

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](#)

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.

Chapter 1

ANONYMITY AND THE LAW, SOME INTRODUCTORY REMARKS

1. INTRODUCTION

This book concerns a concept which is sometimes referred to as a cornerstone of our democratic society: anonymity. With the advent of cyberspace, the means and opportunities of anonymous communications have radically changed. Thus, the new environment has also fuelled dialogue on the beliefs and values behind anonymous communication. Debates rage as to how, by whom, and to what extent cyberspace anonymity should be controlled.

The majority of present-day communication in the on-line world is, however, not anonymous. The identities of those engaged in Internet communication are usually known or are easy to discover. For various reasons, people using the Internet cannot or do not want to keep their identity a secret. Also, the implementation of new technologies, such as the Internet Protocol version 6, are expected to affect various forms of communication which are truly anonymous at present.¹

Recent initiatives such as Microsoft's "Passport" and the subsequent alternative of the Liberty Alliance show a tendency towards more standardised ways to identify customers across web sites. Thus, the bulk of all communication in cyberspace reveals information about a person's identity. These and future possibilities of digitising identity-related characteristics, appear to fuel the quest for anonymous communication.

Various specific reasons underlie this quest. Most importantly, ongoing concerns of digital privacy stimulate the debates about possible ways to avoid being "profiled" on the Net and thus to communicate anonymously. Aside from communication, people are also drawn towards anonymous electronic transactions. After all, those who participate anonymously in legal transactions are no longer dependent on the question of whether those processing personal details are complying with privacy laws. The protection of privacy is being brought about via anonymity.

In addition to privacy considerations, people may wish to remain anonymous for purposes of freedom of speech. It is clear that in various parts of the world,

¹ See Courtney Macavinta, 'Internet Protocol Proposal Raises Privacy Concerns', *Cnet News.com* (14 October 1999), <<http://news.cnet.com/news/0-1005-200-852235.html>>.

people may have an interest in not being identified and thus connected to certain published views and opinions. Due to the international character of the Internet, those reasons for anonymous communications which are related to the “freedom of expression” may gain new dimensions. Also, the reasons why people would want to transact anonymously may be because they are involved in criminal activities or wish to evade the tax authorities and do not want to leave a trail of their dealings.

Finally, we note that challenges to the concept of identity, the identification processes and the identification characteristics used in the process of identification also stimulate the debate on anonymity. Identity theft is at present one of the fastest growing crimes in the United States. Thieves are able to obtain unique access or ability characteristics for identification purposes and our identity has become a vulnerable concept. In the United States an estimated 4.2 million Americans have more than one social security number and birth certificates contain so little information that almost anyone who is approximately the right age and gender can choose which one to use.²

Before the information age, a person’s identity and information relating to his or her identification seemed to be more precisely controlled. But all that has changed. The advent of the information society has vastly increased the need for identifying mechanisms and thus public availability of the relevant technologies. Names, addresses, email addresses, photographs, social security numbers, credit card numbers, etc., are freely available on the Internet and numerous identity-related characteristics are for sale.³ On the Internet, anyone has the opportunity to gain knowledge about other people.

The growing interest of consumers in using the Internet has had a key impact on the worldwide availability of personal information. The use of the new on-line facilities will only grow further. By now, identity and personal information have become essential vehicles for the materialization of electronic commerce and other applications of the Information Society. Emphasis is on user-friendliness, more efficient services support, user empowerment, user mobility and support for human interactions. The nature of the open, borderless and public communication network, where personal information can be readily transferred in digital form, results in a situation where the management of our personal data is being threatened on a large and systematic scale.

The developments described make more and more people reluctant to reveal their true identity. In combination with this, different techniques and services have recently been developed which make Internet activities, such as surfing,

² Lynn M. LoPucki, ‘Human Identification Theory and the Identity Theft Problem’, *Texas Law Review*, February 2002, p. 28.

³ See for examples ‘Web Also Revolutionizing ID Fakery’, *The Washington Post*, 19 May 2000, E1, E10.

anonymous. Facilities are also available to provide individuals with a pseudo-identity.

Hence, anonymous communication is promoted as the solution to the problem. However, anonymous communication raises various 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 constraints upon anonymity when communicating and transacting with others? Finally, aside from the ad-hoc problems that now arise under private law, criminal law, privacy law and procedural law, what is the broader landscape of the legal consequences of anonymity?

2. THE OBJECTIVE, SCOPE AND CONTENT OF THIS BOOK

This book starts from the position that the concept of anonymity is increasingly invoked in the information society debate. While some commentators consider appeals to anonymity to be little more than rhetoric and not worthy of serious consideration, the authors of the various chapters in this book give such appeals a clearer focus by analysing anonymity 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. The focus of the book is therefore on the *legal* implications of anonymity in the *on-line* world. But in the process, the following chapters make reference to related questions that were debated for the off-line world.

For a better understanding of the concept of “anonymity”, the first part of the book is devoted to the technical, historical and philosophical background. In chapter 2, Froomkin shows us that technological advance provides for numerous opportunities to trace and track people down. However, the possibilities for anonymous communication are enhanced by new technologies as well. Thus questions, dilemmas and fields of tension arise. 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 identification, on the other, as an instrument in criminal investigation, commercial marketing, social control, etc.

In chapter 3 we learn from De Hert that concerns about anonymity are not new and have to be put in a societal and political context. In reaction to advocates of social control (by means of surveillance and observation), such as Bentham and Kant, Benjamin Constant expressed himself as a great proponent of anonymity. Not only has thinking developed over the years about control as a means of making society work but the law has also been developing, in the more modern context of privacy protection. Deighton shows in chapter 6 that privacy regulation is not satisfactory. He therefore analyses whether the market itself can provide some solutions. Following up on possible institutional solutions discussed by

Deighton, Nicoll discusses the role of technology in offering solutions. In chapter 4, he provides various examples of such technologies, among them the so-called Privacy Enhancing Technologies. Holzmagel and Sonntag subsequently discuss one of the anonymity service projects, the JANUS project (chapter 5).

Having provided the background by discussing the broader perspective of anonymity in Part I, Part II focuses on various legal implications, problems and tensions surrounding anonymity in an on-line environment. The authors apply their analysis of anonymity to a range of legal domains (running from privacy law through to criminal law, private law and procedural law).

The discussion starts with problems that relate to data protection law. In chapter 7 Walden elaborates on the first stage of making personal data anonymous (the process of anonymization) and analyses the legal status of this in the public health context. The next question in relation to data protection is addressed by Goemans and Dumortier in chapter 8 where they analyse recent legal initiatives on the retention of traffic data, particularly with respect to criminal investigation.

The debate on analysing and archiving traffic data is followed in chapter 9 by a broad analysis by Carr on criminal law issues in relation to anonymity. In discussing these issues she elaborates, among other things, on the 2001 Cybercrime Convention of the Council of Europe.

The book then turns to issues of and implications under private law. Edwards and Howells discuss consumer protection (chapter 10). Grijpink and Prins focus on issues that relate to anonymous transactions under private law (chapter 11). Finally, Sims explains court procedures and remedies to reveal identity for the purpose of legal proceedings (chapter 12). The final chapter of the book (chapter 13) by Nicoll and Prins draws tentative conclusions concerning the dimensions of anonymity, how it is differently defined depending on its context and the tensions or conflicts inherent in the approach which the law is taking and may take in the future.

November 2002

THE EDITORS