University of Oslo
Faculty of Law
Norwegian Research Center for Computers and Law

Anonymity and the Law

Candidate Number: 830006
Supervisor: Dr. Lee A. Bygrave
Delivered: 24th August 2004

Number of words: 14,653 (18,000 Max)

Table of contents

1 Introduction

Anonymity is a very powerful tool which is being used by numerous people for legitimate and non legitimate actions. It can be employed for many different reasons. It can aid in the preservation of privacy and freedom of expression, but it can also aid in criminal behavior.

Many pieces of legislation have been passed encouraging (indirectly if not directly) the use of anonymity, such as Directive 95/46/EC on data protection[1], while others seem to limit its use, as is the case with the Council of Europe Convention on Cyber Crime.[2]

Several scholars, such as Roger Clarke (a consultant and visiting fellow at the Department of Computer Science at the Australian National University) and Michael Froomkin (Professor at the Miami School of Law), have written extensively on the topic.[3]

Yet despite its topicality, much uncertainty exists about the legal or broader normative status for anonymity. The central aim of the thesis is to cast light on that status.

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/11/1995 pp. 31 – 50.* See particularly Recital 26 in the preamble to the Directive.

[2] Convention on Cyber Crime, adopted 23rd Nov. 2001, CETS No. 185. See particularly Art. 16 *et seq.* of the Convention.

[3] See further the papers accessible via <http://www.anu.edu.au/people/Roger.Clarke/BioData.html> and <http://www.law.miami.edu/facadmin/faculty/froomkin.html>.

First I look into the basic definition of anonymity together with other closely related terms like pseudonymity, identifiability, unreachability and authentication. Then I lay down the different motivations for which individuals and/or society have to be anonymous and the different motivations and interests that call for identifiability. Then I see how one can be anonymous in the real physical world and how can this be translated into the online environment.

In the last part I try to provide an overview of the main areas of law that support anonymity or require identifiability. In doing this, I focus on the approach of the United States of America (USA) in deriving an anonymity right from the right to freedom of speech set out in the First Amendment of the US Constitution. Then I explore the European approach to anonymity and the different laws in national or European Community (EC) legislation which allow for or encourage anonymous communication, or which require identifiability. Thereafter I try to see how certain data protection laws treat anonymity, my focus on this point being the provisions of Directives 95/46/EC and 2002/58/EC.[4]

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. *Official Journal L 201, 31/07/2002 pp. 37 – 47.*

2 Anonymity and other basic concepts

2.1 Introduction

In this chapter, I set out the basic definition of anonymity, as well as other definitions that help us to better understand the legal discussion that arises later.

I also lay down the different motivations for both individuals and society to be anonymous, along with the different interests that call for identification.

Finally, I look at the factual possibilities of being anonymous. How can one be anonymous in the real physical world? And how can one transport this state into the virtual online world? Can one be 100% anonymous online? Or does the online environment change our perception of what anonymity means?

2.2 Anonymity and other concepts

2.2.1 Anonymity

Anonymity is – obviously – the state of being anonymous.[5]

[5] *The Compact Oxford English Dictionary*, 2nd ed., 1998. p. 55.

Anonymous is an adjective that qualifies someone or something as "Nameless, Having no name"[6]. It derives from the Late Latin *anōnymous* and from the Greek *anōnumos (an-,* without; + *onuma,* name)[7].

The word "anonymous" can be used in different contexts, the first one being when referring to someone whose name is not given, is unknown or unacknowledged[8] or who otherwise cannot be identified[9] (*an anonymous author*). In this sense, the words "nameless", "unidentified", "unknown", "unnamed", "unavowed" and "innominate" may be viewed as synonyms for anonymous, while the words "named", "known" and "identified" as antonyms.

In another context, anonymous can refer to something which lacks individuality, distinction or recognizability[10], or which has no distinctive character or recognition factor[11] (*brown anonymous houses*). In this regard, "indistinctive", "faceless", "unrecognizable" are synonyms for anonymous while "distinctive" and "recognizable" are antonyms.

From the above, we can see a pattern telling us that anonymity entails freedom from identification, either by not being acknowledged or noticed or by lacking distinctiveness.

In the sense of being unacknowledged, the person (or thing) concerned has not been recognized or admitted as existing.[12] In the sense of lacking distinctiveness, the person (or thing) cannot be individualized to the extent that it

---

[6] *Ibid*.
[7] See <http://dictionary.reference.com/search?q=anonymous>.
[8] *The America Heritage Dictionary of English Language,* 4th ed., 2000, <http://www.bartleby.com>.
[9] See Merriam-Webster Online Dictionary, <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=anonymous>.
[10] *Ibid*.
[11] See *supra* n. 8.
[12] See <http://encarta.msn.com/dictionary_/unacknowledged.html>.

appears bland or interchangeable. And in the sense of being unnoticed, the person (or thing) seems to blend in with its surroundings. All of these senses have one common feature: the person (or thing) cannot be singularly picked out or singularly identified.[13]

If we venture further into different fields of activity we see that anonymity by and large carries the same meaning as indicated above. We see this, for example, in the medical field.[14] In the field of mathematics, however, anonymous is defined as "a term in social choice theory meaning invariance of a result under permutation of voters".[15] In legal dictionaries, the term anonymous is not defined but when we look further into more specific areas definitions are given of some terms that are closely related to anonymity. For instance, the term "anonymizer" is defined as "Remove the personal identity from a record, communication or transaction".[16] However, the definition of *anonymous refunder* ("In computer fraud a person who moves money from one account to another outside the usual methods")[17] omits mention of identifiability or lack of it.

---

[13] See section 2.2.3 for the definition of identified.

[14] For instance, I found the word *anonyma* which is defined as "without name; a term formerly applied to the large vessels in the thorax (now called the brachiocephalic trunk and vein) and the hip bone." This term refers me to the term *innominate* which is defined as: "having no name; unnamed: as, an innominate person or place." This word derives from the Latin *Innonimatus* (*in*- not + *Nominare* to name). Also in medical dictionaries we find the word *anonymize* which is defined as: "Made anonymous, esp. by the removal of names or indetifying particulars: *spec.* designating a form of medical screening, performed chiefly for statistical purpose, in which the identities of the subject are unknown to the investigator." And finally, the terms *anonyms and pseudonyms,* which are defined together as "designation for persons whose name are not known or wish to remain anonymous (anonyms) and for persons who wish to conceal or obscure their identity by assuming a fictitious name (pseudonyms)". For all these definitions, see *On-line Medical Dictionary*, <http://cancerweb.nlc.ac.uk/cgi-bin/omd?anonyms+and+pseudonyms>.

[15] Weisstein, Eric W. "Anonymous", in *MathWorld – A Wolfram Web Resource*, at <http://mathworld.wolfram.com/Anonymous.htm>.

[16] Sookman, Barry B. *Computer, internet and electronic commerce terms: judicial, legislative and technical definitions*, Carswell, Toronto, 2001.

[17] Longley, Dennis, *Data & computer security: dictionary of standards, concepts and terms* McMillian, UK, 1987.

In the fields of computer science and informatics, anonymous is defined as follows: "the condition of having an identity that is unknown or concealed. To hide an entity's real name, an alias may be used. In some applications, anonymous entities may be completely untraceable".[18] According to Roger Clarke, "an anonymous record or transaction is one whose data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data".[19] A definition for *anonymous login* is: "an access control feature (or weakness) in many Internet hosts that enable users to gain access to general-purpose or public services and resources on a host (such as allowing any user to transfer data using ftp) without having a pre-established, user-specific account (i.e., user name and secret password)".[20]

With respect to the online world, the term anonymous is defined as "remaining unknown to the extent that you have not voluntarily identified yourself."[21] And in the *Hackers Lexicon* we find the following definition: "Anonymity is one of the 'holy grails' of hacking. The idea is that a human being can use a system or send messages while protecting their identity from being disclosed".[22]

---

[18] Slade, Rob, *Glossary of Communications, Computer, Data, and Information Security Terms*, <http://sun.soci.niu.edu/~rslade/secgloss.htm#anonymous>.
[19] Clarke, Roger A. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1999. at <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.
[20] See Slade, *op cit.*, <http://sun.soci.niu.edu/~rslade/secgloss.htm#anonymous+login>.
[21] See <http://www.netlingo.com/lookup.cfm?term=anonymous>.
[22] See <http://www.robertgraham.com/pubs/hacking-dict.html#anonymous>.

2.2.2 Pseudonymity

Pseudonymity is very closely related to anonymity. It is the character or condition of being pseudonymous; the use of a pseudonym or assumed name.[23]

A pseudonym is a fictitious name.[24] It derives from the French *pseudonyme* and from the Greek *pseudOnymos* (pseudo= false, deceptive + onyma= name), meaning bearing a false name.

The pseudonym sometimes called allonym is a name, sometimes legally adopted and other times purely fictitious, used by an individual as an alternative identity. It is used when the person performs a particular role. When used by authors it is referred to as *Pen Name* (or *Nom de Plume* in French). When used by actors it is referred to as *Stage Name* or *Screen Name*.

In the internet environment, pseudonymity can be used in the form of aliases, handles or avatars [25] to use as identifiers. For hackers, "pseudonymity is essentially a weaker form of anonymity. You can commit actions that are tied to your pseudonym, but not to your physical presence".[26]

Pseudonymity is seen as the ability to prove a consistent identity without revealing the real self. It is a state which combines many of the advantages of having a known identity with the advantages of not revealing one's real identity, thus being anonymous. The main difference between anonymity and

---

[23] *The Compact Oxford English Dictionary*, 2nd ed., 1998, p. 751.
[24] *Merriam-Webster Online Dictionary*, <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=pseudonym>.
[25] "An avatar is a "digital actor" or icon that represents who you are and where you are in the virtual world. 3-D chat rooms and VRML worlds are examples of places where you would use an avatar to navigate your surroundings and communicate with other users. The avatar can be whatever you want, including a cartoon, an animal, or any graphical element. Just be aware that this image represents you." See <http://www.netlingo.com/lookup.cfm?term=avatar>.
[26] See <http://www.robertgraham.com/pubs/hacking-dict.html#pseudonymity>.

pseudonymity is that while in anonymity the identity is not known and the person tends thus to be impossible or very difficult to target or reach, there exists with pseudonymity a separate persistent "virtual" identity. Therefore, a pseudonym can obtain a response and be identified in different contexts without the person behind it having to reveal his/her real identity.

2.2.3 Identifiability

Identification is the determination of identity; the action or process of determining what a thing is; the recognition of a thing as being what it is.[27] Often the term is used as shorthand for a document (e.g. passport) or mark (e.g. tattoo) that serves to identify a person.

To identify is to determine or establish the identity of someone or something; to ascertain or establish what a given thing or given person is.

Identity is the sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not someone or something else. It derives from middle French *identité,* and from Late Latin *identitat-, identitas,* which derives in turn probably from the Latin term *identidem* meaning repeatedly, a contraction of *idem et idem,* meaning same and same.[28]

In psychology, "personal identity" is defined as the condition or fact of remaining the same person through various facets of existence[29]. People can have

[27] *The Compact Oxford English Dictionary*, 2nd ed., 1998. p. 810.
[28] See <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=identity>.
[29] See <http://wl.middlebury.edu/express/stories/storyReader$22> (Paragraph 2.a).

different identities depending on the environment in which they are acting. Thus, a person can have a particular identity in the online environment which enables him/her to adopt a roll he/she does not have when acting in the offline physical world.

In the field of art, identity is defined as "the characteristics by which a thing (e.g. a product, event, fictional character, concept), a person, or a people (a company, government, or other organization) is definitively known -- as any of these might be identified by a name, signature, sign, symbol, portrait, monogram, flag, heraldic crest, seal, logo, trademark, etc. "Identity" refers to individuality in some ways, and sameness (identical) in others."[30]

In this analysis, identifiability can be seen as the exact opposite of anonymity.

2.2.4 Unreachability

Someone who is unreachable is – obviously – someone who is inaccessible or not contactable.

After looking at the notions of anonymity and identifiability, it can be seen that the lack of identity of a person will tend to render that person difficult or impossible to reach. Therefore, unreachable may be seen as a trait of anonymity. Yet it will not always be so. I can be walking anonymously on the street and still be attacked by a random person who doesn't my name or any other identity trait. Nonetheless, while anonymity does not guarantee unreachability, it can make it

[30] See <http://www.artlex.com/ArtLex/I.html>.

more difficult to be located or even reached. This issue will be discussed in greater length when we take a look at the factual possibility of being anonymous.

2.2.5 Authentication

Authentication is the process of proving that something or someone is real, true, or what people say it/he/she is,[31] thus not false or a copy. The goal of authentication is to confirm the identification of an individual, message, file, or other data.[32]

Authentication is the verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a paper letter. Authentication will identify who an individual is; authorization will identify what the individual is allowed to do.[33]

Authentication goes further than just establishing who a person is in relation to others, like identifying does. It verifies who that person is. This can be achieved by something the person is (like a finger print or dental record), possesses (like an id card) or knows (like a password or pin).

The two primary areas of authentication are user authentication, proving that someone is who they say they are, and message authentication, proving that

[31] See <http://dictionary.cambridge.org/define.asp?key=4934&dict=CALD>.
[32] See <http://www.robertgraham.com/pubs/hacking-dict.html#authentication>.
[33] See <http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?authentication>.

orders were not forged or corrupted. The antonym of authentication is falsification or forgery.

2.3 Motivations for being anonymous

2.3.1 Overview

Anonymity is a relative state of being. It depends on the context in which one is acting and the people to whom one is relating.[34] Further, one can be anonymous without necessarily choosing to be. For example, while roaming in the street of a foreign country I may not choose to be anonymous; I am so simply because no one around me happens to know my identity. In that particular situation I have blended in with the crowd without being especially distinctive to others. But it is also important to note that I may be anonymous in this situation because others choose not to inquire about my identity, possibly out of respect for my privacy and integrity.

In many others situations, people can actively choose to be anonymous and those are the situations that are interesting within the scope of this work.

In this section, I lay down the different motivations people have to be anonymous and why anonymity is good or bad for society. I also lay down the motivations for identifiability and the positive or negative role it plays in society.

[34] See further the comments of Chris Nicolls, cited *infra*,section 2.4.2.

2.3.2 Why people want to be anonymous

As it has been defined, anonymity is the lack of identification.[35] Obviously we can assume that the main reason people want to be anonymous is because they don't want to be identified. Then the question becomes: why don't people want to reveal their identity?

When desiring anonymity, you are trying not to reveal your identity, you want people not interfere with your actions, you want to be left alone, you want privacy.

Most people probably believe that they have a right to be anonymous because it helps them protect their right to privacy. They probably believe in turn that the latter right is fundamental. Certainly, the right to privacy is protected by many treaties and conventions, the most important being the Universal Declaration of Human Rights of 1948 which states in Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[36]

Anonymity is also often regarded as being of key importance for freedom of expression. This right is also protected by many treaties and conventions, including the Universal Declaration of Human Rights.[37]

---

[35] See Section 2.2.1 for the definition of anonymity.
[36] Universal Declaration of Human Rights, available at <http://www.un.org/Overview/rights.html>.
[37] *Ibid*, Art. 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

There are many other reasons why people don't want to reveal their identity, ranging from privacy matters to criminal behaviors.

Here I lay down some of the positive and negative aspects of anonymity while comparing them with the traits of identifiability.

2.3.2.1 Positive aspects of anonymity

Anonymity helps to facilitate the flow of information and communication on public issues; this is part of the idea that "if you kill the messenger you won't hear the bad news".[38] Not everyone is brave enough as to let everybody know what they say and these people need to be encouraged to say what they have to say.[39] Some pertinent examples hot lines for reporting problems and violations, witnesses who appear in Parliamentary or Congressional hearings or in investigative media reports and who are only visible behind a screen and/or whose voice is distorted, unsigned or pseudonymous political communications.

Anonymity also helps to obtain personal information for research in which persons are assumed not to want to give publicly known answers or data. This may often be the case in studies of sexual and criminal behavior or in other social research.

---

[38] Marx, Gary. *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research* In J. Caplan and J. Torpey, *Documenting Individual Identity*. Princeton University Press, 2001. at <http://web.mit.edu/gtmarx/www/identity.html>.

[39] A. Michael Froomkin. *Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases.* 15 U. Pittsburgh Journal of Law & Commerce 395, 1996. at <http://www.law.miami.edu/froomkin/articles/ocean.htm>.

Anonymity encourages attention to the content of a message or behavior rather than who the messenger is. Thus, anonymity can be useful for a well respected person writing in a different area who may want to avoid being stereotyped or having their reputations affected or not taken seriously (e.g. a religious leader who writes about his/her doubts about religion). On the other hand, advocates of identifiability would argue that identity helps in creating a better understanding about the motivations for such writing and aids the credibility of the author.

Anonymity also encourages reporting, information seeking, communicating, sharing and self-help for conditions which are branded as disgraceful and/or which can put the person at a disadvantage or are simply very personal. In this category we can find self-help requests and discussion and support groups for alcohol (like Alcoholics Anonymous), drug, and family abuse, sexual identity, mental and physical illness, and tests for AIDS and other socially transmitted sexual diseases, also for pregnancy. Anonymity may also facilitate sociability experiences among persons who are shy or uncomfortable to interact face to face. Posting personal information such as course grades in a public place using student ID numbers rather than personal names also helps to increase the likelihood that judgments and decision making will be carried out according to designated standards and not personal characteristics deemed to be irrelevant.

In a group support system study, conclusions were drawn that anonymity helps to let participants express themselves more freely and openly and to submit

ideas that might be socially risky, without the fear of repression from other members of the group.[40]

Anonymity helps to obtain a resource or encourage a condition using means that involve illegality or are morally not accepted, but in which the consequence can be good for society. Some examples of these can be a program that exchanges guns for toys and needle exchange programs for drug addicts.

Anonymity also helps "those taking action seen as necessary but unpopular from subsequent obligations, demands, labeling, entanglements or retribution. Like sperm and egg donors or birth parents giving a child up for adoption. Also hiding the identity of judges of competitions and in courts to protect them from inappropriate influence, whether persuasion, coercion or bribes, and retribution."[41]

Further, anonymity can help to protect strategic economic interests. For example, someone with their mind set on a residential development project may be buying small portions of land under an assumed name, either because they have not announced the project or because they don't want to influence the price of the land. Also a company in financial difficulty may attempt to sell goods or services under another name to avoid letting customers know how desperate it is to sell. In auctions, bidders are identified by a number and in many cases it may not be known who the person holding the number represents. Also a person buying goods may want to remain anonymous to avoid further targeting and/or offers from marketing strategies. Those in favor of identifiability may argue that the information gathered in those marketing programs are good not only for the

[40] Martinez, Isabel Ma. *Efectos del anonimato en la comunicacion de grupos que utilizan tecnologias asistidas por odernador. Un estudio Cuantitativo y cuaitativo.* Anales de psicologia, Vol. 17, no. 1, Junio 2001, pp. 121–128 (This is my own translation).

[41] See Marx, *op. cit.*

economic effect they can have, but also for the well being of the consumers. A good example where the information could have been used in favor of the consumer could be the case of QFC, a grocery store in the Washington State, where they have a purchase card which can track the shopping habits of the consumers. Now the store is being sued because they neglected to notify a consumer about the potentially mad-cow tainted meat some consumers bought. The lawsuit claims that the purchase card system could have been used to warn those who bought the allegedly tainted meat.[42]

Another argument in favor of identifiability in business transactions can be that it also "guarantees interactions that are distanced or mediated by time and space."[43] For example, in the case with ordering by credit card an address is frequently needed to deliver goods or to handle complaints and disputes. Identifiability is also beneficial because it aids efficiency and improves service. We can see an example of this in the anecdote Gary Marx tells when he went to a restaurant he had not been to for six months and the waiter looking into a handheld computer asked: "Would you like the salmon you had last time?" [44]

Anonymity also helps people to avoid the compilation and analysis of personal profiles data.[45]

Another social benefit of anonymity can be to encourage experimentation and risk taking without facing large consequences, risk of failure or embarrassment. It enables a kind of cost-free test drive of alternative identities, behavior and reading material (e.g. pretending to be of a different gender, ethnicity, sexual preference, political persuasion etc., in on-line communication).

---

[42] See <http://www.hagens-berman.com/qfc_mad_cow_lawsuit>
[43] See Marx, *op. cit.*
[44] *Ibid*
[45] See Froomkin, *op. cit.*

2.3.2.2 Negative aspects of anonymity

With the benefits of anonymity come also disadvantages. Extreme abuse, illegal and antisocial behavior are the most notable drawbacks of anonymity.[46] However, only a small group of people who use anonymity are sociopaths and/or are primarily attracted by the ease with which they can avoid responsibility and accountability for their actions.[47] At the same time, though, the border between illegal and legal but offensive and/or antisocial use is not always very distinct, and varies depending on the law in each country.

Many people who are against anonymity argue that it is dishonorable because it eliminates accountability.[48] This is one of the strongest arguments against anonymity. As Gary Marx expresses: "It is more difficult to do ill to others when we know who they are and must face the possibility of confronting them. Mutual revelation is a sign of good faith which makes it easier to trust (not unlike the handshake whose origin reportedly was to show that one was not carrying a weapon)."[49] Others close their eyes to anonymous communication because they feel that anonymous messages lack credibility on account of the authors not daring to reveal their identity.

Anonymity can be used to protect a criminal performing many different crimes, for example distribution of child pornography, illegal threats, racial agitation, fraud, intentional damage such as distribution of computer viruses, etc.

---

[46] Rigby, Karina, *Anonymity on the Internet Must be Protected,* Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1995. at <http://swissnet.ai.mit.edu/6095/student-papers/fall95-papers/rigby-anonymity.html>.
[47] *Ibid.*
[48] See Froomkin, *op.cit.*
[49] See Marx, *op. cit.*

It can also be used to seek contacts for performing illegal acts, like a pedophile searching for children to abuse or a swindler searching for people to rip off.

Even when the act is not illegal, anonymity can be used for offensive or disturbing communication. For example, some people use anonymity in order to say nasty things about other people. Also to engage in conducts that may not be accepted by society, like buying gifts for a lover other than the wife or husband. Some people argue that on-line anonymous text used to inflict abuse or hurt is especially bad because "people are more likely to believe things that they see in print, as opposed to something they hear in an anonymous phone call or conversation."[50]

As opposed to anonymity, identifiability is valuable to aid in accountability. Because individuals generally want others to think well of them and/or to avoid negative reactions, people often behave better when they know that others know who they are. Recognition of this dynamic can be found in the anti-mask laws of some states in the USA adopted as a strategy for countering the Klu Klux Klan.

Identifiability helps also to judge reputation and determine bureaucratic eligibility (e.g. to vote, drive a car, fix the sink, cut hair, do surgery, work with children, collect benefits, etc.).

[50] See Rigby, *op. cit.*

2.4 Factual Possibility of Anonymity

Now that we know why people want to be anonymous or identified, I turn to the issue of which situations it is possible to be anonymous.

How can we achieve or maintain anonymity in the real world? Do the same factors apply with respect to online communication? These are two of the questions I attempt to answer in this section.

2.4.1 Anonymity in the Physical World

In the physical world, anonymity is taken for granted. We act in many anonymous ways without even acknowledging this. For example, when we make a cash purchase we have usually not revealed our identity to the clerk that receives the cash, nor has the clerk asked for our name or other identifying particulars. In other business transactions, you may often use the services of an agent to negotiate the terms of a contract without revealing your identity.

It is very easy to become anonymous. You simply can write a letter and not sign it, or sign it with a pseudonym. This type of anonymity is not 100% fool proof, but the ways and means of tracking down the writer of an anonymous letter are not very easy and are not normally used unless the effect of the letter is damaging (as was the case, for example, with the manifesto issued by the

Unabomber – a document that was analyzed minutely by the FBI enabling them to narrow down their search and later identify the writer[51]).

Another common and easy state of anonymity is when we are in public places and blend in with the crowd. Most people won't know who we are and most of the time won't even care as long as we don't cause any harm. In this kind of scenario if a person wants to make sure their anonymity is not compromised they may use different resources to ensure that. For example they may use dark sunglasses to avoid being recognized, or they might use gloves to not leave fingerprints behind.

Another tool that can help someone attain anonymity is the telephone. It is very easy to grab a telephone and call someone and make an anonymous threat or report a crime. Nowadays this is being challenged by "caller id" mechanisms, but there are still public pay phones where one can achieve this. Even in the wireless networks, where the traceability of a cellular phone is very accurate to the point where the exact location of the phone can be determined, there have been countries (e.g. Norway) where one has been able to activate a cellular phone with the purchase of a prepaid calling card, and the purchase of that card has not required the disclosure of any kind of identity pointer of the user. In Norway, this situation has recently changed as new legal provisions require that all telecommunications service providers must keep a record over all their end users.[52]

[51] See Froomkin, *op. cit.*
[52] See paragraph 6-2 in the Regulations to the Electronic Communications Act of 4th July 2003, no. 83.

2.4.2 Anonymity and the Internet

When it comes to the Internet, anonymity presents some different issues to the offline world. The online environment (which at first can be seen as similar to the physical world) is very complicated and many factors that are not present in the physical world enter into play.

The way the Internet works is different from the offline world. For example, it is very difficult to make a simple cash purchase over the Internet due to the paucity of cash equivalents for the online environment. It is also difficult to browse anonymously for items in an online store as our presence will be noticed and monitored because of how the Internet is set up.

To understand how the Internet works and how it differs from the physical world we can take a look at the example given by Roger Clarke in his article "The Internet as a Postal Service: A Fairy Story"[53]. He refers to the Internet as a postal service and this postal service wants to deliver a book from point A to point B, but this book is too big to be sent in one piece. The book is broken into piece small enough to be sent through the postal service. Then each piece is placed into a packet. The packets are numbered sequentially. Each packet has inscribed on it the packet identifier, the number of packets that make up the complete set, the address of the recipient, and the address of the sender. Then the packets are sent through the web and when they reach the final destination the book is put back together thanks to the information inscribed in each packet. This information is very important as the packets can be sent through many different roads and ways,

[53] Clarke, Roger. *The Internet as a Postal Service: A Fairy Story,* February 1998 at <http://www.anu.edu.au/people/Roger.Clarke/II/InternetPS.html>.

but the information on it will help identify the intended recipient. But if the packet is not delivered it can be sent back to the sender because of the information inscribed in the packet. That info can help identify the user that has sent the packets. In the physical world, as I mentioned before, there is no need to put identifiable information on the letter or book one sends in the traditional postal service.

Comparing the browsing activity in a physical store and on the Internet, we can say that on the Internet the items are not displayed there for you to see as in the physical store. On the Internet you must request the items you want to see, more specifically you send out a request of what you want. This request is a packet of information sent to the store where it tells what item you wish to see and the information about where to send the requested item. Thus, browsing on the Internet can leave a lot of information that can contain the identity of the user or can lead to it. As a standard at least the Internet Protocol address[54] must be on the header of the message or packet sent.[55] But most browsers add more information that just an IP. Here is an example of the information gathered by the privacy test at https://www.anonymizer.com:

[54] Referred to from now on as "IP".
[55] Nicoll, Chris, C*oncealing and revealing identity on the internet.* In C. Nicoll, et al. (Eds), *Digital Anonymity and the Law – Tension and Dimensions.* 2003, ITeR, The Hague.

Test:
IP Address

Test Results:
Your IP Address is: 129.240.178.62

What is this? Your IP address is your unique "Internet Address". Much like your phone number, with this information you can be tracked and much of your personal information can be stolen.

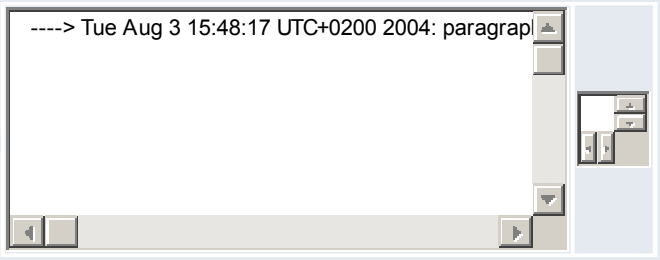
Test:
Browser Info

Test Results:
Operating System: Windows NT
Browser name: Internet Explorer
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

What is this? Having your operating system and browser information can actually enable web sites you visit to provide a better surfing experience (i.e. CNET`s Download.com automatically lands you on a home page with downloads available only for your operating system). However, this information can used in far more dangerous ways, such as tailoring hacker and virus attacks that exploit specific weaknesses in your system that can steal your information or render your PC useless.

Test:
Clipboard

Test Results:



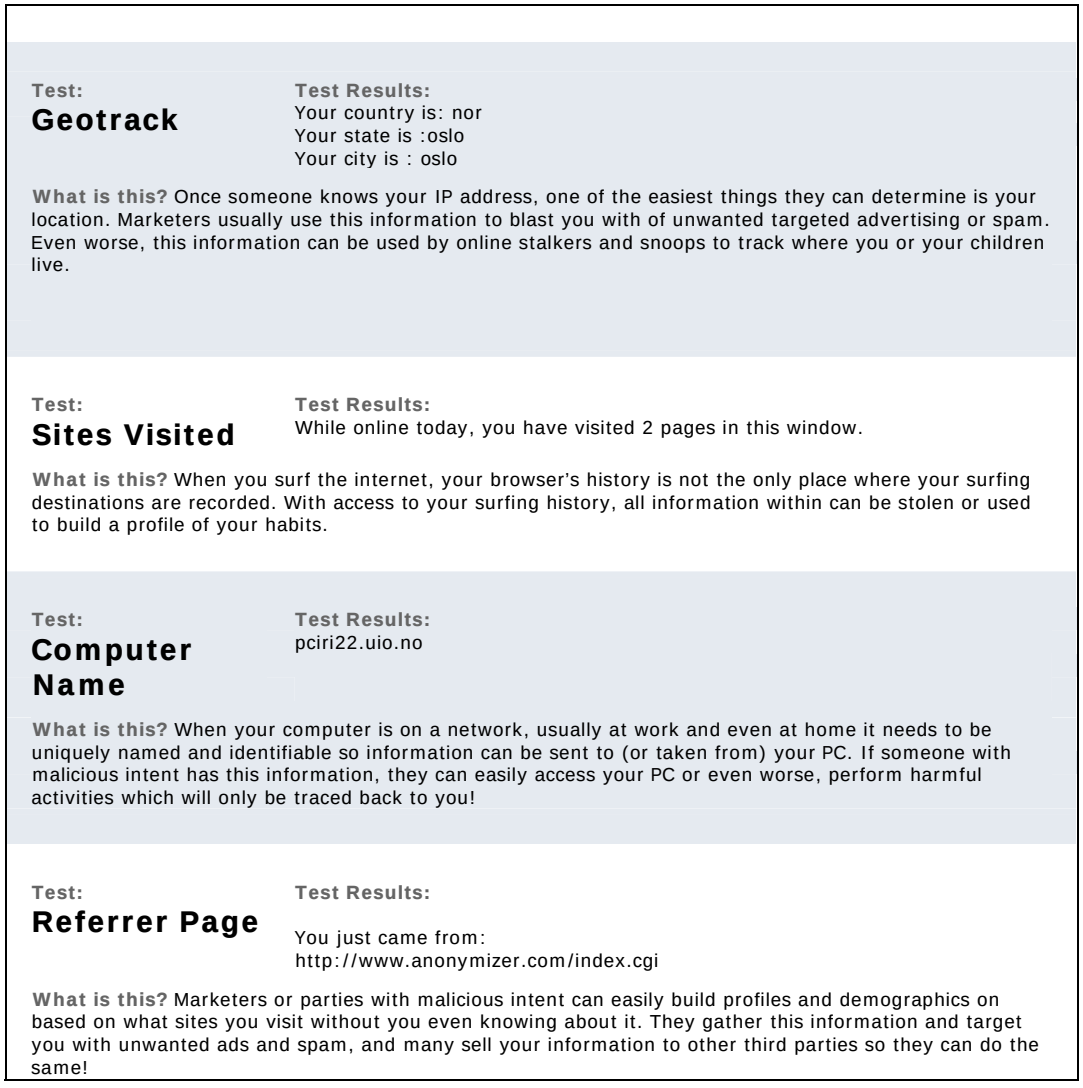
What is this? Sometimes you can be the victim of convenience. While almost everyone uses the "copy and paste" functions on their PC, you probably don't know that currently copied information is active and easily accessible from your computer's memory. Ever copy and paste an e-mail, password, credit card number or other confidential information? For someone looking to find your personal information, this is like taking candy from a baby.

Test:
Sample Cookie

Test Results:
Below is a cookie we've just placed* on your computer:
visa 12/03,1234, XXXX XXXX XXXX 1234

What is this? Cookies like this can contain personal information including:

- Your credit card information
- Your e-mail address
- Your home address & phone number
- The sample cookie we have placed on your computer is for informational purposes only. We are not collecting any information from you in any way.



Test:
Geotrack

Test Results:
Your country is: nor
Your state is :oslo
Your city is : oslo

What is this? Once someone knows your IP address, one of the easiest things they can determine is your location. Marketers usually use this information to blast you with of unwanted targeted advertising or spam. Even worse, this information can be used by online stalkers and snoops to track where you or your children live.

Test:
Sites Visited

Test Results:
While online today, you have visited 2 pages in this window.

What is this? When you surf the internet, your browser's history is not the only place where your surfing destinations are recorded. With access to your surfing history, all information within can be stolen or used to build a profile of your habits.

Test:
Computer Name

Test Results:
pciri22.uio.no

What is this? When your computer is on a network, usually at work and even at home it needs to be uniquely named and identifiable so information can be sent to (or taken from) your PC. If someone with malicious intent has this information, they can easily access your PC or even worse, perform harmful activities which will only be traced back to you!

Test:
Referrer Page

Test Results:

You just came from:
http://www.anonymizer.com/index.cgi

What is this? Marketers or parties with malicious intent can easily build profiles and demographics on based on what sites you visit without you even knowing about it. They gather this information and target you with unwanted ads and spam, and many sell your information to other third parties so they can do the same!

All these pieces of information are used by data miners. The focus of the data miners is on "identifying the trail of an individual user's web browsing within and across site so that behavioral patterns can be analyzed and predicted."[56] They may not be interested in the identity of the user. But on the other hand marketing strategists may in addition to the user's browsing habits wants to know their

[56] Broder, Alan J. *Data mining, the internet and privacy*. In B. M. Masand and M. Spiliopoulou (Eds.): *Web Usage Analysis and User Profiling*, International WEBKDD'99 Workshop, San Diego, California, USA, August 1999, pp. 56–73.

identity and other information such as address, income, etc. This information will help the marketing strategist to target the user with more advertising in a very accurate way.

The best way to link all the browsing data with personal information is by waiting for the user to disclose some personal data and then the link is made to all the other data gathered. Some times this disclosure is not needed as the info gathered may already have the personal data. For example the name given to identify a specific computer may be the actual name of the user. Also the cookies when they are stored in the user computer use the login name of the user to attach it to right user.[57]

Another way data miners or marketing strategists can gather information is by emails. The header of the email contains some information that can be personal and this information can be carried on as the message is being forwarded over the net with the possibility of being able to track it to the original sender.

Here is an example of an email header:[58]

```
Return-Path: mailbox@mindspring.com Received: from
mailmule0.mindspring.com (mailmule0.mindspring.com
[204.180.128.191]) by mailgrunt1.mindspring.com (8.7.4/8.7.3) with
ESMTP id TAA09377 for <mailbox@mindspring.com>; Mon, 24 Feb 1997
19:30:43 -0500 (EST) Received: from LOCALNAME (user-
37kb512.dialup.mindspring.com [207.69.148.34]) by
mailmule0.mindspring.com (8.8.4/8.8.4) with SMTP id TAA00875; Mon,
24 Feb 1997 19:30:34 -0500 (EST) Date: Mon, 24 Feb 1997 19:30:34 -
0500 (EST) Message-Id:
1.5.4.16.19970224193529.22e79a46@pop.mindspring.com X-Sender:
```

[57] The name of the cookie that test set in my computer was cepichar@anonymizer, “cepichar” being the user name I used to log in to the computer I was using at that moment.

[58] Available at <http://help.mindspring.com/docs/006/emailheaders/emailheaders.php3>.

```
mailbox@pop.mindspring.com X-Mailer: Windows Eudora Light Version
1.5.4 (16) Organization: MindSpring Enterprises Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii" To: MindSpring
Technical Support Desk <support@mindspring.com> From:
mailbox@mindspring.com Subject: Reading Mail Headers Cc:
mailbox@mindspring.com
```

Return-Path: mailbox@mindspring.com

Your email client will automatically refer to this header line to determine which address to use when replying, or by the mail server when bouncing back undeliverable mail messages or mailer-daemon error messages. Some mail clients will use variations which might include: Return-Errors-To: or Reply-To: [59]

Received: frommailmule0.mindspring.com (mailmule0.mindspring.com [204.180.128.191]) bymailgrunt1.mindspring.com (8.7.4/8.7.3) with ESMTP id TAA09377 for mailbox@mindspring.com; Mon, 24 Feb 1997 19:30:43 -0500 (EST)

A section is added to this field by each host service that relays the message. Received: lines are read from bottom to top, the higher received lines being the most recent to have been added. While not terribly interesting to the casual user, the information in the Received: field can be quite useful for tracing mail routing problems. The names of the sending and receiving hosts and time-of-receipt may be specified.

The example above shows four pieces of useful information (reading from back to front, in order of decreasing reliability):

The host that added the Received line - mailgrunt1.mindspring.com

The host/IP address of the incoming SMTP connection - mailmule0.mindspring.com

The reverse-DNS lookup of that IP address - 204.180.128.191

The name the sender used in the SMTP HELO command when they connected - mailmule0.mindspring.com

In short, mailmule0.mindspring.com passed the mail on to mailgrunt1.mindspring.com for final delivery to <mailbox@mindspring.com> at approximately 5:30 pm EST on Monday, February 24th.

[59] Note that the return address can be easily forged – as is commonly done by spammers to avoid being reached.

Received: from LOCALNAME (user-37kb512.dialup.mindspring.com [207.69.148.34]) by mailmule0.mindspring.com (8.8.4/8.8.4) with SMTP id TAA00875; Mon, 24 Feb 1997 19:30:34 -0500 (EST)

This is actually the first Received: line. It indicates that the mail message originated from a MindSpring dial-up PPP account with IP address 207.69.148.34. The mail server that eventually accepted the message was mailmule0.mindspring.com , which was using SendMail version 8.8.4, a UNIX mail delivery agent. The mail server also stamped the header with the actual time it received the message. Note that the time indicated is a few seconds before the header line above it.

Organization: MindSpring Enterprises

This line is used to identify the organization (or lack there of!) of the sender. Typically the default configuration for your mail settings is going to be "MindSpring Enterprises" but you can easily change this to something more personal to your family or specific to your business.

Message-Id: 1.5.4.16.19970224193529.22e79a46@pop.mindspring.com

Every mail message is assigned a unique Message-Id which helps your email client, as well as mail server, to keep track of the status of a message, and thought it looks like an email address, it really isn't. Generally this information is of no use to you and only matters to the mail server. For example, if you have Eudora configured to leave a copy of your email on the mail server, the next time you check your mail, your email client will first compare the message id's to determine if it has already seen a message, and if it should download another copy of it or just skip it. Message-Id's are also logged in special mail logs which can be called on by your system administrators (in this case "postmasters") when trying to troubleshoot technical issues like mail loops or forged mail messages.

X-Sender: mailbox@pop.mindspring.com

Some email clients will include an X-Sender header to add another layer of authentication to a mail message. In the example, Eudora uses information supplied in its configurations settings. X- headers may be thought of as "X-tra" information and are more or less X-traneous comments. They do not impact the normal delivery process of the mail.

X-Mailer: Windows Eudora Light Version 1.5.4 (16)

Some email clients will add this header line to indicate the make and version of the software used to send the message. In this case, the mailer used was the 16 bit version 1.5.4 of Eudora Light for Windows, the email client MindSpring currently ships with its software. If I had sent the mail from Netscape's Mozilla mail program, the X-Mailer might have looked something like this:

X-Mailer: Mozilla 3.01 (Win95; I)

Not all email clients include an X-Mailer header.

Mime-Version: 1.0

MIME-compatible email clients look for this line when first determining what to do with attachment files-- if MIME attachments are included, email clients first be sure they understand compatible MIME types. For those of you obsessed with acronyms, MIME stands for Multipurpose Internet Mail Extensions. It is an Internet standard for transferring non-textual data through email. MIME is what makes it possible to exchange graphic documents and multimedia files across systems.

Content-Type: text/plain;charset="us-ascii"

This line tells the receiving email client exactly what MIME type or types are included in the mail message. As long as the MIME-type referenced is compatible with the mail program it should have no problems automatically decoding the attachments. In the example above, [text/plain; charset="us-ascii"] just tells us that the message contains a regular ASCII text message.

As we can see from the above, lots of information can be extracted from the email header as well as from the browser header to help the data miners and the marketing strategists to create a profile of a person's behavior on the Internet.

Yet as mentioned in section 2.3.2.1, there are ways to avoid the gathering of information for profiling purposes. Maintaining a degree of anonymity is one such way; also data protection laws may help in preventing profiling – as elaborated upon in chapter 3.

Numerous tools and services exist which can help to enhance the possibility of being anonymous on the Internet. For anonymous browsing, use may be made of tools and services such as The Anonymizer[60], beHidden.com[61], The Cloak[62], JAP[63] and Rewebber[64]. Also one may use any of the Public Proxy servers listed at <http://www.publicproxyservers.com>.

[60] See <http://www.anonymizer.com/index.cgi> for more information.
[61] See <http://behidden.com/> for more information.
[62] See <http://www.the-cloak.com/anonymous-surfing-home.html> for more information.
[63] See <http://anon.inf.tu-dresden.de/index_en.html> for more information.
[64] See <http://www.rewebber.de/index.php3.en> for more information.

The most common mechanism for anonymous browsing is the use of a proxy server. This is used by most of the tools and services mentioned above. A proxy is "the agency, function, or office of a deputy who acts as a substitute for another."[65] A proxy server is a kind of shield between your computer and the internet page you are accessing. Such servers accumulate and save files that are most often requested by millions of Internet users in a database, called cache. The cache of a proxy server may already contain information you need by the time of your request, making it possible for the proxy to deliver it immediately. Also, proxy servers can help in cases when some web pages make some restrictions on users from certain countries or geographical regions.

An anonymous proxy server hides your IP address and prevents others from gaining unauthorized access to your computer through the Internet. It does not provide anyone with your IP address and effectively hides any information about you and your browsing habits. Also it doesn't let anyone know that you are surfing through a proxy server.

FIGURE 1: STANDARD INTERNET CONNECTION
THE IP ADDRESS OF THE USER IS EXPOSED AND EVERY SITE VISITED CAN SEE IT.

Figure 1 above represents a direct connection to the Internet. In this connection, the web pages can gather most of the information given away by the browser and the cookies in your system.

[65] See <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=proxy>.

FIGURE 2: PROXY INTERNET CONNECTION

THE USER CONNECTS THRU A PROXY SERVER THAT IS CONNECTED TO THE INTERNET. ONLY THE PROXY SERVER'S IP ADDRESS IS REVEALED WHILE THE USER REMAINS ANONYMOUS.

Figure 2 above represents a connection through a proxy server. In this scenario, the person using the browser sends a request of a web page to the proxy server and then the server will get the web page from the Internet and show it to the person that made the request. The host of the web page will see that the request came from the IP of the proxy server, not knowing it was a proxy server that made the request, and most importantly it will never see the IP of the user that requested that page.

Some of the disadvantages of proxy servers are that they might be too slow and that the pages that require the use of cookies, java scripts or any sort of authentication, like banks or payment systems, won't work properly.

For sending anonymous emails there are numerous services and tools available too. Examples of these are @nonymouse.com,[66] and Riot Anonymous Remailer[67] among others.

Professor A. Michael Froomkin[68] in his article *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*[69] gives a very good example of how anonymous remailers work, while at the same time giving different scenarios for traceable and untraceable anonymity.

---

[66] See <http://anonymouse.ws/> for more information.
[67] See <http://riot.eu.org/anon/> for more information.
[68] See *supra* n. 3.
[69] See *supra* n. 39.

Before outlining the example, I want to point out that many scholars agree with Froomkin in pointing out that anonymity on the net is not absolute, and can vary from context to context – as I have already indicated in section 2.3. For example, Chris Nicoll states that:

"[A]nonymity can not be seen as an absolute. … There are three points to be aware of: ●Anonymity is a question of degree; ● the degree of anonymity a person may desire will depend on the circumstances. For example, a criminal will strive to conceal all identity pointers, but a web surfer may be content to conceal only what may make her prey to irritating e-mails; ● a person will not present the same face to everyone in that he or she may be happy for "X" to know of identity pointers "a", "b" and "c" but seek to conceal attribute "b" from "Z"."[70]

As we can see, depending on the circumstances one might want to use a less secure form of anonymity or a more secure form.

Now going back to Froomkin's example, he explains the workings of an anonymous remailer. If "A" wants to send a letter to "B" without letting "B" know where it came from, all "A" needs to do is send the email to the remailer where all the info regarding "A's" identity will be taken out, then the remailer will send the email to "B". Froomkin sees this kind of transaction as traceable anonymity as the identity of "A" could be easily obtained either by persuading the remailer to give the identity, which he might have kept in a log, or by using the aid of a judge, in case "A" has committed a crime, to force the remailer to give the identity.

[70] See Nicoll, *supra* n. 55.

Froomkin states that "much greater security, and nearly iron-clad anonymity, can be achieved at the price of some what greater complexity through the use of untraceable anonymity"[71] and he gives an example of how this can be achieved.

The example goes more or less like this: "A" sends an email to "B" using three remailers ("X", "Y" and "Z") and to reinforce the security of the message "A" encrypts it with "B's" public key so that only "B" can read it. Then "A" puts the encrypted message in a message to "Z" with instructions to send it to "B". Then "A" encrypts the message to "Z" so that only "Z" can know whom to send it to and puts it in a message to "Y" and so on. Then "A" sends the message through the remailers until "B" gets it. In this case the reconstruction of the chain will be more difficult than in the first example as various factors can intervene; one of these being that each of the remailers is in a different country or jurisdiction.

After looking at these examples I am reminded of a conversation I had with Professor Jon Bing where he told me that anonymity depended on economics. The accomplishment of being anonymous depended on how much money, effort and time one party is willing to spend to maintain its anonymity set against how much money, effort and time the other party is willing to spend trying to reveal the other's identity.

The examples given above for browsing and sending emails anonymously are the most commonly used. There are others systems and tools, like *LPWA*[72] and

[71] See Froomkin *supra* n. 39.
[72] See <http://www.bell-labs.com/project/lpwa/> for more information.

Onion Routing[73]. Also there are many studies taking place that are looking into the possibility of anonymity on the internet – for example JANUS[74] and APES.[75]

2.5 Concluding Remarks

There is no question that anonymity is good for the development of the individual and society. But there are also negative aspects. To determine when anonymity should be allowed or not is a difficult task.

In every place we visit on the Internet we leave a trace, regardless of whether or not we are anonymous. The more we use the Internet the more data about us will be collected. As the Working Party on the Protection of Individuals with regard to the Processing of Personal Data states, "…the risks to our personal privacy lie not only in the existence of large amounts of personal data on the Internet, but also in the development of software capable of searching the network and drawing together all the available data about a named person."[76] Nevertheless, our degree of anonymity will influence the degree to which those data can be meaningfully linked to form a profile of us and allow personalized contact with us.

Anonymity can be achieved both in the real world and in the cyber world. But as we will see from the next chapter, the different legal interests that collide have

[73] See <http://www.onion-router.net/> for more information.
[74] See <http://www.virgate.net/> for more information.
[75] APES (Anonymity and Privacy in Electronic Services) is a project of the Belgian Flemish government aimed at developing tools and techniques for adding anonymity and pseudonyms to on-line services. For more information, visit <https://www.cosic.esat.kuleuven.ac.be/apes/>.
[76] See <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp6_en.pdf>.

not allowed the development of a standard approach to its use online. This is despite a big amount of effort being put into developing technologies and policies which will allow the balancing of the principal rights with other public policy principles.[77]

[77] *Ibid.*

3 Anonymity and the Law

3.1 Introduction

As we saw in the previous chapter, anonymity is a desirable state for individuals and for society. The different threats against the freedom of speech and the right to privacy have led to development of an extensive selection of tools and services to enhance the protection of such rights.

A pertinent question is the extent to which such tools and services are legal. To answer the question we have to look into the law and determine when anonymity is permitted.

In this chapter I lay down some of the different approaches taken in the world with respect to the legal status of anonymity. I focus on the law of the USA and the law of the EC.

3.2 Is there a right to be anonymous?

3.2.1 The US Approach to Anonymity

In the United States of America the notion of the right to anonymity comes from the constitutional protection for freedom of speech.

Anonymous writing has played an important role in the expression of ideas and particularly in the modeling of their country's independence as the federalists' papers written by James Madison et al. were originally published under the pen name of "PUBLIUS"[78].

There is no explicit constitutional right of anonymity in the United States, but the jurisprudence has stated that the right to be anonymous derives from the First Amendment to the Bill of Rights in the Constitution.

The first relevant case that reached the US Supreme Court was *Lewis Publishing Co. v. Morgan*[79] in 1913. In this case the registration and publication provision in the Post Office Appropriation Act of 1912 was challenged. The challenged provision required "every news paper, magazine, periodical or other publications" to file with the Post Master General a list of its editorial and business officers and its proprietors, and to publish this information twice a year.[80] The court decided that this provision had more to do with the intent to classify mail to be able to provide the necessary second class mail subsidy and that it was a legitimate

[78] Notes and Comments, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, Yale Law Journal, 1961, vol. 70, pp. 1084 et seq.
[79] *Lewis Publishing Co. v. Morgan*, 299 U. S. 288 (1913).
[80] Post Office Appropriation Act of 14th August 1912, ch. 389 §2, 37 STAT 554.

provision that did not infringe the First Amendment right to disseminate ideas impersonally (as the plaintiff claimed).

The first US Supreme Court decision that upheld the right to be anonymous was *Tally v. California.*[81] In this case, the Supreme Court cited the First Amendment in overruling a statute banning the distribution of anonymous hand bills. The court reviewed the historic basis of the right of anonymity by stating that "anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymous or not at all." [82]

The second most important case to reach the Supreme Court was *MacIntyre v. Ohio Elections Commission.*[83] In this case, the Court quoted the Tally decision and added: "Anonymity . . . provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent … The specific holding in *Talley* related to advocacy of an economic boycott, but the Court's reasoning embraced a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation."[84] With those words, the Supreme Court said that the right to be anonymous should be guarded as it is a very hard earned value of society.

---

[81] *Talley v. California*, 362 U.S. 60 (1960).
[82] *Ibid*.
[83] *MacIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).
[84] *Ibid*.

Another interesting case, though it does not deal directly with the issue of anonymity, is *National Advancement of Colored People (NAACP) v. Alabama*,[85] decided in 1958. The decision stated that the disclosure of the list of members of the NAACP ordered by an Alabama court was against the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech. By doing so the Supreme Court "recognized the vital relationship between freedom to associate and privacy in one's associations.… Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs…. on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility. Under these circumstances, we think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."[86] Indirectly, the court here recognized a right to associate anonymously in order to protect the privacy of those who joined any association.

No case regarding online anonymity has yet reached the US Supreme Court. However, the issue has been debated in the lower courts.

The first case to determine the issue of anonymity on the Internet was *A.C.L.U.[87] of Georgia v. Miller.*[88] In this case, the US District Court found that a

[85] *N.A.A.C.P. v. Alabama,* 357 U.S. 449 (1958).
[86] *Ibid.*
[87] A.C.L.U. = American Civil Liberties Union.

Georgia statute attaching criminal consequences to the act of anonymous or pseudonymous communication over the Internet violated the First Amendment guarantee of free speech. In reaching its decision, "the Court found that the statute was presumptively invalid on the basis that the identity of the speaker is no different from other aspects of a document's content that the author is free to include or exclude."[89]

3.2.2 The European Approach to Anonymity

In Europe – as in the United States of America – there is no explicit right to be anonymous. There are, however, some laws at the national level which deal with the issue of anonymity. In Belgium, for example, the Royal Decree of 13th March 2001 on the processing of personal data for historical, statistical and scientific purpose lays down some anonymity requirements.[90] Also in Belgium there is a draft law of 22nd March 2001 on anonymous witnesses.[91]

In France, the Law on Freedom of Communication of 30th September 1986, modified by Law 2004-575 of 21st June 2004, recognizes a right to access the internet anonymously.[92] There is also an article in the Social Action and Family Code that allows for women who are giving their child for adoption at birth to

---

[88] *A.C.L.U. of Georgia v. Miller*, 977 F. Supp. 1228 (N.D.Ga 1997).
[89] *Ibid.*
[90] Goemans, Caroline. *Anonymity on the Internet: concept and legal aspects***.** Workshop APES Interdisciplinary Center for Law and IT, ICRI, K.U.Leuven, 19 April 2001, at <www.law.kuleuven.ac.be/icri/documents/58anonymity.ppt>.
[91] *Ibid.*
[92] Loi n° 86-1067 du 30 septembre 1986 Loi relative à la liberté de communication "Loi Léotard". at <http://www.legifrance.gouv.fr/WAspad/Visu?cid=20455&indice=1&table=CONSOLIDE&ligneDeb=1>.

keep their identity a secret.[93] Article L.222-6 says that every woman that requires, at the moment of birth, that her identity and admission to a health institute remains a secret, will be informed of the legal consequences of her petition and the importance for every person to know their origins and history. She will be then asked to write down, if she accepts, information about her health and that of the father, the origin of the baby and the circumstances of the birth, and in a sealed envelope her identity. Then she will be informed of the possibility she has to waive at any moment the secrecy of her identity. If she does not waive it her identity can only be disclosed on the conditions set out by article L.147-6 of the same Code. These conditions are if the mother unambiguously consented to waive her secrecy and if the mother dies and she did not express for her identity to remain secret after death. The code also states that for this matter no identity document will be required nor any investigation shall be processed.

Here we can see that the French legislator has given a lot of thought to the right of being anonymous and tried to balance this right with other fundamental rights.

There is a case regarding these provisions which reached the European Court of Human Rights, where the applicant was given for adoption in the circumstances mentioned above and was subsequently demanding the revelation of her biological mother's identity, stating that she had a right to know her family history pursuant to Article 8 of the European Human Rights Convention. The Court agreed with the French government that the anonymity of the mother should remain as the applicant was given access to the documentation regarding

[93] Code de l'Action Sociale et des Familles, Article L.222-6 as amended by *Loi nº 2002-93 du 22 janvier 2002 art. 2 Journal Officiel du 23 janvier 2002.*

the circumstances of her birth and the right of the mother to preserve her anonymity to protect her privacy.[94]

Another case which reached the European Court of Human Rights and which touches on the issue of anonymity is *Z v. Finland*[95] where the Court found a violation of Article 8 when a Finnish court released some documents that had some health information regarding the applicant without removing all identifying data first.

Hence, the European Court of Human Rights has recognized (at least indirectly) the non-disclosure of identity as a tool for the protection of the right to respect for private life in Article 8.

In Germany, the Federal Data Protection Act encourages the anonymization of personal data. In section 3(6) it states that ""Rendering anonymous" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual."[96] It goes further on stating that "data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and *rendering persons anonymous*, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection."[97] Also in section 30 it set out the rules for the collection and storage of data in the course of business for the purpose of transfer in anonymised form. Additionally, the German Federal Teleservices Data Protection Act obliges

[94] Case of *Odièvre v. France* (Application no. 00042326/98)
[95] Case of *Z v. Finland* (Application no. 00022009/93)
[96] German Federal Data Protection Act as of 1st January 2002. English translation at <http://www.bdd.de/Download/bdsg_eng.pdf>.
[97] *Ibid.* See section 3(a). (intentional italic)

teleservices providers to "offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options."[98]

In the Netherlands, the Franken Commission on Constitutional Rights in the Digital Age recommended that the "incorporation of a constitutional right on anonymity, based on the right of privacy, should be rejected".[99]

On the other hand, at a pan-European level there are some laws that deal with anonymity relatively directly. The EC Directive on Electronic Signatures expresses the right of a person to mention a pseudonym instead of a real name.[100] Also the Electronic Commerce Directive in recital 14 expresses that the "directive cannot prevent the anonymous use of open networks such as the internet."[101]

Another mention of anonymity is made in the Data Protection Directive when it states "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."[102] There will be a more comprehensive discussion on this issue in the next section.[103] Also the Working Party on the Protection of Individuals with regard to the Processing of Personal Data has issued a recommendation[104] about anonymity on the Internet.

---

[98] German Act on the Protection of Personal Data Used in Teleservices (Gesetz über den Datenschutz bei Teledienstenen) Federal Law Gazette (Bundesgesetzblatt) 1997 I 1871. See Section 4(1).
[99] See *supra.* n. 90.
[100] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal L 013, 19/01/2000 pp. 12 – 20,* Article 8.
[101] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal L 178, 17/07/2000 pp. 1 – 16*.
[102] See *supra* n. 1, Recital 26.
[103] See section 3.3 for the discussion.
[104] See *supra* n. 76.

The Council of Europe in Recommendation R (99) 5 of 23rd February 1999 states that "anonymous access to and the use of services, and anonymous means of making payments, are the best protection of privacy", and urges the users to "find out about technical ways to achieve anonymity." The recommendations by the Council are not legally binding on its members, but the latter do take them very seriously and try to implement them as best as possible.[105]

As we can see then, there are some legal documents that explicitly deal with the issue of anonymity.

While some countries (like Germany) see that anonymity is derived from and part of the right of privacy, others (like France) tend to lean more to the right of freedom of expression. Both the right to privacy and the right to freedom of expression are protected in the European Convention of Human Rights.

Article 8(1) of the European Convention of Human Rights states that: "Everyone has the right to respect for his private and family life, his home and his correspondence." This right clearly covers private communication. In this direction, Article 5 of Directive 2002/58/EC on privacy and electronic communications establishes the confidentiality of electronic communications, making it mandatory that each EU member state "shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned."

Article 10(1) of the European Convention of Human Rights states: "Everyone has the right to freedom of expression. This right shall include freedom to hold

[105] See Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague, Kluwer Law International, 2002, p. 36.

opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

Now Articles 8 and 10 of the European Convention of Human Rights may be the gateway to an anonymity right. Yet these rights are not absolute and can be overridden (under Articles 8(2) and 10(2)) "in accordance with the law" and if "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

An example of how the privacy rights can be challenged, to avoid the anonymity of a person, is in the case of spammers or senders of commercial communication (unsolicited or not), which are under an obligation set out by Articles 6 and 7 of the Electronic Commerce Directive to identify the sender of the communication and to set out clearly that the communication is a commercial one. By not allowing the spammer or sender of a commercial communication to hide under anonymity, the law has given more weight to the privacy rights of the recipient, which when bothered by such type of communication can discard it right away and continue with his/her private life. Another reason the law makes the identification requirement is to let the recipient know where to address his/her complaints.

As we can see, there are some provisions that do not allow anonymity and thus require identifiability. Most of these provisions are in favor of the consumers, such as the Electronic Commerce Directive that requires all service providers to render some information to be able to provide their services.

Other typical instances of identifiability requirements occur where it is necessary to protect one or more of the parties involved in certain transactions. For example, in contracts that are done over some distance or period of time, the disclosure of the identities of the parties involved is to guarantee the completion of the contract and to ensure payment. In other contexts, knowledge of the identity of the subject is required to prevent the commitment of a crime or to make sure that the person is eligible to perform the action that is required from him/her. When selling cigarettes, the vendor must often establish that the buyer is old enough, or when a doctor performs a procedure he/she must establish that he/she has the necessary license to do so.

In the prevention of other crimes like cybercrime some provisions of the Cybercrime Convention[106] are aimed to aid in identifying the wrong doers. In its procedural part, the Convention stipulates that retention of computer data should be in a way that allows for the identification of the subscriber (Article 18). For some people this may be a violation of subscriber privacy by not guaranteeing their anonymity.[107] Others claim that these provisions will infringe the right to freedom of expression as there is a "generalized concern arising from such accounts that an online identification requirement will result in self-censorship and place a substantial burden on the speech and freedom of association of persons who wish to participate in online communities."[108] The Convention does not prohibit anonymous communication, but it does provide for the identity of the subscriber to be retained. With this it erases the possibility of untraceable anonymity while trying to stop the criminals that act on the Internet. At the same

[106] See *supra* n. 2.
[107] Aldesco, Albert I. Comment. *The demise of anonymity: a constitutional challenge to the Convention on Cybercrime.* Loy. L.A. Ent. L. Rev., 2002, vol. 23, pp. 81–123.
[108] *Ibid.* p. 108.

time, it preserves a traceable anonymity for those who make use of the Internet lawfully and legitimately.

As we see from the above, the laws that support anonymity and identifiability tend to manifest a careful balancing of interests and rights. This balancing process is difficult to do in the abstract, without taking into account the concrete circumstances of the particular case.

3.3 Anonymity and Data Protection: An example

Directive 95/46/EC is one of the legal instruments in the European Union that encourages the anonymization of data. In this particular case, the Directive stipulates that data that is anonymized can no longer be considered personal data, because all the identifying elements have been removed, thus making the "data subject no longer identifiable"[109] and should not be considered within the scope of the Directive.

Here we see the Directive attempting to give a definition of what anonymous data should be, and by the looks of it, anonymous data are data that can no longer be linked to an identifiable person.

An important issue here concerns the meaning of the word "identifiable" as opposed to "identified". An identified person is someone whose identity is already known and certain, while identifiable is someone who can potentially be identified. The Directive gives some light on the definition of identifiable when it

[109] See *supra* n 1.

states that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Article 2(a)). According to that definition, most data should be considered identifiable if they relate to a person. However, the Directive draws limits with respect to the means and amount of effort involved in linking data to a person. It states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" (recital 26). This could mean that a person will only be considered identifiable if his/her identity can be obtained easily and without the aid of sophisticated methods.[110] However, Professor Bygrave points out that the Directive uses the phrase "likely reasonable" and he explains that the term "likely" could mean a probability of identification while the term "reasonable" could refer to "difficulty (e.g., in terms of time and resource utilization)."[111] He further explains that the probability criterion arguably merges with the criterion of reasonableness.

Also Article 6(1)(e) of the Directive allows keeping identified personal data only for as long it is necessary for the purpose for which the data were collected. This provision in some way is allowing that data can be used after its purpose has been fulfilled if the identification elements of it have been removed, in other words if the data have been anonymized. Article 7 sets out the rules when the data do not need to be anonymous and still can be processed. This is when the data subject has unambiguously given his consent or it is necessary for the compliance of a legal obligation or is necessary for the performance of a task in the public interest or in the exercise of official authority or is necessary for the

[110] This appears to be the criterion adopted under the 1981 Council of Europe Convention on data protection, CETS 108, Article 2(a). See further Bygrave, *supra* n. 105, p. 43.
[111] *Ibid.*, p. 44.

purpose of the legitimate interest pursued by the controller except when overridden by the interests for fundamental rights. Also processing personal data is permitted if necessary for the performance of a contract to which the data subject is party. This last provision seems to be in accordance with the regular commercial use when some data are needed to make sure that a contract will be carried out.

In the Directive on privacy and electronic communications the issue of anonymity is dealt with in a more concise and direct manner. The Directive recommends that "the Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimizing the processing of personal data and of using anonymous or pseudonymous data where possible" (recital 9). Further emphasis on the desirability of anonymity is laid in recital 30, which encourages that electronic communications networks should be designed to keep the processing of personal data to a minimum and which also encourages aggregation of traffic data. Also noteworthy is recital 33, which states that "in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card".

This last provision appears to be in conflict with the thrust of the Cybercrime Convention which requires the identification of subscribers. An example of this conflict can be seen in the Norwegian law where the possibility of anonymous

access encouraged by the Directive on privacy and electronic communications has been turned back with the new regulations to the Act on Electronic Communications mandating that all e-communication providers must keep a record of their end users.[112]

Finally, the Directive lays down as a ground rule that analysis of traffic data for marketing communications services or for provision of value added services may only occur if the data subject consents or if the data are anonymised (Article 6; recital 26).

With all of these provisions, the Directive goes a long way to recognizing anonymity as an important normative interest if not right. However, it still leaves ambiguous the notion of anonymity – as does Directive 95/46/EC. Anonymisation is not directly defined in either Directive and is left as a function of the very diffuse notion of identifiability (see above). This also leaves open the possibility that some data may be released in a form which is apparently anonymous from the perspective of the data controller at hand but which is nevertheless not entirely anonymous for others to whom the data are divulged. It is unclear whether the drafters of the Directives have been aware of this problem. Nonetheless, the above analysis would suggest that while the drafters have been increasingly concerned about the value of anonymity, they have not yet given sufficient attention to the practical implications of anonymity as a legal concept.

[112] See *supra* n. 52.

4 Conclusion

At a glance, anonymity seems to be a desirable state for individuals and society as it helps facilitate the flow of information and communication as well as protecting one's privacy.

At the same time, the legal status of anonymity has not yet been properly defined. The same can be said with respect to its normative roots.

In Europe, the Working Party on the Protection of Individuals with regards to the Processing of Personal Data and the Council of Europe have issued recommendations regarding the use of anonymity on the internet. These recommendations state that in order to maintain the same level of protection for their privacy online, all individuals should have the same ability to remain anonymous in the same manner as they do offline. They also recognize the need to set some controls to avoid an abusive use of anonymity.

These recommendations have not always been followed in the right direction. This can be seen in Norway where a system that allowed for persons to anonymously obtain access to the wireless communication network (as recommended by the Directive on privacy and electronic communications) has now been replaced by new provisions requiring the identifiability of all electronic communications users. This may not be the end of anonymity, but it signals a start towards a more controlled environment where identifiability is easier to achieve.

As long as there is no stronger pronunciation toward the recognition of a right to be anonymous, these examples of conflicts between what's desired and what's

really applied will always be present. The balance between a right to be anonymous and the interest of identifiability has rarely if ever been tested in a court of law to the extent to which one or the other has totally prevailed. In the absence of other legal standards, individuals and organizations have quite a bit of leeway in determining when and where they shall be anonymous. However, letting each individual decide when and where anonymity is permitted will likely end in chaos as ad hoc personal interests will considerably determine the "when and where" of anonymity *contra* identifiability.

The need for a larger and more standardized recognition of a right to be anonymous is necessary to help harmonize national and community laws on these matters. There is much to be said that in such harmonization, anonymity should be the standard point of departure, with identifiability the exception.

5 Bibliography

5.1 Legislation, recommendations and reports

5.1.1 European Union

5.1.1.1 Directives

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/11/1995 P. 0031 – 0050.*

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures**,** *Official Journal L 013, 19/01/2000 P. 0012 – 0020.*

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *Official Journal L 178, 17/07/2000 P. 0001 – 0016.*

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal L 201, 31/07/2002 P. 0037 – 0047.*

5.1.1.2 Recommendations

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *RECOMMENDATION 3/97: Anonymity on the Internet,* Adopted on 3 December 1997, XV D /5022/97 final, WP 6, at:
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp6_en.pdf>

5.1.2 Council of Europe.

5.1.2.1 Conventions

Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005 (1950) at
<http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG>

Convention on Cyber crime CETS No.: 185 (2001) at
<http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG>

5.1.2.2 Recommendations

Council of Europe recommendation Rec (99)5 / 23 February 1999 on the protection of privacy on the Internet.

5.1.3 France

Code de L'action Sociale et des Familles, Article L.222-6 as amended by *Loi nº 2002-93 du 22 janvier 2002 art. 2 Journal Officiel du 23 janvier 2002.*

Loi n° 86-1067 du 30 septembre 1986 Loi relative à la liberté de communication “Loi Léotard”. At
<http://www.legifrance.gouv.fr/WAspad/Visu?cid=20455&indice=1&table=CONSOLIDE&ligneDeb=1>

5.1.4 Germany

German Act on the Protection of Personal Data Used in Teleservices (Gesetz über den Datenschutz bei Telediensten) Federal Law Gazette (Bundesgesetzblatt) 1997 I 1871 See Section 4(1)

German Federal Data Protection Act as of January 1st 2002. English translation at <http://www.bdd.de/Download/bdsg_eng.pdf>

5.1.5 Norway

Act on Electronic Communications of July 4th, 2003, no. 83.

5.1.6 United Nations

Universal Declaration of Human Rights. At <http://www.un.org/Overview/rights.html>

5.1.7 United States of America

Post Office Appropriation Act of August 14, 1912. ch. 389 §2,37 STAT 554.

The Constitution of the United States of America. At <http://www.law.cornell.edu/constitution/constitution.overview.html>

5.2 Books and Articles

Aldesco, Albert I. Comment. *The demise of anonymity: a constitutional challenge to the Convention on Cybercrime.* 23 Loy. L.A. Ent. L. Rev. 81- 123 (2002).

Brazier, F.M.T. Oskamp, A. Prins, J.E.J. Schellekens, M.H.M. Wijngaards, N.J.E. *Are anonymous agents realistic?* In: Proceedings of the LEA 2003: The Law and Electronic Agents , June , 2003 , Oskamp, A. Weitzenboeck, E.

Broder, Alan J. *Data mining, the internet and Privacy*. In B. M. Masand and M. Spiliopoulou (Eds.): *Web Usage Analysis and User Profiling*, International WEBKDD'99 Workshop, San Diego, California, USA

Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002)

Clarke, Roger. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1999. at <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>

____ *The Internet as a Postal Service: A Fairy Story'*, February 1998 at, <http://www.anu.edu.au/people/Roger.Clarke/II/InternetPS.html >

Eklund, Esa. *Controlling and Securing Personal Privacy and Anonymity in the Information Society.* At <http://www.niksula.cs.hut.fi/~eklund/Opinnot/netsec.html>

Feasby, Jonathon T., *Who was that masked man? Online defamation, freedom of expression, and the right to speak anonymously*. Canadian Journal of Law and Technology, Vol. 1 No. 1, January 2002. At <http://cjlt.dal.ca/vol1_no1/articles/01_01_Feasby_defam_fset.html>

Froomkin, A. Michael. *Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases*. 15 U. Pittsburgh Journal of Law & Commerce 395, 1996. At <http://www.law.miami.edu/froomkin/articles/ocean.htm>

____ *Anonymity and Its Enmities*, 1995 J. ONLINE L. art. 4. at <http://www.wm.edu/law/publications/jol/95_96/froomkin.html>

Goemans, Caroline. *Anonymity on the Internet: concept and legal aspects***.** Workshop APES Interdisciplinary Center for Law and IT, ICRI, K.U.Leuven, 19 April 2001, at <www.law.kuleuven.ac.be/icri/documents/58anonymity.ppt>

Gia B. Lee, *Addressing Anonymous Messages in Cyberspace*, Harvard University Journal of Computer-Mediated Communication, Vol. 2, No. 1, June 1996.

Kabay, M. E. *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy,* Annual Conference of the European Institute for Computer Antivirus Research (EICAR), Munich, Germany 168 March 1998. at <http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Privacy/Anonymity_Pseudonymity.PDF>

Martínez, Isabel Ma. *Efectos del anonimato en la comunicación de grupos que utilizan tecnologías asistidas por ordenador. Un estudio Cuantitativo y cualitativo.* Anales de psicología, Vol. 17, no. 1 Junio 2001, Pág. 121-128

Marx, Gary. *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research* In J. Caplan and J. Torpey (Eds.) , *Documenting Individual Identity*. Princeton University Press, 2001. at <http://web.mit.edu/gtmarx/www/identity.html>

Nicoll, Chris, et al. (Eds), *Digital Anonymity and the law – Tension and Dimensions.* 2003, ITeR, the Hauge.

Nissenbaum, Helen. *Protecting Privacy in an Information Age: The Problem of Privacy in Public.* Law and Philosophy, 17: 559-596, 1998.

____ *The Meaning of Anonymity in an Information Age*, The Information Society, 15:141-144, 1999 (Reprinted in *Readings in CyberEthics* (2001) R.A. Spinello and H.T. Tavani (eds.) Sudbury: Jones and Bartlett)

Notes and Comments, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084 (1961);

Rigby, Karina, *Anonymity on the Internet Must be Protected*, Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1995. at <http://swissnet.ai.mit.edu/6095/student-papers/fall95-papers/rigby-anonymity.html >

Wells B. Anne, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*. 104 Yale L.J. 1639 (1994-1995)

5.3 Dictionaries and Web Resources

Art Lex, Art Dictionary at <http://www.artlex.com>

Cambridge Dictionaries Online at <http://dictionary.cambridge.org>

Encarta on line, at <http://encarta.msn.com>

Free On-line Dictionary of Computing, at <http://foldoc.doc.ic.ac.uk>

Hacking Dictionary a <http://www.robertgraham.com/pubs/hacking-dict.html>

Longley, Dennis, *Data & computer security: dictionary of standards, concepts and terms* McMillian, UK, 1987.

Merriam-Webster Online Dictionary, at <http://www.m-w.com/ >

Net Lingo, The Internet Dictionary at <http://www.netlingo.com>

On-line Medical Dictionary, at <http://cancerweb.nlc.ac.uk/>

Slade, Rob, *Glossary of Communications, Computer, Data, and Information Security Terms*, at <http://sun.soci.niu.edu/~rslade/secgloss.htm#anonymous>.

Sookman, Barry B. *Computer, internet and electronic commerce terms: judicial, legislative and technical definitions*, Carswell, Toronto, 2001.

The America Heritage Dictionary of English Language, 4th ed., 2000, at <http://www.bartleby.com>

The Compact Oxford English Dictionary, 2nd ed., 1998.

Weisstein, Eric W. "Anonymous", in *MathWorld – A Wolfram Web Resource*, at <http://mathworld.wolfram.com/Anonymous.htm>.