CHAPTER 7 *Conclusions*

In Chapter 1, we presented a rationale for the particular agenda—personal privacy—that drove the architectural design in Chapter 2, the security issues addressed in Chapter 3, and the sample application in Chapter 4. In Chapter 5, we demonstrated that the result appears to meet its design goals without forcing privacy and functionality to be traded off against each other. Finally, in Chapter 6, we investigated some work related to this research, exploring other matchmakers, decentralized systems, and explicitly political systems. In this chapter, we shall draw some general conclusions about the work presented here.

We have demonstrated that starting from a social or political agenda can have wide-ranging effects on how technology is designed. This research has shown that carefully protecting the personal privacy of users in a broad class of applications can lead to a design which is technically superior in several respects—indeed, the decentralized nature of the design, its reliance on strong cryptography, and many other design elements seemed inevitable once the underlying agenda was chosen. The result indicates that, for a large class of potential applications, protecting privacy does not necessarily require that one make a tradeoff between privacy and either robustness or functionality.

It is hoped that the widespread availability of this research will lead to commercial and legislative chnages in several viewpoints, including

- the relation of technology to issues of personal privacy, and
- the utility of strong cryptography.

This is, after all, the fundamental goal of the research—while Yenta is an important and useful application, and while its use can serve as both an advertisement for the underlying concepts and also help solve real problems for real users, it is the architecture and the rationale for its development which are the most important issues here.

As discussed in Section 5.9, one of the enduring issues concerns getting those with financial incentives in their users' lack of privacy to adopt the technology discussed here. The Yenta application itself, by serving as an example and by raising awareness of the issues, may help in this regard. However, it is only the first step along a long but ultimately rewarding path.