



Project Libra

Optimizing Individual
and Public Interests in
Information Technology

2 0 0 4



RAND SCIENCE AND TECHNOLOGY

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Preface

This document describes the vision for a program of research to investigate policy implications of emerging information technologies. The research would explore capabilities of future systems of wireless technologies and sensors that implement appropriate protections of privacy and civil liberties; experiment with decisionmaking processes that optimize the balance between privacy concerns and the public and personal benefits of these information technologies; and examine the mutual adaptation of attitudes, behaviors, policy, and technology that come about with experience.

Project Libra was conceived as a joint research activity of the RAND Corporation and Carnegie Mellon University. The RAND portion of this research in the public interest was supported by RAND, using discretionary funds made possible by the generosity of RAND's donors, the fees earned on client-funded research, and independent research and development (IR&D) funds provided by the Department of Defense.

This document is one of several publications that serve to archive the results of this IR&D investment, and to make these results available for subsequent discussion and further development.

Abstract

New information technologies have created unprecedented opportunities to collect, store, and transfer information in ways that make our lives both easier and safer, but the potential for these technologies to be used in ways that diminish our privacy and civil liberties is equally unprecedented. Effective decisionmaking in this domain will require many kinds of knowledge. To build this knowledge base, the RAND Corporation and Carnegie Mellon University propose an integrated, multidisciplinary research program to be conducted within a living laboratory embodying next-generation information technology on the Carnegie Mellon campus. Our goal is to inform national discussions about technical issues and policy choices associated with information technology as it relates to privacy. This paper presents our vision of this research program.

Acknowledgments

Jolene Galegher played a significant role in the preparation of this prospectus. The authors wish to acknowledge her important contributions. We also thank our many RAND and Carnegie Mellon colleagues who reviewed and provided valuable input to our research program plans at several points in their development.

Introduction

New information technologies have created unprecedented opportunities to collect, store, and transfer information in ways that make our lives both easier and safer, but the potential for these technologies to be used in ways that diminish our privacy and civil liberties—especially given heightened concerns about national security—is equally unprecedented. Difficult choices lie ahead. We will need to consider, over and over again, the relationship between the potential usefulness of information technology in protecting ourselves and its potential to violate American traditions of freedom from unwarranted surveillance.

Effective decisionmaking in this domain will require many kinds of knowledge—knowledge about individual and community preferences regarding the use of privacy-compromising technology, about the effects of particular configurations of technology on individual and group behavior, about strategies for making choices regarding the use of technology within a community, and about how technology might be adapted to serve our concerns for security while honoring our concerns about privacy.

To build this knowledge base, the RAND Corporation and Carnegie Mellon University propose an integrated, multidisciplinary research program to be conducted within a living laboratory embodying next-generation information technology on the Carnegie Mellon campus. In this environment, we will attempt to identify policymaking processes that are seen as fair within the context of a particular community, the elements of desirable policies, and the acceptability and utility of specific safety-enhancing, privacy-compromising technologies. We bring to this problem distinct, but complementary, experience in the design of advanced technology; behavioral analysis of the social impact of technology; law; and policy analysis.

Our goal is to inform national discussions about technical issues and policy choices associated with information technology as it relates to privacy. Although our primary focus is the balance of concerns about security and privacy, we believe the results of this research will also be

relevant to privacy issues that arise from commercial uses of information technology.

Identifying Rational Balance Points: Research Goals

Advanced technologies are already being used in efforts to increase public safety. They have, for instance, been used to detect violations of traffic laws, to identify criminals at public events, and to warn of terrorist activities. Given appropriate authorization, law enforcement officials are permitted to monitor telephone traffic, and it has recently been reported that they have identified previously difficult-to-track calls made from prepaid cell phones, Internet-based phone service, and prepaid phone cards to known al Qaeda locations both inside and outside our borders.

The availability of these technologies may enable government authorities to increase public safety, but they are obligated to do so without unduly compromising civil liberties. Thus, they must not only understand information technology but must also act to influence its design and deployment. The demand for increased security creates new commercial opportunities for technology developers, but taking advantage of those opportunities requires that they be not only technically proficient but also responsive to citizens' concerns about privacy. In short, the technology and policy communities must both inform and be informed by each other. Our research will provide the empirical foundation needed to facilitate communication between these domains and decisions within them.

Our agenda is driven by the idea of identifying *rational balance points* between competing interests. A rational balance point is reached when, in the eyes of the community, decisions are based on fair processes, well reasoned, and acceptable. With regard to the use of technologies that diminish individual privacy in order to protect the larger community, attaining rational balance points involves (1) developing and providing access to technology that benefits both individuals and society, (2) specifying policies that govern the use of such technologies and procedures for formulating those policies, and (3) the mutual adaptation of individual and group behavior, information technology, and policies that govern technology and its use.

To determine the properties of rational balance points and how people arrive at them, our research will focus on three topics:

- Technology capabilities that can be used to protect privacy while meeting individual and public needs
- Strategies communities can use to identify rational balance points between competing demands of individual privacy and personal and public goods
- The reciprocal adaptation of social behaviors and potentially intrusive technologies as a community gains experience with technology and policies governing their use

Research on these topics would yield important insights into community responses to privacy-compromising technology. It would also help to determine whether deliberative processes are helpful and important with regard to making choices that involve trade-offs between privacy and competing goods and, if so, what the desirable features of such deliberative processes might be. Finally, it could provide evidence about privacy concerns that might inform both the design of next-generation technologies and the development of policies governing their use.

Establishing an Information Infrastructure for Research: A Field Laboratory

We propose to create a field laboratory that would allow us to study the development and effects of technology policies, as well as community behaviors and attitudes toward technologies and technology policies. This laboratory would be established at Carnegie Mellon University, with extensions to other communities to follow.

Carnegie Mellon's information infrastructure is well integrated into campus life, offering the services of a modern, technologically sophisticated institution. We propose to extend this infrastructure to include new personal devices (PDs) and sensors. The PDs would integrate the features of multiple devices including (1) multimedia communications and entertainment, (2) identity tokens (e.g., an ID card), (3) authorization tokens (e.g., a key or swipe card), (4) location awareness, (5) biometric sensors, and (6) signaling (e.g., to authorize a transaction or

receive a notice from another component of the infrastructure). The sensors would be devices such as cameras and radio frequency ID readers. Both PDs and sensors would be fully integrated into the information infrastructure.

The proposed extensions of Carnegie Mellon's existing information infrastructure would result in an environment with services that would be appealing to many individuals. The same features, however, permit the information infrastructure to collect information about the individual and make it available to other individuals or business and governance processes. Such information can be beneficial both to individuals and the community. For instance, enhanced communication capabilities would permit people to contact each other at any time and any place, and enhanced surveillance capabilities might increase safety within the community. But the same information could be seen as intrusive and could even put individuals at risk if, for instance, knowledge of their whereabouts made them vulnerable to stalking or other forms of harassment.

This environment, then, would provide an appropriate setting in which to study alternative policy choices, the technology capabilities required to implement them, the processes for making choices, and their impact on society. We believe these technologies represent a plausible future infrastructure for America and the world.

Ethical Issues

Given its focus on the role of privacy-compromising technologies in increasing security for individuals and communities, consideration of ethical issues is essential. Such issues will include, at least, the kinds of monitoring and data collection that will be permitted and the role of particular constituencies—especially students—in decisions regarding the project. Our plans for dealing with these concerns include providing opportunities for members of the campus community to present their views as projects are formulated, both as individuals and as members of committees established for this purpose. In addition, we will appoint an external advisory board comprised of scientists, experts in law and technology policy, and privacy advocates; this board will oversee the project as a whole and will have the authority to override the decisions of

project managers. Individual projects to be carried out within the test bed must be approved by the Institutional Review Boards (IRBs) at RAND and Carnegie Mellon. These committees are required by law to ensure the rights and well-being of human subjects in research.

Project Management

This proposed research is inherently multidisciplinary, and the need for expertise in multiple domains has been taken into account in shaping the leadership team, which is made up of senior scholars in constitutional law, public policy, computer science, behavioral science, and administration of university computing systems. As is indicated in the bios that follow, project leaders are all senior scholars whose expertise has been recognized in many ways—through federal and foundation grants to support their research, chaired professorships, invitations to serve on national and international scientific committees, and appointments to administrative and policymaking posts within their institutions. As a team, we have extensive experience in large-scale technology development programs (Balkovich, Morris), the design and execution of complex behavioral research related to the use of information technology (Bikson, Kraut), the analysis and implementation of technology policy (Farber, Shane), and the development and administration of campus computing and telecommunications systems (Smith). In addition, two members of our team (Bikson, Kraut) currently serve on the IRBs at their respective institutions. This experience would enable them to provide guidance about ethical issues, but they would not, of course, be involved in institutional decisions about studies conducted under the auspices of Project Libra.

Significance

This research program is designed to generate the kinds of knowledge required to make policy decisions regarding the use of information technology to promote national security, while protecting the privacy and civil liberties of members of the community. The technological environment we envision, constructed from the next generation of

wireless devices and sensors, will provide opportunities to examine the effects of alternative technological configurations, the preferences of individuals and communities with regard to such technology, the effects of technological interventions on individual and group behavior, and the suitability of alternative procedures for making decisions about technology policy within a community.

The results of the research program described here could significantly influence national discussions about the issues, choices, and governance of information technology as it relates to privacy in American society. It should help to identify new information technology capabilities critical to implementing acceptable policies. We also anticipate this research will help to identify processes that improve public participation in the formulation of information technology policy and to educate a new generation of information technology users and developers. These outcomes would be beneficial in relation to discussions of privacy in many aspects of American life—in the use of marketing data to identify potential consumers, in the personalization of news sources, in the disclosure of medical information for diverse purposes, and in public safety—in short, in any area that might require a trade-off of privacy for a personal or social benefit.

Project Leaders

Ed Balkovich and **James Morris** have led large campus-based technology experiments: Projects Andrew (at Carnegie Mellon) and Athena (at MIT). Both of these projects became central to computer-based communication and file-sharing systems at their respective institutions. Balkovich, a senior engineer at RAND, has also pursued projects concerning the societal impacts of information and communications technology. He has held senior positions in industry and academia and has been a member of several National Research Council committees. In addition to his work on the Andrew system, Morris has conducted research on the principles of programming languages and search algorithms. He has been the principal investigator of several National Science Foundation (NSF) and DARPA projects focused on computer-mediated communication. He is currently the dean of the School of Computer Science at CMU.

Tora Bikson is a senior scientist in the Behavioral Sciences Group at RAND, where she also serves as chair of the Institutional Review Board. She has investigated factors that affect the successful incorporation of innovative technologies in both organizational and interpersonal contexts. Bikson also has extensive experience as a scientific advisor, having served as a technical consultant to the United Nations and NSF, as well as committees concerned with information technology for the National Academy of Engineering, National Academy of Sciences, National Academy of Public Administration, National Archives and Records Administration, and the Social Science Research Council.

David Farber is Professor of Computer Science and Public Policy in the School of Computer Science at Carnegie Mellon, having recently retired from the University of Pennsylvania where he was Moore Professor of Telecommunication in the School of Engineering and of Public Policy in the Wharton School. His career has focused on the understanding and development of distributed systems and networking systems. He served as the chief technologist of the Federal Communications Commission, was a member of the National Research Council's Computer Science and Telecommunications Board for more than ten years, and is currently a member of the board of trustees of the Electronic Frontier Foundation and an advisor to the Electronic Privacy Information Center and the Center for Democracy and Technology. He is a senior advisor to many companies both domestically and internationally.

Robert Kraut is the Herbert A. Simon Professor of Human-Computer Interaction at CMU. Since the mid-1980s, he has been a leader in the field of computer-supported cooperative work, a discipline that involves the development and analysis of computer and telecommunications technologies to support workgroups in various domains. His work is characterized by a cycle of needs assessment, technological design, and evaluation. He is working to understand the effect of nationwide computer networks, such as Minitel in France or the Internet in the United States, on organizational and interpersonal networks and is currently the codirector of an NSF-funded project examining everyday uses of the Internet in U.S. households. He is also a member of Carnegie Mellon's Institutional Review Board.

Peter Shane is Joseph S. Platt-Porter, Wright, Morris & Arthur Professor of Law at the Ohio State University and Distinguished Service Professor (Adjunct) of Law and Public Policy at the Heinz School of Public Policy and Management at Carnegie Mellon University. At CMU, he chairs the

advisory board of the Institute for the Study of Information Technology and Society. Professor Shane is an internationally recognized expert in constitutional and administrative law, with particular interests in the democratic uses of new information and communications technologies. He is also the principal investigator on an NSF study designed to develop and test software to facilitate online citizen deliberation regarding public policy issues.

Joel Smith is vice provost and chief information officer at CMU, where he is responsible for the strategic evolution of the university's central computing infrastructure. He oversees a division that employs approximately 150 professional and technical staff and encompasses a broad range of operational, support, and development efforts. Under his leadership, the CMU Office of Technology for Education has deployed and supported a campuswide course information system now used in about 360 courses and has provided internal seed funding and consulting for a number of technology-enhanced learning projects. He has also directed projects funded by CMU and NSF focused on the development of educational software.