Procedures for Collecting Viewing Choices. Policies and procedures used by companies in the collection and dissemination of private information have become commonplace, motivated in large part by the growing privacy concerns of consumers and privacy advocates. To the extent that privacy policies are intended both to inform and to reassure a company's customers, the development, implementation, and communication of those policies has become vital in ensuring the continued viability of what is broadly considered e-commerce. For these reasons, most e-commerce companies have established privacy policies and communicated those policies in public forums, most commonly on their Web sites [8]

TiVo can be considered an e-commerce company in the sense that it maintains interactive business relationships with consumers through electronic networks. As such, TiVo has in place a highly detailed, well-documented procedure that communicates its intent to keep subscribers' personal viewing choices private, and the technological steps it follows to enforce the policy [11]. Subscribers have options specifically concerning the collection and transmission of their viewing information. They can choose one of three options: Opt in—where viewing data and identifiable information is transmitted from the receiver; Opt out—where no viewing data is transmitted from the receiver; and Opt neutral—where viewing data without identifiable information is transmitted from the receiver. If subscribers do not explicitly choose to opt in, all viewing information received by TiVo's servers is automatically separated from any information that could be used to match it to individual receivers or subscribers. Account information and anonymous viewing data then are stored in separate systems. To further ensure that anonymous viewing data cannot be associated with an individual subscriber, viewing data is randomly transferred to one of a number of servers when it is stored. The file transfer logs are turned off and timestamps are erased from the data every three hours. These measures serve no purpose except to guarantee that anonymous viewing data remains anonymous.

From an advertiser's or PVR provider's perspective, the formulation of acceptable privacy policies is in opposition to the company's ability to build individual viewer profiles. Because TiVo's privacy policies do not allow it to match a viewer with his or her viewing choices, those policies, as currently written, do not allow for customized advertising. Therefore, a fundamental question is how and whether a company can formulate privacy policies that allow for individual profiling and customized advertising, while also protecting the privacy rights of its customers.

Another key issue in the formulation and implementation of privacy procedures is the level of trust the subscriber and other stakeholders have in those procedures. While auditable policies and procedures are a staple of successful online companies, the steps a profiling company, in particular, must take to engender trust is an open question. Procedures might have apparent validity, but if they are not followed correctly, they might not produce acceptable outcomes. Considering media reports of corporate malfeasance, it is not surprising that some stakeholders might not trust TiVo to behave in a manner consistent with its published policy.

Potential Outcomes from Collecting Viewing Choices. An assessment of outcomes essentially is a cost-benefit calculation. In this regard, it is difficult to assign a monetary value to privacy, primarily because different individuals tend to place different values on their privacy; those values are inherently subjective, and the level of privacy infringement is often difficult to ascertain in the short term. Nevertheless, a recent report from Forrester Research suggests that people are willing to give up some privacy in exchange for something of value, which can be represented as monetary compensation, product discounts, increased convenience, and other tangible or intangible benefits [7]. For example, companies routinely capture individual consumer purchasing transactions involving frequent shopper cards, but that has not stopped consumers from using the cards in increasing numbers. AC Nielsen reports the number of consumers participating in a frequent shopper program more than doubled between 1996 and 2003, and now 80% of all consumers participate in at least one program [4]. Assuming they recognize the privacy implications, users of such cards clearly believe the cost of losing some privacy is outweighed by the lower monetary cost of using the card.

To a prospective PVR customer, any forfeiture of privacy is an intangible cost. It is difficult not only to detect whether a privacy infringement is present—or to verify its absence—but also, as noted, to determine the magnitude of the privacy violation. There is, for example, the question of whether the loss of privacy due to explicitly provided personal information is more or less costly than the loss of privacy due to implicit monitoring of viewing behaviors. Similarly, does the lack of certainty in profiling an individual—or more precisely, the magnitude of the uncertainty—affect the magnitude of the privacy violation and therefore its perceived cost to the viewer?