

# Table of Contents

<b>Chapter 1: Introduction</b> . . . . .	<b>15</b>
1.1 The fundamental premise. . . . .	15
1.2 What's ahead? . . . . .	16
1.3 What are we protecting? . . . . .	16
1.4 The right to privacy . . . . .	19
1.5 The problems with centralized solutions . . . . .	22
1.6 Advantages of a decentralized solution . . . . .	24
1.7 A brief summary of this research. . . . .	25
1.7.1 The architecture and its sample application. . . . .	26
1.7.2 Evaluation . . . . .	26
1.8 Summary . . . . .	27
<b>Chapter 2: System Architecture</b> . . . . .	<b>29</b>
2.1 Introduction . . . . .	29
2.2 Application traits . . . . .	30
2.3 Application traits we are not considering . . . . .	31
2.4 Yenta—the sample application . . . . .	32
2.5 The overall architecture . . . . .	33
2.6 Determining one user's characteristics . . . . .	33
2.7 Bootstrapping. . . . .	34
2.8 Forming groups of users—clustering. . . . .	35
2.8.1 Data structures used in finding referrals and clusters . . . . .	35
2.8.2 Referrals and clustering . . . . .	35
2.8.3 Privacy of the information exchanged. . . . .	38
2.9 What exactly is a cluster? . . . . .	39
2.10 Using the resulting clusters . . . . .	41
2.10.1 One-to-one communication . . . . .	41
2.10.2 Broadcasting to all agents in a cluster . . . . .	41
2.10.3 Hiding identities. . . . .	42
2.11 Reputations . . . . .	43
2.12 Running multiple agents on one host. . . . .	44
2.13 Evaluation hooks . . . . .	46
2.14 Summary . . . . .	48
<b>Chapter 3: Privacy and Security</b> . . . . .	<b>49</b>
3.1 Introduction . . . . .	49
3.2 The problem. . . . .	49
3.2.1 The threat model: what attacks may we expect? . . . . .	49
3.2.2 How private is private? . . . . .	51
3.2.3 Security design desiderata . . . . .	51
3.2.4 Problems not addressed . . . . .	53

3.3	Cryptographic techniques . . . . .	54
3.3.1	Symmetric encryption . . . . .	54
3.3.2	Public-key encryption . . . . .	54
3.3.3	Cryptographic hashes . . . . .	55
3.3.4	Key distribution . . . . .	55
3.4	Structure of the solutions . . . . .	56
3.4.1	The nature of identity . . . . .	56
3.4.2	Eavesdropping . . . . .	57
3.4.3	Malicious agents . . . . .	57
3.4.4	Protecting the distribution . . . . .	57
3.5	Selected additional topics . . . . .	59
3.6	Summary . . . . .	60
<b>Chapter 4: The Sample Application: Yenta . . . . .</b>		<b>63</b>
4.1	Introduction . . . . .	63
4.2	Yenta's purpose . . . . .	63
4.3	Sample scenarios . . . . .	63
4.4	Affordances . . . . .	64
4.4.1	User interface . . . . .	64
4.4.2	Yenta runs forever . . . . .	64
4.4.3	Handles . . . . .	65
4.4.4	Determining user interests . . . . .	65
4.4.5	Messaging . . . . .	66
4.4.6	Introductions . . . . .	67
4.4.7	Reputations . . . . .	67
4.4.8	Bookmarks . . . . .	67
4.4.9	News . . . . .	67
4.4.10	Help . . . . .	68
4.4.11	Configuration . . . . .	68
4.4.12	Other operations . . . . .	68
4.5	Politics . . . . .	68
4.6	Implementation details . . . . .	69
4.6.1	The C code . . . . .	69
4.6.2	The Scheme code . . . . .	70
4.6.3	Dumping . . . . .	71
4.6.4	Architectures . . . . .	71
4.7	Determining user interests . . . . .	71
4.7.1	Producing word vectors . . . . .	71
4.7.2	Clustering . . . . .	72
4.8	Security considerations . . . . .	73
4.8.1	Encrypting connections . . . . .	73
4.8.2	Protecting persistent state . . . . .	73
4.8.3	Random numbers . . . . .	77
4.9	Summary . . . . .	77

<b>Chapter 5: Evaluation</b> . . . . .	<b>85</b>
5.1 Introduction . . . . .	85
5.2 Simulation results. . . . .	86
5.3 Collecting data from Yenta. . . . .	87
5.4 What data is collected? . . . . .	89
5.5 A sample of results. . . . .	90
5.5.1 Qualitative results . . . . .	91
5.5.2 Quantitative results . . . . .	92
5.6 Security . . . . .	93
5.7 Risk analysis . . . . .	96
5.7.1 Denial of service . . . . .	97
5.7.2 Integrity and confidentiality—protocols . . . . .	98
5.7.3 Integrity and confidentiality—spies. . . . .	99
5.7.4 Contagion. . . . .	99
5.7.5 Central servers . . . . .	100
5.7.6 Nontechnical risks . . . . .	101
5.8 Other applications of this architecture . . . . .	101
5.9 Motivating adoption of the technology . . . . .	104
5.10 Future work . . . . .	106
5.10.1 Sociological study . . . . .	106
5.10.2 Political evaluation. . . . .	106
5.11 Summary . . . . .	106
<b>Chapter 6: Related Work</b> . . . . .	<b>109</b>
6.1 Introduction . . . . .	109
6.2 Matchmakers . . . . .	109
6.3 Decentralized systems . . . . .	111
6.4 Political software and systems. . . . .	112
6.5 Summary . . . . .	114
<b>Chapter 7: Conclusions</b> . . . . .	<b>117</b>
<b>References</b> . . . . .	<b>119</b>

