BOOK NOTE

WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS

By Ann Wells Branscomb.[1]
New York, New York: Basic Books. 1994.
Pp. 241. $25.00 (hard).

As we plunge forward into the information age, new technologies for manipulating information are being widely developed. These advances allow names, purchasing trends, and other personal facts to be almost effortlessly transferred and traded in a relatively unregulated electronic marketplace. Along with the advantages of this free flow of information comes a loss to privacy as ever-increasing databases of personal information are traded in this new information arena. The regulation of this trade requires the balancing of the First Amendment ideal of free speech, the protections of privacy law, and rights guaranteed through intellectual property law. The tension these conflicting rights create is becoming a new battleground for legal academics and the legal system.

Who Owns Information? From Privacy to Public Access attempts to identify and describe the current legal status of a number of information issues which have both privacy and property interests at stake. The book starts by stating the general proposition that there has been a transition in our society where information "has passed from being an instrument through which we acquire and manage other assets to being a primary asset itself" (p. 1). A series of case studies is then provided which help to illuminate both specific problems and their current treatment within the legal system.

The book is written primarily for the lay person with an interest in information technologies and legal issues and requires no technical background in either of these areas. While this focus does make the book more accessible, it unfortunately prevents a deep exploration into issues that might be of interest to a professional. A foundation is developed

1. Legal scholar in residence, Harvard University, Program on Information Resources Policy.

which identifies a number of intriguing and important issues, but the professional seeking in depth analysis of these issues will need to research further in order to understand many of the subtler nuances.

The first two cases in the book explore the tension between an individual's privacy interest on the one hand and the property interests of a public utility on the other. The investigation into this conflict is made through an investigation of individuals' interest in their own name, address (Chapter One), and telephone number (Chapter Two).

Another conflict analyzed is that arising between the interests of the government and the individual. Chapter Three investigates the area of medical histories, ranging from the privacy interests of those who have contracted the HIV virus, to the public interest benefit of having a centralized database of medical information available to medical practitioners throughout the country. Issues pertaining to the field of arts and entertainment are also tackled. In Chapter Four, Branscomb tackles the issue of image ownership, encompassing not only the more traditional question of photographic ownership as expanded to computer images, but also the question of computer enhanced images and colorization of movies. Chapter Six discusses the ownership of cable video entertainment and describes the battle between the cable companies and those individuals who have purchased satellite dishes.

A critical area of investigation involves issues related to computers; the ownership of these systems engender all of the other issues discussed in the book and is thus a central concern. Without these systems, the other debates become moot. The most traditional issue in this non-traditional area of information ownership (discussed in Chapter Eight) is the protection of computer software, "the crown jewels of the information economy" (p. 157). This protection is currently accomplished via a patchwork of traditional copyright, patent, and trade secret protections. Chapter Five discusses the ownership of electronic messages[2] where the primary issues of concern are: 1) do the authors of electronic mail ("e-mail") messages have a First Amendment right to write whatever they want; and 2) do system (network) administrators then have the permission, right, or responsibility to monitor such messages.

Finally, an enlightening review of the ownership disputes that have been raging among academics over the rights to study and publish the text

---

2. For a related discussion, see also Michael I. Meyerson, *Virtual Constitutions: The Creation of Rules for Governing Private Networks*, 8 HARV. J.L. & TECH. 129 (1994).

and translations of the Dead Sea Scrolls is included in Chapter Seven. The book concludes in Chapter Nine by asking: "Who Owns Government Information?" (p. 159), or "[h]ow public information is to be made available to the public" (p. 173).

As the ownership of computer software is perhaps the driving issue in this exploration of information ownership, Branscomb's treatment thereof merits further discussion. Also, the treatment of such issues typifies the treatment received by other topics discussed in the text. "At the beginning . . . it was not at all certain that software would find protection in patents or in copyrights. So lawyers turned increasingly to the trade secrets law . . ." (p. 142). This trend was slowed in the early 1980s, we are told, by: 1) Congress' amendment of the copyright law in 1980, explicitly allowing copyrighting of computer software; and 2) by the 1981 Supreme Court decision *Diamond v. Diehr*[3] which authorized the patent office "to issue patents for certain kinds of computer software" (p. 142).

The exposition of these software conflicts—especially the problems with the application of traditional patent and copyright law thereto—then proceeds through a discussion of the development of early computer spreadsheet systems and the legal protections of the "look and feel" of a software package.[4] This chapter is concluded with the posing of the pervading question, "[h]as the role of computer software become so critical to the economic health of the nation and the world that it deserves its own system of legal protection, extracting the optimum practices from existing legal regimes?" (p. 158). The implicit answer is that it has, but unfortunately no ideas for this are presented. Branscomb concludes this section with the statement that "the law may currently be adequate, but adequate may not be good enough" (p. 157).

The other issue treated in the book relating to protection of computer software is the protection and use of e-mail in both the corporate and large-scale network domains. In the case of corporate systems, it seems that a company may limit use of such systems to company related business much as they would limit photocopier usage; they may even monitor messages in order to enforce such regulations. In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA")[5]

---

3. 450 U.S. 175 (1981).

4. This discussion revolves around the litigation arising from look-alike systems modeled after Lotus Corporation's spreadsheet software system "Lotus 1-2-3." Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37 (D. Mass. 1990).

5. Title I of the ECPA is codified at 18 U.S.C. § 2510 *et seq.* (1988). Title II of the

which "ensure[s] that electronic messages on telecommunications transport and information systems offered to the public . . . receive the same protection from disclosure as voice messages" (p. 94). Note that this does not apply to internal corporate systems.[6]

Things become even more complicated with commercial e-mail network systems. Prodigy, which retains the right to review messages posted on its bulletin boards, became a target for protesters when discriminatory messages were allowed to be published on its system. Since the right of review was retained, Prodigy was seen as responsible for preventing discriminatory usage of its facilities and was held accountable by some people for not so doing. CompuServe, another commercial network system, has avoided such problems by disclaiming the right of review. Rather than being publisher or editor, CompuServe sees itself as a distributor of messages. Therefore, it is not held liable for the content of user messages on its system.[7]

These chapters, like the others, briefly chronicle a history of the law leading up to one or two captivating examples and then briefly discuss the meaning and relevance of these examples. In this sense, the book is analogous to a law school casebook which may briefly give statutory language but then attempts to flesh out the details and scope of the principal being discussed through sample cases. Unfortunately, while a casebook generally presents enough cases to provide a broad view of the issue at hand, this book presents only one or two anecdotes, and usually they speak to the central tendencies or just one side of the principle at issue. The examples neither give a broad enough view to circumscribe boundaries of the topic, nor do they identify issues which arise at the unclear boundaries.

One tends to leave this anecdotal survey with the feeling that big business is exploiting the individual by collecting, using, and abusing information at the expense of the individual's privacy interests. This tone is set in many chapters including those on the ownership of names, addresses, telephone numbers, e-mail messages, and medical histories. While these chapters do present some of the benefits afforded to the individual by business use of this information,[8] the reader is still left

---

ECPA is codified at 18 U.S.C. § 2701 *et seq.* (1988).

6. No discussion is provided of the implication that a company could also listen in on a telephone call made from a company telephone.

7. *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

8. This is done most notably in the discussion of the benefits of a centralized repository

feeling like an exploited individual and believing that Big Brother may not be all that distant. For example, the chapter on video entertainment presents the story of an electronic pirate's criminal offense against HBO,[9] and, even here, the story is told in such a way that the big cable corporation is made as much of a "bad guy" as the pirate.

Throughout the book a recurring theme is the conflict among intellectual property interests, privacy issues, and free speech. Many of these discussions are directed towards the policies and statutes that have been, or could be, applied. While occasionally some common law cases are presented as illustrations, little effort is spent outside the software chapter on the effects these decisions, their interpretations, and future decisions may have on the ownership of information. Ms. Branscomb seems to be focused on civil rather than common law and thus appears to advocate a statutory change rather than a change in interpretation of the existing corpora of traditional intellectual property and privacy law. Unfortunately, even the exact nature of such a statutory change is not explored.

Viewed from a law and economics interpretation,[10] the tensions described in the book can also be seen as a question of who should be afforded the entitlement to information and how this entitlement should be protected.[11] Is it more efficient for the individual to have control of these interests or for the corporate or governmental agency to have control? These issues are highlighted by the bipartite discussion in the chapter on medical histories. Branscomb first explores the abuses that can occur if an individual's privacy interests are violated. She then discusses the better service and overall efficiency that could be achieved by granting an entitlement to the corporate or governmental agency that could most efficiently administer such a system via a centralized repository of medical information.[12]

The list of cases and issues discussed in *Who Owns Information? From*

---

of medical information.

9. An individual interrupted the satellite signal being used by HBO and replaced it with a message of his own.

10. *See generally* A. MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND ECONOMICS (1989).

11. For a complete discussion of the granting and protection of entitlements from the law and economics point of view, see Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral* 85 HARV. L. REV. 1089 (1972).

12. Note that this approach is not taken in the text but would have been an interesting approach to the issues presented therein.

Privacy to Public Access is meant less to be comprehensive than illustrative. Likewise, the legal analysis points to the current state of affairs without providing any strong opinion of how to proceed. Sadly, the conclusion reached maintains that the First Amendment of the Constitution, intellectual property law, and privacy law are insufficient to solve the problems associated with the rise of an information-based economy. "Given the fact that these three areas of the law established themselves well before questions about the value of electronic-mediated information arose, they often say little or nothing about many of the most pressing issues regarding information as property" (p. 178). The author, too, says little or nothing about how to proceed from here.

Joshua B. Konvisser