

Tilburg University

Digital Anonymity and the Law. Tensions and Dimensions

Nicoll, C.; Prins, J.E.J.; van Dellen, M.J.M.

Publication date:
2003

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):

Nicoll, C., Prins, J. E. J., & van Dellen, M. J. M. (Eds.) (2003). *Digital Anonymity and the Law. Tensions and Dimensions*. (Information Technology & Law Series; No. 2). T.M.C. Asser Press.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

DIGITAL ANONYMITY AND THE LAW

Tensions and Dimensions

Series Editors

Aernout H.J. Schmidt, *Editor-in-Chief*
Center for eLaw@Leiden, Leiden University

Berry J. Bonenkamp, *Managing Editor*
NWO/ITeR, The Hague

Philip E. van Tongeren, *Publishing Editor*
T·M·C·ASSER PRESS, The Hague

For other titles in the Series see p. 000

INFORMATION TECHNOLOGY & LAW SERIES (2)

DIGITAL ANONYMITY AND THE LAW
Tensions and Dimensions

edited by

C. Nicoll
J.E.J. Prins
M.J.M. van Dellen

T•M•C•ASSER PRESS
The Hague

The *Information Technology & Law Series* is published
for ITeR by T·M·C·ASSER PRESS
P.O. Box 16163,2500 BD The Hague, The Netherlands

The *Information Technology & Law Series* is an initiative of ITeR, the National Programme for Information Technology and Law, which is a research programme set up by the Dutch government and the Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 ITeR has published all of its research results in its own book series. In 2002 *ITeR* launched the present internationally orientated and English language *Information Technology & Law Series*. This series deals with the implications of information technology for legal systems and institutions. It is not restricted to publishing ITeR's research results. Hence, authors are invited and encouraged to submit their manuscripts for inclusion. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office

NWO/ITeR
P.O. Box 93461
2509 AL The Hague, The Netherlands
Tel. +31(0)70-3440950; Fax +31(0)70-3832841
E-mail: iter@nwo.nl
Website: www.nwo.nl/iter

Single Copies and Standing Orders

The books in the *Information Technology & Law Series* can either be purchased as single copies at the regular retail price or through a standing order at a discount. Orders and standing orders can be sent to either of the distributing addresses at the top of this page.

ISBN 90-6704-156-4

ISSN 1570-2782

All rights reserved.

© 2003, ITeR, The Hague, and the authors

No part of the material protected by this copyright notice may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

Lay-out and cover: Oasis Productions, Nieuwerkerk a/d IJssel, The Netherlands

Printing and binding: Koninklijke Wöhrmann BV, Zutphen, The Netherlands ?

PREFACE

The right to anonymous exchange of information as well as anonymous communication is in an odd state of paradox. While the formal legal protection of this right appears at an all-time high, developments in both the public and private sector show a growing number of legal and especially technical means to undermine anonymity. The growing interest of people in using the Internet has had a key impact on the worldwide availability of personal information. Everyday life is evidence that technological advance provides numerous opportunities to trace and track people down. They fuel the commercial interests of persons and organisations who seek to know exactly who is accessing certain digital content in order to be able to charge for it. The pressure on anonymous communication has grown substantially after the 2001 terrorist attack on the World Trade Center and the subsequent new political climate. Although it is still difficult to oversee their exact implications, measures such as the US Patriot Act, the European Cybercrime Convention and the European Union rules on data retention may perhaps be only the very first signs that the exercise of the right to the anonymous exchange of information is under substantial pressure.

These and other developments have fuelled the dialogue on the beliefs and values behind anonymous communication. Debates rage about how, by whom, and to what extent cyberspace anonymity should be controlled, for technological advance not only provides for new opportunities to trace and track people down. The possibilities for anonymous communication are enhanced by new technologies as well. Different techniques and services have been developed which make Internet activities, such as surfing, anonymous. Facilities are also available to provide individuals with a pseudo-identity. Thus, anonymous communication raises various questions, among them legal questions. What exactly do we mean by anonymity? Why would people want to communicate and transact on an anonymous basis? What are the practical and legal restraints upon anonymity when communicating and transacting with others? Where does one draw the line between anonymity as a tool, on the one hand, for citizens to protect their civil and constitutional rights, privacy and other interests and, on the other, identification as an instrument in criminal investigation, commercial marketing, social control, etc. And, aside from the ad-hoc problems that now arise under private law, criminal law, privacy law and procedural law, what is the larger landscape of the legal consequences of anonymity?

This book starts from the position that the concept of anonymity is increasingly invoked in the information society debate. The authors of the various chapters in this book give appeals to anonymity a distinct meaning by analysing ano-

nymity from various different angles, interests, responsibilities and developments. With the culmination of these reflections, the book aims to gain a further insight into and an understanding of the concept of anonymity.

Before embarking on the analysis, we wish to thank a few people. The reflections on the concept of anonymity began to concern us some seven years ago. On the basis of our first deliberations we organized, in September 2000, an international workshop, subsidized by the Globus Institute of Tilburg University. This workshop appeared invaluable to our further understanding of the developments and we benefited enormously from the discussions and arguments which we had with the participants, among them Michael Froomkin who also contributed to this book. Whereas the focus of the first years was mainly on the constitutional rights dimension of anonymity, we decided more recently to expand the scope to broader implications and the international dimensions of the theme. Thus, we brought together an international team of experts from different backgrounds and legal traditions to reflect on other dimensions of the theme. We wish to thank them all for contributing to the discussions and this book. We also wish to thank the Dutch National Programme for Information Technology and Law (part of the Dutch Scientific Council – NWO) for making the research possible. Finally, we express our gratitude to Vivian Carter and Rachel Poels for their tremendous help with the editing of this book.

Tilburg, The Netherlands
Auckland, New Zealand
1 November 2002

MIRIAM VAN DELLEN
CHRIS NICOLL
CORIEN PRINS

TABLE OF CONTENTS

Preface		V
Abbreviations		XIII
One	Anonymity and the Law, Some Introductory Remarks	1
1.	Introduction	1
2.	The objective, scope and content of this book	3
 <i>Part I</i>		
Two	Anonymity in the Balance – A. Michael Froomkin	5
1.	Underlying Issues	6
2.	Legal Doctrine	15
3.	9/11 and Beyond	28
4.	Lobbying for Additional Protection	44
5.	Anonymity in the Balance?	45
Three	The Case of Anonymity in Western Political Philosophy. Benjamin Constant’s Refutation of Republican and Utilitarian Arguments Against Anonymity – Paul de Hert	47
1.	Introduction	47
2.	A Right to Anonymity in a Modern World	49
3.	Constant on Utilitarian Arguments Against Anonymity	75
4.	Conclusion	93
4.1	The eighteenth century: Pivotal for anonymity	93
4.2	Principes de politique: A treatise on anonymity?	96
Four	Concealing and Revealing Identity on the Internet – Chris Nicoll	99
1.	The Nature of Anonymity	99
2.	Anonymity on the Web	100
3.	The Goal of this Chapter	100
4.	How to Use the Internet Architecture to Conceal or Obscure Identity	101
5.	IP Spoofing	106
6.	Anonymous Re-mailers	108
7.	Content Anonymity	109
8.	Legal Structures that Obscure Identity	110
9.	Agency	111
10.	Trusts	114

11.	Clubs and Private Associations	115
12.	Tracing Internet Traffic	116
13.	Conclusions	119
Five	A Case Study: The JANUS Project – <i>Bernd Holznagel and Matthias Sonntag</i>	121
1.	Introduction	121
2.	Technical background	122
2.1	Communication on the WWW	122
2.2	Anonymity Services	123
2.2.1	The Anonymizer	123
2.2.2	LPWA	123
2.2.3	Crowds	123
2.2.4	Onion Routing	124
2.2.5	JANUS	124
3.	Fields of Application	126
4.	Legal Implications	127
4.1	General Requirements	127
4.2	No conflict with criminal law	128
4.3	Responsibility for illegal acts	130
4.3.1	No limitation of liability for one's own information	130
4.3.2	Limitation of liability	131
4.4	Requirements under the laws on data protection	133
5.	Outlook	135
 Part II		
Six	Market Solutions to Privacy Problems? – <i>John Deighton</i>	137
1.	Introduction	137
2.	Privacy and Identity	138
3.	Rights and Assets	139
3.1	Regulation of Privacy	140
3.2	Regulation of Identity	141
3.3	The Market in Identity	141
3.4	The Market in Privacy	143
4.	Resolution	144
5.	Conclusion	145
Seven	Anonymising Personal Data under European Law – <i>Ian Walden</i>	147
1.	Introduction	147
2.	The Anonymization Process	148
3.	Directive 95/46/EC and Statutory Interpretation	150
4.	The Nature of the Right of Privacy	152

5.	Anonymization as a Secondary Use	153
6.	Statutory Limitation	156
7.	Concluding Remarks	159
Eight	Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-line Anonymity – <i>Caroline Goemans and Jos Dumortier</i>	161
1.	Background	161
2.	The concept of “traffic data”	162
3.	Interests at stake	165
3.1	Internet Service Providers	165
3.2	Law enforcement authorities	166
3.3	Data protection advocates	167
4.	The processing of traffic data – legal framework	169
4.1	EU Data protection rules	169
4.2	Exceptions for law enforcement purposes	172
4.2.1	The principles	172
4.2.2	The case law of the European Court of Human Rights	173
5.	Possible impact on the use of on-line anonymity	179
6.	Conclusion	182
Nine	Anonymity, the Internet and Criminal Law Issues – <i>Indira Carr</i>	185
1.	Introduction	185
2.	Anonymity, the Internet and the Case For and Against	189
3.	Criminality on the Internet	195
4.	The Council of Europe and Procedural Aspects of Cybercrime Investigation	197
4.1	R 95(13)	197
4.2	The Council of Europe	204
5.	Conclusion	206
Ten	Anonymity, Consumers and the Internet: Where Everyone Knows You’re A Dog – <i>Lilian Edwards and Geraint Howells</i>	207
1.	Introduction: the opportunity and the problem	207
1.1	On-line collection of information about consumers	215
1.2	Payment-related information collection	219
1.3	Pros and cons for the consumer of disclosing personal information	219
1.4	Forms of regulation: markets, social norms, laws and “code”	222
1.5	Markets	224
1.6	Norms	228
1.7	Law	233
2.	European laws	233
2.1	US laws	236

3.	Technology	239
4.	Conclusions	244
Eleven	New Rules for Anonymous Electronic Transactions? An exploration of the private law implications of digital anonymity – <i>Jan Grijpink and Corien Prins</i>	249
1.	Background	249
2.	Anonymity: a question of degree	251
3.	The technical feasibility and social significance of anonymity	254
4.	The Legal Implications of Absolute Anonymity under Private Law	255
4.1	Absolute anonymity under contract law	256
4.1.1	The Formation of an Absolutely Anonymous Electronic Contract	257
4.1.2	The Implementation of an Absolutely Anonymous Contract	258
4.2	Absolute anonymity under the law of property	259
5.	Semi-anonymity	260
5.1	Semi-anonymity under contract law	261
5.1.1	Semi-anonymous contracts	261
5.1.2	Problems concerning the implementation of the semi-anonymous contract	262
5.2	Semi-anonymity under property law	263
6.	Are New Legal Structures for Digital Anonymity Desirable?	264
6.1	Legal culture: the choice between prevention or damage control	264
6.2	The function of the law: the choice between legislation or self- regulation	265
6.3	Developing new rules: the choice between renovation or building from scratch	266
7.	Conclusion	267
Twelve	Court Assisted Means Of Revealing Identity On The Internet – <i>Alexandra Sims</i>	271
1.	Introduction	271
2.	Criteria	276
3.	Timing	279
4.	The Scope of Accessible Information	280
5.	Conclusion	284
Thirteen	Anonymity: Challenges for Politics and Law – <i>Chris Nicoll and Corien Prins</i>	287
1.	The Concept of Anonymity	287
2.	Anonymity and Privacy	289
3.	Anonymity and Contracting	290
4.	Tensions	291
5.	Striking a balance	293

6.	The Future	295
	About the authors	299
	Index	303

ABBREVIATIONS

ACLU	American Civil Liberties Union
ADACS	Activities for the Development and Consolidation of Democratic Stability
Alb. L.J. Sci. & Tech.	Albany Law Journal of Science & Technology
All ER	All England Law Reports
AOL	America Online
ARP	Address Resolution Protocol
ASs	Autonomous Systems
ATCS	Anti-Terrorism, Crime and Security Act
BBS	Bulletin Board Systems
BDSG	Bundesdatenschutzgesetz
B.U.L. Rev.	Boston University Law Review
CCTV	Closed Circuit Television
CIA	Central Intelligence Agency
CIDR	Classless interdomain routing
CLF	Common logfile format
Comp. & Internet	The Computer and Internet
Colum. L. Rev.	Columbia Law Review
Conn. L. Rev.	Connecticut Law Review
Cornell L. Rev.	Cornell Law Review
DARPA	The Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DMCA	Digital Millennium Copyright Act
DP	Data protection
DRM	Digital Rights Management
DTI	Department of Trade and Industry
DuD	Datenschutz und Datensicherheit
ECHR	European Convention on Human Rights
EPIC	Electronic Privacy Information Center
Euro ISPA	European Internet Service Providers Association
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
Fed. Comm. L. J.	Federal Communications Law Journal
FIPs	Fair Information Principles
Fla. L. Rev.	Florida Law Review
Fordham Intell. Prop. Media & Ent. L.J. Journal	Fordham Intellectual Property Media & Entertainment Law Journal
FTC	Federal Trade Commission
FTP	File Transfer Protocol
GUID	Globally-unique identifiers
Harv. L. Rev.	Harvard Law Review
Hastings L.J.	Hastings Law Journal
HTTP	Hypertext Transfer Protocol
ICRI	Interdisciplinary Centre for Law & Information Technology
IEEE	Institute of Electrical and Electronics Engineers, Inc.

Inf. Comm. Tech. Law	Information and Communications Technology Law
Int. Rev. Law Comps and Tech	International Review of Law, Computers & Technology
IP	Internet Protocol
IRS	International Revenue Service
ISPA	Internet Service Providers Association
ISP	Internet Service Provider
IT	Information Technology
IWF	Internet Watch Foundation
J. Computer & Information L.	Journal of Computer & Information Law
JILT	Journal of Information Law & Technology
JZ	Juristen Zeitung
LINX	London Internet Exchange
LPWA	Lucent Personalized Web Assistant
Mich. Telecomm. & Tech. L. Rev.	Michigan Telecommunications and Technology Law Review
MMR-Beil.	MultiMedia und Recht
MPAA	Motion Picture Association of America
NAACP	The National Association for the Advancement of Colored People
NAT	Network Address Translation
NCC	National Consumer Council
NIC	Network Interface Card
N. Cal. L. Rev.	North Carolina Law Review
NJ	Nederlandse Jurisprudentie
NJW	Neue Juristische Wochenschrift
N. M. L. Rev.	New Mexico Law Review
Nw. U.L. Rev.	Northwestern University Law Review
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal of the European Union
OSP	Online Service Provider
PEM	Privacy Enhancing Medium
Pepp. L. Rev.	Pepperdine Law Review
PET	Privacy-Enhancing Technology
PGP	Pretty Good Privacy
PICS	Platform for Internet Content Selection
PSP	privacy service provider
QB	Law Reports Queen's Bench Division
RIAA	Recording Industry Association of America
RICO	The Racketeer Influenced and Corrupt Organizations Act
RIP	Regulation of Investigatory Powers
Seattle University L. Rev.	Seattle University Law Review
SLAPP	Strategic litigation against public participation
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
Stan. L. Rev.	Stanford Law Review
TDDSG	Teledienstschutzgesetz
TLS	Transport Layer Security
T.M. Cooley L. Rev.	Thomas M. Cooley Law Review
TTP	Trusted Third Party
Tul. L. Rev.	Tulane Law Review
U. Chi. L. Rev.	The University of Chicago Law Review
UNCITRAL	United Nations Commission on International Trade Law
U. Penn. L. Rev.	University of Pennsylvania Law Review
U. Pitt. L. Rev.	University of Pittsburgh Law Review

U. Pitt. J. L. & Com.	University of Pittsburgh Journal of Law and Commerce
URL	Uniform Resource Locator
Va. J.L. & Tech.	Virginia Journal of Law and Technology
Wall St. J.	The Wall Street Journal
Wash. L. Rev.	Washington Law Review
Wash. U. L.Q.	Washington University Law Quarterly
WTO	World Trade Organization
Yale L.J.	The Yale Law Journal
WWW	World Wide Web