

*Software agents, surveillance, and the right to privacy:
a legislative framework for agent-enabled surveillance*



Leiden University Press

SIKS dissertation series no. 2007-05

The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems

Lay-out: Anne-Marie Krens – Tekstbeeld – Oegstgeest

Leiden University Press is an imprint of Amsterdam University Press

© B.W. Schermer / Leiden University Press, 2007

ISBN 978 90 8728 021 5

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden veeelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voorzover het maken van reprografische veeelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3051, 2130 KB Hoofddorp, www.reprorecht.nl). Voor het overnemen van (een) gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (art. 16 Auteurswet 1912) kan men zich wenden tot de Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/pro).

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

Software agents, surveillance,
and the right to privacy:
a legislative framework for
agent-enabled surveillance

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 9 mei 2007
klokke 15.00 uur

door

Bart Willem Schermer

geboren te Alkmaar in 1978

Promotiecommissie:

Promotor: Prof. dr. H.J. van den Herik
Referent: Prof. dr. H. Franken
Overige leden: Prof. dr. F.M.T. Brazier (Vrije Universiteit Amsterdam)
Prof. dr. R.E. van Esch
Prof. dr. E.O. Postma (Universiteit Maastricht)
Prof. dr. A.H.J. Schmidt
Prof. mr. J.L. de Wijkerslooth

Preface

To write this thesis I used an Apple laptop computer that gave me access to a variety of cognitive tools such as a word processor, a PDF reader, and the internet. A mere twenty years ago I would not have had the benefit of these technologies, either because they did not exist, or because they were not yet ready for mass adoption. To me this illustrates how fast technology is changing our lives.

The pace at which technology is developing accelerates at an exponential rate (Kurzweil 2005). Between the development of agriculture in the Fertile Crescent and the invention of the wheel lies a period of four thousand years. Between the invention of the catapult and the invention of the cannon there is a period of two thousand years, and the period between the development of paper and the movable type printing press is a thousand years. The invention and mass adoption of technologies such as cars, airplanes, computers, and the internet all took place in the past century.

I believe that the accelerated development and the current convergence of new technologies will greatly benefit mankind. For instance, future technologies will have the potential to stop the environmental damage that threatens our planet, help to eliminate poverty, and will successfully combat the effects of old age. However, while the potential benefits of technology are considerable, the risks that flow forth from misuse and abuse are also substantial.

My primary motivation for writing this thesis is as follows: I feel that we have reached a point in time where the pace of technological development is so fast, and its potential impact on society so significant, that the introduction and subsequent use of disruptive future technologies should be subjected to a closer scrutiny than so far takes place. In my opinion society as a whole should become more aware of the policy issues surrounding new technologies.

For this thesis I have chosen to focus on specific policy issues related to artificial intelligence technology. In the summer of 1956 the Dartmouth College hosted the first conference on artificial intelligence. Now, fifty years later, the use of artificial intelligence is widespread within our society, despite the fact that artificial intelligence acting on the level of a human being has not yet been achieved.

One area in particular that can benefit from the application of artificial intelligence is surveillance. Using artificial intelligence technology for sur-

veillance purposes can increase national security and public safety. However, this also places additional power into the hands of the government. It is therefore important to give careful consideration to the ways in which governments use surveillance technologies, and how these technologies may change the balance of power within society.

The great statesman and third president of the United States, Thomas Jefferson, once said: “the price of freedom is eternal vigilance”. In this time of high technology I feel Jefferson’s statement is even more relevant. The power of technology can quickly distort the balance of power between the populace and their elected leaders, or may have other unwanted or unintended consequences. Therefore, it is essential to remain vigilant when it comes to the use of powerful new technologies for surveillance purposes. By keeping a close eye on the use of new technologies we may ensure that we reap their benefits, while avoiding possible negative effects. I hope that by writing this thesis I will have contributed to this goal.

Bart W. Schermer
Leiden, January 2007

Table of Contents

ABBREVIATIONS	XIII
1 INTRODUCTION	1
1.1 Knowledge is power	1
1.2 Technology and control	3
1.3 Agents and interfaces	4
1.4 Control and the surveillance society	6
1.4.1 Six characteristic features of the Information society	7
1.4.2 Panopticon	8
1.5 Privacy and liberty	9
1.5.1 Information retrieval from software agents	10
1.5.2 Information retrieval by software agents	11
1.6 Problem definition	11
1.6.1 Three causes	12
1.6.2 How to safeguard privacy and liberty?	13
1.6.3 The precise formulation	13
1.7 Research goals and research questions	13
1.8 Research approach	14
1.9 Thesis overview by chapter	15
2 SOFTWARE AGENTS	17
2.1 Artificial intelligence	17
2.2 Situated intelligence	19
2.3 Agency and autonomy	20
2.4 Agent characteristics	22
2.4.1 Reactive	22
2.4.2 Pro-active and goal-oriented	22
2.4.3 Deliberative	23
2.4.4 Continual	23
2.4.5 Adaptive	23
2.4.6 Communicative	24
2.4.7 Mobile	24
2.5 Agent typologies	24
2.6 Agent architectures	25
2.6.1 Reactive agents	26
2.6.2 Deliberative agents	26
2.6.3 Hybrid agents	27
2.7 Multi-agent systems	27
2.7.1 Architecture and standardisation	28

2.8	From closed to open systems	30
2.8.1	Phase I: Closed agent systems (2005-2008)	30
2.8.2	Phase II: Cross-boundary systems (2008-2012)	30
2.8.3	Phase III: Open systems (2012-2015)	31
2.8.4	Phase IV: Fully scalable systems (2015 and beyond)	31
2.9	Agent development in broader perspective	31
2.10	Legal issues on agents	32
2.10.1	Autonomy	32
2.10.2	Legal status of agents	32
2.10.3	Identification, authentication, and authorisation	33
2.10.4	Integrity	34
2.11	Provisional conclusion	34
3	SURVEILLANCE AND CONTROL	35
3.1	The two faces of surveillance	35
3.1.1	Disciplinary surveillance	36
3.1.2	Liberal surveillance	38
3.2	The surveillant assemblage	39
3.3	Electronic surveillance	40
3.4	System integration	40
3.5	Superpanopticon and panoptic sort	42
3.5.1	Superpanopticon	43
3.5.2	Panoptic sort	43
3.6	Reversal: the unseen Panopticon	44
3.7	Synoptic surveillance	45
3.8	Provisional conclusions	47
4	SURVEILLANCE AND SOFTWARE AGENTS	49
4.1	Knowledge discovery	50
4.1.1	Implementation	50
4.1.2	Current examples	53
4.1.3	Future	55
4.2	Data gathering	57
4.2.1	Implementation	58
4.2.2	Current examples	58
4.2.3	Future	59
4.3	Automated monitoring	60
4.3.1	Implementation	61
4.3.2	Current examples	61
4.3.3	Future	62
4.4	Decision support	65
4.4.1	Implementation	65
4.4.2	Current examples	66
4.4.3	Future	68
4.5	Provisional conclusion	68

5	THE RIGHT TO PRIVACY	71
5.1	Conceptions of privacy	72
5.2	Dimensions of privacy	76
5.3	The constitutional protection of privacy	77
5.3.1	International privacy legislation	78
5.3.2	The constitutional protection of privacy in the Netherlands	79
5.3.3	The constitutional protection of privacy in the United States	83
5.4	The changing face of privacy	85
5.5	Informational privacy	87
5.5.1	Fair Information Practice Principles (1973)	87
5.5.2	OECD Privacy Guidelines (1980)	88
5.5.3	Council of Europe Convention on Privacy (1981)	90
5.6	Electronic surveillance and the law	90
5.7	Criminal procedure and privacy in the Netherlands	91
5.7.1	The Data Protection Act	91
5.7.2	The Dutch Code of Criminal Procedure	91
5.7.3	Computer Crime Bill II	92
5.7.4	Special investigative powers	92
5.7.5	Wet vorderen gegevens telecommunicatie (Title IVA, section 7 CCP)	96
5.7.6	Wet bevoegdheden vorderen gegevens (Title IVA, section 8 CCP)	97
5.7.7	Police Files Act (PFA)	97
5.7.8	Special investigative powers for the investigation of terrorist activities	99
5.7.9	Data Retention Directive (2006/24/EC)	99
5.8	National security and privacy in the Netherlands	100
5.8.1	The European context	100
5.8.2	The General Intelligence and Security Service (AIVD)	101
5.9	Criminal procedure and privacy in the United States	102
5.9.1	Privacy Act of 1974	102
5.9.2	Title 18 USC, Crimes and Criminal Procedure	103
5.9.3	The Attorney General's Guidelines	104
5.9.4	The United States Patriot Act	104
5.10	National security and privacy in the United States	106
5.10.1	Title 50 USC, War and National Defense	106
5.10.2	The United States Patriot Act	107
5.10.3	Legislation concerning Terrorist Surveillance Programs	108
5.11	The different phases in an investigation	109
5.11.1	The Netherlands	110
5.11.2	The United States	111
5.12	General remarks on substantive criminal law	112
5.13	Risk justice	113
5.14	Provisional conclusion	113
6	PRIVACY AND LIBERTY	115
6.1	The conception of privacy as limit to power	115
6.2	Two concepts of liberty	117
6.2.1	The concept of negative liberty	118

6.2.2	The concept of positive liberty	120
6.3	Privacy and the two concepts of liberty	121
6.3.1	Privacy and negative liberty	121
6.3.2	Privacy and positive liberty	122
6.4	Difficulties with the right to privacy in the information society	123
6.4.1	Vagueness and context	124
6.4.2	Public versus private	125
6.4.3	The reasonable expectation of privacy	127
6.4.4	Individual right	128
6.4.5	Bad publicity	130
6.5	Provisional conclusion	131
7	PRIVACY AND LIBERTY IN THE LIGHT OF SOFTWARE AGENTS	133
7.1	Quantitative effects of agent technology	134
7.1.1	More efficient data monitoring and data gathering	134
7.1.2	More effective data exchange and data mining	135
7.1.3	System integration	137
7.1.4	Empowering surveillance operators	138
7.1.5	Replacing surveillance operators	139
7.1.6	Conclusions on quantitative effects	139
7.2	Qualitative effects of agent technology	140
7.2.1	Competence and authority	140
7.2.2	Emergent behaviour	141
7.2.3	Adaptation	141
7.2.4	Transparency and insight	142
7.2.5	Strength of agent metaphor	143
7.2.6	Conclusions on qualitative effects	143
7.3	The future development of agent-enabled surveillance	144
7.4	Provisional conclusions	145
8	THE LEGAL FRAMEWORK REVIEWED	147
8.1	The functions of the legal framework	147
8.1.1	Structuring society	148
8.1.2	Facilitating an individual's life	149
8.2	Legal issues and legislative reactions	150
8.2.1	Legal issues resulting from quantitative and qualitative effects	150
8.2.2	Legislative reactions	151
8.3	Legal issues related to quantitative effects	153
8.3.1	Efficient monitoring and data gathering	153
8.3.2	Effective data exchange and data mining	154
8.3.3	System integration	156
8.3.4	Empowering surveillance operators	157
8.3.5	Replacing surveillance operators	157
8.4	Legal issues related to qualitative effects	158
8.4.1	Legal status and qualification of investigative powers	158
8.4.2	Jurisdiction	160
8.4.3	Transparency	160

8.4.4	Use limitation	161
8.4.5	Strength of the agent metaphor	162
8.5	The legal framework evaluated	162
8.5.1	Quantitative effects	162
8.5.2	Qualitative effects	168
8.6	Provisional conclusions	169
9	AN ENHANCED LEGAL FRAMEWORK	171
9.1	General considerations	171
9.1.1	Requirements for the legal framework	172
9.1.2	The role of technology	176
9.1.3	Scale, effectiveness, and the legal framework	178
9.2	Dealing with the quantitative effects of agent-enabled surveillance	179
9.2.1	Efficient monitoring and data gathering	180
9.2.2	Effective data exchange and data mining	181
9.2.3	System integration	183
9.2.4	Empowering surveillance operators	184
9.2.5	Replacing surveillance operators	185
9.3	Dealing with the qualitative effects of agent-enabled surveillance	186
9.3.1	Legal status and qualification of investigative powers	186
9.3.2	Jurisdiction	189
9.3.3	Transparency and accountability	190
9.3.4	Use limitation	191
9.3.5	Strength of agent metaphor	194
9.4	Towards a legal framework for agent-enabled surveillance	194
9.4.1	Quantitative effects: rethinking privacy?	195
9.4.2	Qualitative effects: implementing new rules for a new technology	200
9.5	Provisional conclusions	201
10	CONCLUSIONS	203
10.1	The essence of surveillance technology	203
10.2	The essence of agent-enabled surveillance	205
10.3	The impact of agent-enabled surveillance	206
10.4	The impact of agent-enabled surveillance on the legal framework	208
10.5	The regulation of agent-enabled surveillance	210
10.6	Final conclusions	213
10.7	Suggestions for future research	215
	SUMMARY	217
	SAMENVATTING	223
	REFERENCES	231
	CURRICULUM VITAE	243

Abbreviations

ACL	Agent Communication Language
ACLU	American Civil Liberties Union
AI	Artificial Intelligence
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AmI	Ambient Intelligence
ANITA	Administrative Normative Information Transaction Agents
BDI	Belief, Desire, Intention
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCP	Dutch Code of Criminal Procedure
CCTV	Closed Circuit Television
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DDM	Distributed Data Mining
DOJ	Department of Justice
GAO	Government Accountability Office
EC	European Commission
ECHR	European Court of Human Rights / European Convention on Human Rights
EELD	Electronic Evidence and Link Discovery
FBI	Federal Bureau of Investigation
FIPA	Foundation for Intelligent Physical Agents
FISA	Foreign Intelligence Surveillance Act of 1978
FOIA	Freedom of Information Act
GPS	Global Positioning System
ICCPR	International Covenant on Civil Rights and Political Rights
ICT	Information and Communication Technology
IPv6	Internet Protocol Version 6
IRC	Internet Relay Chat
KDD	Knowledge Discovery in Databases
KQML	Knowledge Query Manipulation Language
MAS	Multi-Agent System
MID	Militaire Inlichtingen Dienst
MOUT	Military Operations in Urban Terrain
NCCUSL	National Conference of Commissioners on Uniform State Laws
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
PDF	Portable Document Format
PETs	Privacy Enhancing Technologies

PFA	Police Files Act
RFID	Radio Frequency Identification
TIA(O)	Total Information Awareness (Office)
TSP	Terrorist Surveillance Program
UDHR	Universal Declaration of Human Rights
UETA	Uniform Electronic Transactions Act
USC	United States Code
WIV	Wet op de Inlichtingen en Veiligheidsdiensten