privacy matters during the Reagan presidency [illustrates] once again the importance of the political climate for effective implementation of data protection and limiting surveillance.").
16. Id. at 204.
17. CNIL Report, supra n. 4 at 59-60.
18. Flaherty, supra n. 1, at 246-52.
19. Id. at 41.
20. Id.
21. Id. at 42-3. See Hessiches Datenschutzgesetsz, GVBl. I 1986, 309, § 30.
22. Flaherty, supra n. 1 at 56.

made some changes in this picture. The positive change is that the Federal Data Protection Commissioner is now to be elected by the Federal Parliament.[23] Under the previous law, the Commissioner was selected by the government without formal legislative approval.[24] The negative change is that the Commissioner's auditing of certain kinds of files is now limited by the concerned individual's ability to refuse access to this information.[25] This veto power may handicap the Commissioner's oversight of certain agencies.[26]

The role of the Canadian and German commissioners is to advise, admonish, and assist the government. Moreover, they have a special obligation to help anyone who believes that the government's processing of his personal data has caused a hardship to a legal interest. Although binding legal decisions concerning data protection rest elsewhere, Canadian and German data protection commissioners can investigate and submit formal complaints to the responsible federal ministers. They can also "appeal to the media and to the legislature."[27]

In *Protecting Privacy in Surveillance Societies*, Flaherty describes a paradox within the administration of data protection law. The boards that have less authority directly assigned to them have been the most successful ones. Oversight agencies that lack the ultimate authority to approve processing systems have done more for data protection than the licensing boards with such authority. Flaherty writes, "[w]hile West German or Canadian data protectors run the risk of having their advice ignored or spurned, their Swedish and French counterparts, whose powers of compulsion are much greater, are often reluctant to take strong stands against surveillance practices for fear of offending the government and other powerful interests."[28] Sometimes the power of persuasion is more important than a *de jure* power of decision. The Canadian and German data protection commissioners have made significant contributions towards improving the legal regulation of their respective nation's processing of personal data.

III

The United States of America has taken a third route in this area of law. Flaherty observes, "[t]he United States carries out data

23. Or to be more precise: the Federal Data Protection Commissioner is now nominated by the government (as in the old law), elected by the legislature, and is appointed by the President (as in the old law). Gesetz zur Fortentwicklung der Datenschutzverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGBl. I 1990, 2954, § 22(1) (hereinafter cited as German Data Protection Law).

24. Gesetz zum Schutz vor Mißbrauch personenbezogner Daten bei der Datenverarbeitung, vom 27. Januar 1977, BGBl. I 1977, 201, § 17 (1).

25. German Data Protection Law, supra n. 23 at § 24(2).

26. Compare Bundesbeauftragten für den Datenschutz, 13. Tätigkeitsbericht 86 (1991) with Hessische Datenschutzbeauftragte, 19. Tätigkeitsbericht 22-25 (1990).

27. Flaherty, supra n. 1 at 43.

28. Id. at 66.

protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency."[29] Flaherty describes a system in which no single agency has been created to carry out oversight. The direct origins of this approach rest in the Ford administration's firm opposition to the creation of a Privacy Board during the period of the Privacy Act's promulgation. This disfavor rested on a presidential belief that such a commission would "second-guess citizens and agencies" and would unnecessarily increase governmental bureaucracy.[30] The compromise that was struck was to disperse oversight responsibilities throughout the government and to convene a Privacy Protection Study Commission, which was designed to hold hearings, issue reports, and go out of business within a limited period of time. To the extent that oversight of governmental data processing has been provided for, it is given primarily to the Office of Management and Budget (OMB), an already existing executive branch agency with important duties, some of which are antagonistic to data protection.

The spreading of responsibilities within government and the granting of a role to OMB were not wise moves. Each governmental agency is responsible for its own compliance with data protection laws. But Flaherty notes that federal agencies have not made much of a commitment, either in terms of personnel or other resources, to achieving compliance. As for the OMB, it has never carried out an "effective monitoring of the implementation and impact" of data protection laws that is comparable with the efforts made in other nations.[31] Flaherty's verdict is a negative one: the "OMB does not carry out inspections, audits, investigations, or handle complaints; in fact, it dislikes activities unrelated to the federal budget."[32] Flaherty accounts for this attitude partially in terms of "politics." He argues that the OMB not only shared President Reagan's lack of interest in the data protection issue, but also matched his purported enthusiasm for reducing the cost of government by increasing the application of computers and their sharing of personal data.[33] This role of the OMB is not compatible with leadership in the field of data protection.

Flaherty's view of American data protection law is justifiably gloomy. In an age where "any data can be risky for purposes of surveillance, given appropriate (or inappropriate) associations with other information,"[34] an independent government agency is needed to observe and criticize the state's data processing practices. Fortunately, such an "alarm system" for civil liberties has recently been

29. Id. at 305. For discussion of constitutional elements of the ordering of data protection in America and Germany, see Schwartz, "The Computer in German and American Constitutional Law," 37 *Am. J. Comp. L.* 675 (1989).

30. Id. at 311 (quoting President Ford).

31. Id. at 333.

32. Id.

33. Id. at 325.

34. Id. at 374.

proposed by Representative Robert Wise. Unfortunately, this law may not have a good chance of passage in the current Congress.

The "Data Protection Act of 1991" would create a three-member board as a new independent agency of the Executive Branch. Careful measures exist in this bill to help provide for the actual independence of this agency. The role of the proposed board would be to offer model guidelines, issue advisory opinions, monitor compliance with data protection laws, and "accept and investigate complaints about violations of data protection rights and standards and fair information practices."[35] This bill would change America's "dispersed responsibility" approach to data protection into the kind of "advisory" model that has already proved of merit in Germany and Canada. Such a modification of American law would reflect the views of Flaherty's *Protecting Privacy in Surveillance Societies*. This book has shaped and will continue to help define the terms in which a field of law is discussed. That is an accomplishment few legal scholars attain.

CONSTITUTIONAL LAW

RAISONNER LA RAISON D'ÉTAT, VERS UNE EUROPE DES DROITS DE L'HOMME, TRAVAUX DU SÉMINAIRE "POLITIQUE CRIMINELLE ET DROITS DE L'HOMME". Edited by Mireille Delmas-Marty. Paris: Presses Universitaires de France, 1989.

*Reviewed by Wolfgang Fikentscher**

The book contains the papers presented at a symposium which was convened to study the meaning of the concept "state" in view of the growing together of the European nations to a European system of supranationality. To have a proper point of departure of what "state" means in this context, the challenge of the modern state by various terrorist groups was chosen as the catalyst of understanding. Consequently, the first chapter deals with this claim of the modern state to be a legitimate form of human organization, a claim that has been denied by many terrorist philosophies and practices. The central concept, according to the author of this chapter, which has to be used for the defense of the state is the "raison d'état." It is a term hard to be translated, and may be best rendered by "self esteem of the state."

The second part of the book is devoted to reports, country by country, how the reasoning why there should be a state is nationally understood and practiced, as against terrorists, and in general. The

35. American Data Protection Bill, supra n. 2 at Sec 5(2)(I).

* Professor of Law, Munich.