Political Artifacts and Personal Privacy: The Yenta Multi-Agent Distributed Matchmaking System

by
Leonard Newton Foner

SB Electrical Engineering and Computer Science
Massachusetts Institute of Technology
June 1986

SM Media Arts and Sciences
Massachusetts Institute of Technology
June 1994

Submitted to the Program in Media Arts and Sciences,
School of Architecture and Planning,
in Partial Fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY
at the
Massachusetts Institute of Technology
June 1999

Signature of Author

Program in Media Arts and Sciences
April 30, 1999

Certified By

Pattie Maes
Associate Professor of Media Arts and Sciences
Program in Media Arts and Sciences

Accepted by

Stephen A. Benton
Chairperson
Departmental Committee on Graduate Students
Program in Media Arts and Sciences

Political Artifacts and Personal Privacy: The Yenta Multi-Agent Distributed Matchmaking System

by
Leonard Newton Foner

Submitted to the Program in Media Arts and Sciences,
School of Architecture and Planning, on April 30, 1999
in Partial Fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY
at the Massachusetts Institute of Technology

Abstract

Technology does not exist in a social vacuum. The design and patterns of use of any particular technological artifact have implications both for the direct users of the technology, and for society at large. Decisions made by technology designers and implementors thus have political implications that are often ignored. If these implications are not made a part of the design process, the resulting effects on society can be quite undesirable.

The research advanced here therefore begins with a political decision: It is almost always a greater social good to protect personal information against unauthorized disclosure than it is to allow such disclosure. This decision is expressly in conflict with those of many businesses and government entities. Starting from this premise, a multi-agent architecture was designed that uses both strong cryptography and decentralization to enable a broad class of Internet-based software applications to handle personal information in a way that is highly resistant to disclosure. Further, the design is robust in ways that can enable users to trust it more easily: They can trust it to keep private information private, and they can trust that no single entity can take the system away from them. Thus, by starting with the explicit political goal of encouraging well-placed user trust, the research described here not only makes its social choices clear, it also demonstrates certain technical advantages over more traditional approaches.

We discuss the political and technical background of this research, and explain what sorts of applications are enabled by the multi-agent architecture proposed. We then describe a representative example of this architecture---the Yenta matchmaking system. Yenta uses the coordinated interaction of large numbers of agents to form coalitions of users across the Internet who share common interests, and then enables both one-to-one and group conversations among them. It does so with a high degree of privacy, security, and robustness, without requiring its users to place unwarranted trust in any single point in the system.

Thesis Supervisor: Pattie Maes
Title: Associate Professor, Program in Media Arts and Sciences

This work was supported in part by British Telecom and Telecom Italia.

Political Artifacts and Personal Privacy:
The Yenta Multi-Agent Distributed Matchmaking System

by

Leonard Newton Foner

The following people served as readers for this thesis:

Reader

Peter G. Neumann
Principal Scientist
Computer Science Lab
SRI International

Reader

Deborah Hurley
Director, Harvard Information Infrastructure Project
Kennedy School of Government
Harvard University

Reader

Henry Jenkins
Professor of Literature
Director, Film and Media Studies Program
MIT Literature Department

Acknowledgments

This work could never have happened without the support and assistance of many people.

First and foremost, I thank my advisor, Pattie Maes, for her invaluable advice and encouragement in the years we have worked together.

I also thank the rest of my committee—Peter Neumann, Deborah Hurley, and Henry Jenkins—for their attention and advice.

I am forever grateful to Lisa Kamm for her unflagging friendship and support, and for her invaluable legal and political acumen. I am also deeply indebted to Michele Evard for her friendship and encouragement, and for helping to pass on the oral tradition that is so much a part of a Media Lab dissertation.

A large number of people contributed in one way or another to the development of Yenta and its ancillary systems. I thank Brad Rhodes for his friendship, for important feedback on certain aspects of Yenta's design, and for his development of the Remembrance Agent, whose document comparison engine has been passed back and forth, rewritten, and rearranged innumerable times between us and among several of our UROPs, whom I also thank.

Barry Crabtree, of British Telecom, was enthusiastic about Yenta from the beginning, not only contributing to an early prototype, but also in arranging for gorgeous animations from simulations of Yenta's network behavior.

Undergraduates, as part of MIT's UROP program, contribute mightily to many research projects and help make MIT what it is. Daniel Barkalow and Aaron Ucko have spent untold hours doing first-rate work on Yenta's code. Without their help, Yenta may never have been finished. They have my highest commendation and my most heartfelt thanks. In addition, Sofya Raskhodnikova, Edward Kogan, Bayard Wenzel, Aditya Prabhakar, and Katie King have made important contributions to one part or another of Yenta. I thank also Abhay Saxena, Peter Davis, Brian Sniffen, and Pamela Mukerji. Tomoko Akiba created Yenta's wonderful surrealistic icons, and Maggie Oh made its logo. Ray Lee wrote an excellent original prototype for Yvette, and Ivan Nestlerode upgraded and polished it until it was ready for prime time.

I also thank the authors of SSLeay, SCM, autoconf, automake, and gcc, without which this project could not even have been contemplated.

Finally, I would like to thank the many people not already mentioned above who have reviewed copies of this manuscript and provided comments on it, including David Anderson, Judy Anderson, Marlena Erdos, and David Bridgham.