Defining Anonymity and its Dimensions in the Electronic World

Bart Goddyn

Submitted to the Interdisciplinary Centre for Law and Information Technology (ICRI) of the Catholic University of Leuven in partial fulfilment of the requirements for the seminar on 'Law and Information Science'

January 2001

Abstract

This paper constitutes a part of a seminar project on 'Anonymity on the Internet' at the Faculty of Law of the Catholic University of Leuven. It provides an attempt to define the concept of anonymity since a qualification of the right to anonymity needs a thoughtful approach of the concept itself, in proportion to other concepts such as 'identity', 'privacy' and 'pseudonymity'. Moreover, the paper presents some aspects and notions of types and levels of anonymity in the electronic world. This approach of 'anonymity' mainly concerns digital communications and transactions.

Contents

1. Introduction

The widespread practice of computer databases containing personal information, together with the emergent use of digital communications, has created new problems relating to personal privacy. The deficiency of adequate security facilities and the impossibility to prevent unauthorised access to personal information feed the idea of 'information privacy[1]', - and more particularly anonymity -, encouraging new privacy safeguarding techniques at the same time. It is a trying task to decide what is legal or who should be held responsible for anonymous communications and transactions in the electronic world. Qualifying this right to anonymity implies a thorough discussion about its aspects and implications in the electronic world and primarily the definition of its concept and its related notions.

2. Defining 'anonymity' and related notions

Many anonymous communication systems claim anonymity without specifying a precise definition. It is not obvious indeed to define a phenomenon at the intersection of law, policy and computer science, with consequences for commerce, for personal liberty, and for the way we live and interact with each other[2]. In fact, this implies that the concept of anonymity should be considered proceeding from sociological, legal, ethical, technological, and policy approaches. A working definition of the concept may apply to all these approaches of anonymity.

2.1. Working definition of 'anonymity'

2.1.1. Lexical definition

A lexical, or dictionary, definition is given by the first-rate[3] Merriam-Webster's Collegiate Dictionary[4] and will do as a starting point. The dictionary describes anonymity as 'the state of being anonymous'. The adjective 'anonymous' is explained as 'not named or identified' or 'of unknown authorship or origin' or 'lacking individuality, distinction, or recognizability'. As it will turn out below, this definition contains some workable elements.

2.1.2. Synonym-definition

The synonym-definition of 'anonymity' is 'namelessness' which is derived from the etymological meaning of the word 'anonymity'[5]. This definition doesn't suit me fine because -on further consideration- the lack of the name is not sufficient to be anonymous[6].

2.1.3. Negative definition

A concept can be defined by determining or identifying its opposite qualities, or just by stipulating what it does *not* mean[7]. This gets me to the opposite of being anonymous, which is to be identifiable. Simply stated, anonymity is the absence of identity[8]. I use this as a working definition as it will be clear that this definition has to be nuanced. Anticipating further statements, I would like to postulate that anonymity is the absence of a *true* identity, given that a false identity is, strictly speaking, an identity but also a way to be anonymous.

2.2. Identity

The working definition of anonymity compels me to explain 'identity' rather than giving a definition of the concept of 'name', used in the synonym-definition. Knowing someone's identity is, as said, more than taking note of his name.

2.2.1. Definition of 'identity'

'Identity' is the data needed to allow one to track down somebody, for instance an old friend who shows up on the Internet. In this case, 'identity' closely follows the dictionary definition which formulates the concept as *the distinguishing character or personality of an individual*[9]. To the person verifying the identity of that old friend, that other person's identity constitutes a totality of memories: an internal representation of the distinguishing character or personality of an entity, as the verifier has come to know that entity through the relationship between him and his old friend. That totality of memories is labeled by a *name*. However, the name is not an identity; it is a label for one. It is also neither unique nor global[10].

An entity is identified by *essential* and *unique* characteristics. In the real world[11], these characteristics might include, among other things, the unchanging physical traits of the person, his preferences, or other people's perceptions of the individual's personality[12]. These characteristics are liable to evolutions.

The same goes for an identity. An identity is *essential*, both in real life as well as in the electronic world. Personal identity is the pronounced side of personality. It is the side that others can perceive, while personality is the backbone behind it. Identity is *unique* given that no two identities are the same. A specific identity may look like another but maps to a unique set of characteristics. When two persons share some of the same characteristics, this obviously doesn't imply that they have the same identity.

It remains to be seen whether a false identity is still an identity. When a person falsely assumes another's identity, his apparent characteristics are not consistent to his real characteristics. Strictly spoken, a false identity is indeed an identity but only a copy of the existing unique identity or at least an apparently existing identity.

This goes to the problem of ‘identity theft’ or ‘identity fraud’. These are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain[13]. Identity theft and identity fraud are in fact two drastic ways for a pursuit of anonymity. The electronic world creates opportunities for identity theft.

An inherent property of electronic communications and transactions is that they can be perfectly recorded and duplicated, so that a particular *digital identity* may not be unique at all.

2.2.2. Identity in the electronic world

For centuries, two related but nevertheless distinct elements made up the identity of most people. The physical element was based on their presence, on direct interaction in the physical reality of daily life; the other element was informational, based on written records which identify them as single individuals. Now, centring around the Internet, new technologies introduce an additional type of identity: ‘*digital identity*’. The electronic world simplifies the collecting and processing of information given that many processes require identity information.

Digital identity can be simply defined as the digital information that creates the image of an individually identifiable person. Digital identity is *the means whereby data are associated with a digital persona*. The digital persona is the model of the individual established through the collection, storage and analysis of data about that person[14].

A digital identity is very different from a traditional, analog informational identity. Contrary to the physical identity, nearly all aspects of the digital identity or the information that is being assembled to create the image of an individual person can be influenced and changed. Consequently, optimistic hopes have been voiced that *a new freedom* would emerge through digital identities: a free, unrestricted creation by the person who is represented. A man can assume the identity of a woman, a child that of an adult and so on. The somewhat arbitrary constraints of the physical can be overcome to express the *true* personality, or at least the identity that the creator wants at a particular moment. On the Internet, so goes the somewhat paradoxical promise, we can finally be who we really are, or who we really want to be; unlimited by social conventions and free from being stereotyped based on unwanted but ever-present aspects of our physical selves like age, gender, race or physical appearance. New media are presented as offering a radical new beginning, a conscious rebirth. As the Internet grows, so does the hope that we can remake ourselves at convenience to an even larger extent. Implicitly assumed in this view is a total separation of the physical and the electronic world, as expressed in slogans such as: "Once you're on-line, you no longer have a body". Given their fluidity, digital media open up new venues to experiment with identity that would have been entirely unimaginable in the physical world. I dilate upon this subject within the scope of the concept of pseudonymity[15].

Nowadays, identity information is important as it is viewed as *a valuable commodity*. Businesses use it to determine and to profile prospective customers on the market or as a proxy for its customers' preferences. The obtained information is then used to guide the direct marketing of other products to customers or for the retooling of current products[16].
Digital technology is changing the relationship between businesses and their customers. The ability of an organization to adapt to this changing business landscape, in part depends on the capacity and flexibility of its digital processes. To work well, the infrastructure of an organization[17] must efficiently manage the information about people that is used by business applications such as 'knowledge management', 'e-commerce' and 'business operations'[18]. In this context 'digital identity' stands for this computerized information. It includes all of the attributes that represent a person, including descriptors such as title, role, location, rights and privileges to company resources, and personnel information such as salary, benefits, and tenure.

2.2.2.1. Functions of digital identity

Looking at the Internet, it is evident that its information system is characterized by great fluidity and relatively more open access. Therefore, a digital identity system must serve four *functions*[19].

- Identification:

  Identification is the main function of digital identity. It is indispensable, as the other functions won't apply without it. Roger Clarke, a scholar with a long professional interest in questions of identity, identification and privacy in the electronic world[20], describes it as 'a process whereby a real-world entity is recognized, and its 'identity' established'[21]. He enumerates some examples of identification techniques, which can assist in associating data with persons: names, codes, knowledge, tokens and biometrics (a term used to refer to the techniques that are based on some physical and difficult-to-alienate characteristics, such as: appearance, social behaviour, natural physiography and imposed physical characteristics). Similar notions come back when discussing the types of identity and the dimensions of privacy[22]. Clarke summarizes the importance of personal identification as follows: "The purposes of the interchange of identification include

  - to provide a gesture of goodwill;
  - to develop mutual confidence;
  - to reduce the scope for dishonesty;
  - to enable each person to initiate the next round of communications;
  - to enable each person to associate transactions and information with the other person".

- Authentication:

  Authentication is the process of verifying the identity of each person using an organization's computing infrastructure. Because people are granted access to particular resources based on their identities, it is important that individual identity be verified in order to protect privacy and ensure security of the computer systems in question. Authentication verifies identity by requiring proof of identity, such as username and password or smart card and PIN combination. Another definition that follows naturally from the line of the working definition: it is the process whereby some chosen attribute of a real-world entity ('the distinguishing character or personality of an individual') is demonstrated to belong to that entity.

- Integrity:

  The digital identity has to provide certainty that a communication or a transaction has not been modified en route.

- Non-repudiation:

  The digital identity has to ensure the inability of the identified person to deny that he effected the communication or the transaction or that he participated and received the object of the communication or the transaction in question.

2.2.2.2. Forms of digital identity

The most frequent forms of digital identity on the Internet may serve as examples of digital identities. However, each example is a relative form of digital identity due to the lack of an effective architecture to verify identity on the Internet at this time.

- E-mail:

  E-mail is the main form of on-line communication[23]. It uses a protocol called SMTP (Simple Mail Transfer Protocol). An e-mail client is used to compose and receive messages, and communicates with an SMTP server which figures out where to send the message and takes responsibility for getting it there. E-mail addresses are the most common identifiers on the Internet because they are the most direct and easy way to reach somebody.
  However, the current SMTP protocol for sending e-mail includes no reliable identity verification and authentication. To establish the identity of an e-mail message, for instance, it is not enough that the recipient of the message sees the equivalent of "jattorney@lawfirm.com" in the "From" line of his e-mail program. Faking an e-mail identity is so simple that it does not even qualify as hacking these days. That is where digital signatures and authentication come in.

- Passwords:

  Passwords are used to verify a person's identity. However, they are easily shared. The biggest disadvantage is that passwords can be easily cracked by software that is benevolently referred to as 'password recovery' software. Password crackers use algorithms to crack passwords. The algorithms are generally referred to as 'dictionary' (trying common words or phrases) or 'brute force' (trying every possible combination) 'attacks'. New software cannot guarantee protection from this password cracking software, though with protective software, it can take days or weeks to crack specialized passwords. A correct password doesn't prove that the user of it really is any particular person. There is no secure link between a password and a physical or digital identity.

- Credit card numbers:

  Credit card numbers are often used as a form of identification but they are not intended to identify personal characteristics. A credit card number is only a payment mechanism. Moreover, a credit card number reveals much more information about the user than needed in a particular context. Credit card numbers have the same disadvantages as passwords.

- Internet Protocol addresses:

  The common term for a network location is 'address'. Each system on the Internet has an address. This address is called an Internet Protocol (IP) address[24]. The IP address is personally identifiable information that is automatically captured by another computer when any communications link is made over the Internet[25]. The content of this information depends on how the digital persona is connected to the Internet and other information about him that may be available. However, IP addresses link only to a computer and do not identify the user of that computer. Besides, many IP addresses are dynamic and thus variable or temporary.

Identifiability via these forms of digital identity is, as shown, relative. The current identity architecture needs an overhaul in order to facilitate flexible but secure and reliable verification of digital identity. Further details of proposals and solutions to meet to this problem are irrelevant to this paper.

2.2.3. Identity and anonymity

There are several types of identity. It is considerable to specify these types, as the various types of identity obviously involve a differentiation of levels of anonymity[26]. There are as much levels of identity as levels of anonymity. Anonymity is after all one polar value of a broad dimension of identifiability versus non-identifiability[27]. Gary Marx, Professor Emeritus of Sociology at the Massachusetts Institute of Technology, suggests seven broad types[28] of identity.

- *Legal name*: someone's name is a key to other information about that person, given that the name usually involves connection to a biological or social lineage.

- *Locatability*: a person's address involves the ability to locate that person. On the Internet, this involves knowing the actual identity or even a pseudonym by an e-mail address, a password, and a login account. However, more than one person may use the same address.

- *Pseudonyms that can be linked to the legal name and/or locatability* (literally a form of pseudo-anonymity)[29].

- *Pseudonyms that cannot be linked to other forms of identity knowledge* (real anonymity) [30].

- *Pattern knowledge*: distinctive appearance or behaviour patterns may identify a person whose actual identity or locatability is not known. This is why I passed criticism on the use of the synonym-definition as a working definition of anonymity; the lack of a name is not sufficient to be anonymous[31]. Being unnamed doesn't have to be the same as being unknown. Persons who anonymously make frequent use of a specific digital communication may come to be known because of the distinctive style of their communication.

- *Social categorization*: a person can be identified by his belonging to a social category. Some sources of identity don't differentiate the individual from others sharing the same sources (e.g. gender, ethnicity, religion, age, class, education, region, sexual orientation, linguistic patterns, organizational memberships and classifications, health status, employment, leisure activities).

- *Symbols of eligibility or non-eligibility*: the possession of knowledge (passwords or codes) or artefacts (e.g. tickets, badges) or skills may label someone as a particular kind of person to be treated in a certain way. This is important to contemporary discussions because it offers a way to control personal information and exclude abuse. Encryption technologies make this form of increased importance.

The level of anonymity you have is a result of the choices you make about your *privacy*.

2.3. Privacy

Identity knowledge is an aspect of *information privacy*[32]. It is worth considering the definition of privacy briefly, as well as the distinction between some dimensions of privacy against the background of the types of identity. It will be entirely clear that the analogy between the above-mentioned types of identity and these dimensions of privacy can be carried further on the subject of anonymity.

2.3.1. Definition and dimensions of privacy

Privacy can be defined as *the interest that the individuals have in sustaining a personal space, free from interference by other people and organizations*[33]. In fact there are many apprehensions of what privacy really is because each person perceives it differently. The perception is mainly based on personal and socio-cultural backgrounds. Privacy is also situation and relation specific.

Privacy has various *dimensions*: privacy of the person, privacy of personal behaviour, privacy of personal communications and privacy of personal data [34].

- *Privacy of the person*: this refers to the integrity of the individual's body.
- *Privacy of personal behaviour*: this relates to the individual's behaviour and particularly to someone's socio-cultural attitudes in private and public places.
- *Privacy of personal communications*: individuals claim an interest to communicate with each other, without routine control of their communications by other persons or organizations.
- *Privacy of personal data*: individuals claim an interest to restrain other individuals and organizations from processing their data. They must at least be able to exercise a substantial degree of control over their data and use thereof.

The term 'information privacy' is used to refer to the combination of communication privacy and data privacy. The privacy in the electronic world mainly concentrates on information privacy[35]. However, the privacy of personal behaviour is still an important aspect because of more specific mechanisms for observing or extracting behavioural patterns from information.

2.3.2. Privacy in the electronic world

The widespread practice of computer databases containing personal information and the emergent use of digital communications and transactions has created new problems relating to 'information privacy'. The deficiency of adequate security facilities on the one hand and the impossibility to prevent unauthorised access to personal information on the other hand encourage privacy safeguarding techniques. *Privacy protection* is a process of finding appropriate balances between privacy and multiple competing interests[36].

2.3.3. Privacy and anonymity

When browsing through literature about privacy and anonymity, there seems to be no evident distinction between these concepts. Therefore, it's important to describe their relation.

As said, anonymity is closely related to the concept of identity. An anonymous person does not reveal his true identity. Identity is essential to each person that wants to control personal information. Identity protection is thus a part of privacy protection. Consequently, anonymity is a method of privacy protection. In this respect, *anonymity is a part of privacy*.

Nevertheless, an identity might be determined based on or by cross-referencing different kinds of information, for instance, information on one's behavioural and social patterns and one's personal information[37], so that *anonymity is not sufficient to safeguard one's privacy*.

In the electronic world, the two concepts seem to have approached each other. Many computer systems need to identify a user. That way, the concept of anonymity becomes increasingly significant with regard to privacy protection in electronic services.

A common belief is that those who choose to communicate anonymously via strong cryptography or other cryptographic protections on privacy have 'something to hide', and that normal upright citizens have no need for anonymity. Similarly, some believe that people who speak anonymously are somehow ashamed of the actions that they take behind the shield of anonymity. However, this idea that only shame generates a desire for privacy is a very narrow view considering the reality of indispensable privacy protection.

2.4. Pseudonymity

2.4.1. Definition of ‘pseudonymity’

Pseudonymity is the use of a pseudonym. A pseudonym is a fictitious distinguishing mark by which a certain communication or transaction can be traced back to a certain existing person. It is, with regard to the notion of anonymity, important to distinguish pseudonyms that can be linked to identifiers such as the legal name and/or locatability (pseudo-anonymity), from pseudonyms that can not be linked to other forms of identity knowledge (real anonymity).

According to Roger Clarke, pseudonymity is generally used to enable the protection of individuals who are at risk of undue embarrassment or physical harm[38]. He refers to celebrities and VIP’s, who are subject to widespread but excessive interest among sections of the media and the general public, to protected witnesses, people under threat from stalkers, and people in security-sensitive occupations.

In regard of pseudonymity in the electronic world, I don’t really agree with these examples of what pseudonymity generally is and where it is used. It is necessary to point out that digital identity, often typified by pseudonyms, is not always bound by the physical constraints of the body.

2.4.2. Pseudonymity in the electronic world

For the sake of convenience, digital identity emerges in the social spaces created in computer networks, most commonly known as cyberspace(s). It consists of the construction of a 'digital persona’; a self-image by which an individual presents him or herself to others. Digital identity is usually characterized as being the result of an active construction, and many believe that it provides the best opportunity to express who we really are, or who we really would like to be. The new Self is said to be multiple, distributed and fluid and, most of all, a representation of its possessor 's will[39].

On the other hand, digital identity is in many ways similar to personal identity. Firstly, digital identity, similarly to 'personal identity', is not free from the influence of its possessor's personality. In turn, personality traits are not autonomously chosen. Thus, while some may argue that the expression of 'the possessor's will' is the true expression of the self, I think that this expression is, at least, the result of a constrained personal will. Secondly, the stereotypes that guide interpersonal communication and that are principal shapers of 'personal identity’ are still present in cyberspace and, in fact, due to the lack of visual cues, these stereotypes can be even stronger in cyberspace[40]. Although digital identity is not always bound by the physical constraints of the body, it is not free from restrictions. These restrictions arise both from the necessity to use certain technologies in order to express us, and from the specificities of these predefined technologies.

The need to use certain technologies is translated in an exclusion of all those who do not have access to them, or who do not possess the expertise to create the ‘cyber-identity’ they envision. Furthermore, it is translated into limitations -due to technical constraints, such as bandwidth- in the contents that can be used to construct and express 'identity'. The specificities of the technology relate to the 'politics' of the artefact itself. For example, digital technologies are potentially control technologies, i.e., technologies that can be used to monitor the behaviour of the individual. Pseudonyms in the electronic world are frequently determined by the above reflections on digital identity.

The use of a pseudonym in the electronic world is put into practice by the use of so-called ‘digital pseudonyms’. These are public keys used to verify signatures made by the anonymous holder of the corresponding private key. A "roster", or list of pseudonyms, is created by an authority that decides which applications for pseudonyms it accepts, but is unable to trace the pseudonyms in the completed roster. The applications may be sent to the authority anonymously, by untraceable mail, for example, or they may be provided in some other way[41].

2.4.3. Pseudonymity and anonymity

It should be noticed that these forms of pseudonymity are two of the seven broad types of identity as mentioned above. It is obvious that pseudonymity is a way to be pseudo- or fully anonymous[42].

- In the event of *pseudo-anonymity*, that pseudonym is an identifier for somebody to a transaction or a communication, at first doesn’t reveal one’s identity but that is indirectly sufficient to associate the transaction or the communication with the particular human being who uses the fictitious name. This is also called *traceable pseudonymity*.

- In case of *real or full anonymity*, the pseudonym cannot be linked to any form of identity knowledge at all. This is *untraceable pseudonymity*.

Comparing to pseudonymity, anonymity means that the agent of a communication or transaction has no observable persistent characteristics. Pseudonymity, on the other hand, means that there is some characteristic associated with the agent for that communication or transaction, and that this characteristic provides a mechanism for recognizing the other communications or transactions also involving this party. Anonymity is in some sense ‘more private’ than pseudonymity, because there is less to trace[43].

3. Some aspects of anonymity

This chapter discusses some social and ethical aspects of anonymity against the background of rationales for anonymity and identifiability.

3.1. Rationales for anonymity and identifiability

Anonymity is, as said, a method for privacy protection[44]. Privacy protection is among other things, one rationale for anonymity. Gary Marx identifies a number of major rationales and contexts where anonymity or identifiability is required or permitted. His enumeration is not exhaustive but covers the most common contexts in which anonymity and identifiability are viewed as socially desirable[45].

3.1.1. Rationales in support of anonymity

Anonymity is required or permitted:

- to facilitate the flow of information and communication on public issues;
- to obtain personal information for research in which persons are assumed not to want to give publicly attributable answers or data;
- to encourage attention to the content of a message or behaviour rather than to the nominal characteristics of the messenger which may detract from that;
- to encourage reporting, information seeking, communicating, sharing and self-help for conditions that are stigmatising and/or which can put the person at a strategic disadvantage or are simply very personal;
- to obtain a resource or encourage a condition using means that involve illegality or are morally impugnable, but in which the goal sought is seen as the lesser evil;
- to protect donors of a resource or those taking action seen as necessary but unpopular from subsequent obligations, demands, labeling, entanglements or retribution;
- to protect strategic economic interests, whether as a buyer or a seller;
- to protect one's time, space and person from unwanted intrusions[46];
- to increase the likelihood that judgements and decision-making will be carried out according to designated standards and not personal characteristics deemed to be irrelevant;
- to protect reputation and assets. The "theft of identity"[47] and sending of inauthentic messages has emerged as a significant by-product of the expansion of electronically mediated (as against face-to-face) interactions;
- to avoid persecution;
- to enhance rituals, games, play and celebrations. Letting loose, pretending and playing new roles are seen as factors in mental and social health. Part of the fun and suspense of the game is not knowing who;
- to encourage experimentation and risk taking without facing large consequences, risk of failure or embarrassment since one's identity is protected;

- to protect personhood or "it's none of your business". What is central here is not some instrumental goal as with most of the above, but simply the autonomy of the person. This can be an aspect of manners and involves an expectation of anonymity as part of respect for the dignity of the person and recognition of the fact that the revelation of personal information is tied to intimacy;
- for traditional expectations. This is a bit different than the above because the custom that is honoured does not appear to have emerged from a reasoned policy decision, but rather is an artefact of the way a technology developed or the way group life evolved.

3.1.2. Rationales in support of identifiability

These contexts and rationales in support of anonymity must be balanced by a consideration of the opposite. The rationales in support of identifiability are simpler, clearer and less disputed.

Identifiability is required, expected or permitted:

- to aide in accountability;
- to judge reputation;
- to pay dues or receive just deserts;
- to aide efficiency and improve service;
- to determine bureaucratic eligibility;
- to guarantee interactions that are distanced or mediated by time and space;
- to aide research;
- to protect health and consumers;
- to aid in relationship building;
- to aid in social orientation.

Many of all these rationales of anonymity and identifiability apply as much to the real world as to the electronic world.

3.2. Social aspects of anonymity

Technology changes have profound consequences on social behaviour. For example, the development of mass-produced automobiles, made possible by the development of suburban shopping malls in the United States, which in turn led to an adolescent mall culture unimaginable in the 1920's[48]. It seems quite likely that the pervasive spread of the Internet will have equally profound effects on social organization and interactions. It should be interesting to study what is already known about the effects of anonymity as we analyse anonymity in the electronic world. The following accounts briefly review some well-established information on anonymity and social behaviour from the social psychology literature.

3.2.1. The theory of deindividuation and antisociality

In general, the findings of scientists are not encouraging for the future of the electronic world unless we can somehow avoid the known association of antisocial behaviour and anonymity.

Early studies on people in groups focused on anonymity as a root of the perceived frequency of antisocial behaviour[49]. The anonymous members of a crowd show reduced inhibition of antisocial and reckless, impulsive behaviour. They are subject to increased irritability and suggestibility.

Later social psychologists formulated a theory of deindividuation in which they proposed that one's personal sense of identity can be overwhelmed by the sense of belonging to a group. Zimbardo suggested that anonymity, diffusion of responsibility and arousal contributed to deindividuation and antisociality. He noted that deindividuated people display reduced inhibitions, reduced reliance on internal standards on their behaviour, and little self-awareness[50].

As mentioned briefly in the introductory comments for section 3.2., there is some reason to suppose that technology can contribute to the deindividuation of its users. Anonymity has been postulated in anecdotal reports to account in part for the strong contrast in behaviour of normal people who become aggressive and hostile while driving cars[51]. It seems intuitively plausible that being isolated in a tight personal space, a cocoon of glass and metal, gives some drivers a feeling of power precisely because of their (possibly temporary) anonymity. In addition, the anonymity of the other drivers may lead to a kind of dehumanisation of the other.

Similarly, Zimbardo is of the opinion that the *isolation of an Internet user* may also contribute to aggression; the object of wrath may, much like the driver of another car, be dehumanised. Possibly, writers of computer viruses and others in the criminal computer underground focus so intensely on the challenge of defeating machines that they lose sight of their human victims. Criminal hackers have expressed themselves as attacking systems, not people.

3.2.2. Anonymity and aggression

Experimental work by Zimbardo suggested that anonymity can significantly increase aggression[52]. For example, when women were asked to deliver electric shocks to victims, those who agreed to wear white lab coats and hoods administered -what they thought were- longer shocks to the alleged victims compared to women who wore their own clothes and nametags.

In a cross-cultural study, Watson analysed the correlations between the ritual, anonymizing costumes and war paint of warriors and their style of battle and post-battle treatment of prisoners[53]. He found a strong positive relationship between anonymity and brutality. These findings suggest that so-called "dark-side *hackers*" may significantly be influenced in their willingness to cause damage to computer systems and networks, precisely because their very anonymity influences them to cross normal behavioural boundaries.
These people may not be the permanently, irremediably damaged human beings they sometimes seem to be; they may be relatively normal people responding in predictable ways to the absence of stable identification and identity.

3.2.3. Anonymity, dishonesty and self-awareness

Anonymity increases the likelihood that people will transgress rules and laws. As said, the avoiding of persecution is a rationale in support of anonymity.

Anonymity changes people's normal inhibitions and influences them to behave abnormally because it seems that the deindividuation of anonymous people lowers their self-reflective propensities[54].

3.2.4. Anonymity and pro-social behaviour

The picture is not necessarily all bad. Sometimes a different context can liberate anonymous subjects from their counter-productive inhibitions. The constructive, supportive communications often seen in *discussion groups* dealing with substance abuse, abusive relationships and other personal and interpersonal problems illustrate the possible benefits of anonymity in a positive context.

3.3. Legal aspects of anonymity

For the legal aspects of anonymity I refer to the explanations of colleagues participating in the seminar project 'Anonymity on the Internet'.

3.4. Ethical aspects of anonymity

It may be clear both from the United States Constitution and from the case law held by the U.S. Supreme Court (ACLU v. Miller, McIntyre v. Ohio Elections Commission, Talley v. California, Lamont v. Postmaster General and suchlike), that anonymous publication, communications and transactions are legal and protected rights for U.S. citizens. This is the same with regard to European legislation and jurisdiction. However, the legal support for anonymity is not the only issue we must consider: even if we are legally allowed to be anonymous, is it morally a good idea?

3.4.1. Ethical issues on anonymity

There are many ways to anonymity that we consider to be 'bad uses'. Although it is not intended to discuss the good and the bad things about anonymity in this paper, the bad uses can be broken down, briefly, into a number of categories, based on the type of use or offence involved.

These are issues that generally come up in the context of *anonymous speech or communication* systems, rather than specifically in the context of *anonymous publication* systems. They include:

- Death threats: users may be able to make death threats without accountability.
- Terrorism communications: users may be able to coordinate and conspire to plan terrorist activities against the state or other organizations or individuals.
- Kidnapping communications: similarly, users might conspire and coordinate to plan kidnappings or other illegal actions.
- Spam: users might make use of the anonymous channel to spam victims with targeted advertisements or other text.
- Harassment: as opposed to targeted spam, stalkers might make directed communications intended to embarrass, defame, or threaten.
- Blackmail: users might publish material without disclosing the key, and then threaten to publicize the location of the material.

These issues are addressed in a broader scope by other organizations, such as the Cato Institute[55], Amnesty International and the Electronic Frontier Foundation[56]. I refer to the literature of these organizations.

Another topic that is related to free and anonymous speech is the question as to whether making speech anonymous decreases the *credibility of its content*.

An issue with substantial impact on society and economics is the fact that anonymous communication, and indeed also anonymous publication, can be used to share documents in a way that violates *copyright or patent laws*, or exposes *trade secrets*. Recent issues, for example the distribution of PGP being restricted due to patent issues, show that these laws contain a number of controversial issues.

On the other hand, more clear-cut cases such as copying a band's music in violation of the band's copyright and wishes are very prevalent, and becoming even more common.

3.4.2. The need of ethical rules for policy guidelines

Gary Marx presents 13 procedural questions to guide the development and assessment of any Internet policy regarding anonymity. The key issue for ethics and public policy is the question under what conditions it is right or wrong to favour anonymity or identifiability. There are many contexts in which most people would agree that some form of anonymity or identifiability is desirable. But there are others where we encounter a thicket of moral ambiguity and competing rationales and where a balancing act may be called for[57].

3.5. Technological aspects of anonymity

I refer to the explanations of Peter Rigole, a colleague participating in the seminar project 'Anonymity on the Internet'[58], for the technological aspects of anonymity.

4. Anonymity in the electronic world

The foregoing accounts centred upon some essential notions within the scope of the definition of ‘anonymity’ and its aspects. These were the foundations to concentrate on the undermentioned characteristics of anonymity in the electronic world.

4.1. Real world versus electronic world

Before making an exploration of anonymity in the electronic world, it will be helpful to establish some common explanation of the terms *real world* and *electronic world*.

4.1.1. Anonymity in the real world

The *real world* refers to the material and physical world of everyday human interactions. Using ‘real world’ in this way is not intended to insinuate that the electronic world is less significant, useful or even ‘real’ than the worldly level on which we interact; it is only a convenient reference to distinguish the physical from the electronic.

Anonymity in the real world is *the absence of a real world identity*. Some authors define it simply as being without a name or with an unknown name. As suggested above, this ‘namelessness’ is not enough to be anonymous.

The term ‘anonymity’ in the real world is imbued with a negative connotation. Nevertheless, anonymity has an honourable history in world philosophy and politics. Anonymity is not inherently linked to antisocial behaviour[59].

4.1.2. Anonymity in the electronic world

In this paper the *electronic world*, also called ‘cyberspace’, refers to the totality of electronic data storage and transmission; this paper focuses on communications and transactions using the Internet.

Anonymity in the electronic world is *the absence of (digital) identity*. Identity on the Internet is primarily the e-mail address[60]. The e-mail address sometimes provides for crude and unreliable information about affiliation and geographic location via e.g. domain names. Roger Clarke has written an excellent introduction on the question what is meant by identity in the electronic world[61]. Another well-known author on this subject is ‘L. Detweiler’[62]; it is still unknown whether this is a real name or not. Detweiler suggests that identity on the Internet is amorphous and unstable because there is no one-to-one relationship between people and e-mail addresses.

One person may use multiple e-mail addresses and many people may share a single address. I also refer to what has been stated above with regard to identity in the electronic world[63].

I would like to remark that the fluidity of identity on the *Internet* is one of its most attractive features. It simplifies the use of anonymous communications or transactions[64]. This belongs to the qualities of the Internet as a unique communication and transaction medium.

The Internet is, as an essential part of the electronic world, really a network of networks and is comprised of a number of different technologies and infrastructures. Viewed as a whole, it is uniquely:

- *Global*: The Internet provides immediate access to information from around the world. With simple e-mail, it is easy to send a message to anybody on earth. Through the World Wide Web, millions of information sources are available from around the world.

- *Decentralized*: The Internet was designed by purpose to be decentralized. The absence of gatekeepers, the availability of numerous hosting sites and the irrelevance of geographic location mean that material can almost always be published outside the control of governments, monopolies or oligopolies.

- *Open*: The Internet has low barriers to access. Service can be priced very inexpensively. The costs of creating and disseminating content are extremely low. Because of the Internet, anybody who has a computer and a modem can be a publisher.

- *Abundant*: The digitisation of information and the ability to transmit it over the telephone network, combined with the decentralized nature of the Internet, mean that the Internet has essentially unlimited capacity to hold information. In economic terms, the marginal cost of adding another website, sending another e-mail message, or posting to a newsgroup is essentially zero.

- *Interactive*: The Internet is designed for bi-directional communication: all Internet users can be both speakers and listeners. The Internet allows responsive communication from one-to-one, from one-to-many, and from many-to-one.

- *User-controlled*: The Internet allows users to exercise far more choice than even cable or television or short wave radio. The user can skip from site to site in ways that are not dictated by the content providers or by the access provider. Users can control what content reaches their computers. Users can encrypt their communications to hide them from government censors.

- *Infrastructure independent*: The Internet is not linked to any infrastructure other than the telephone system. Dial-up access is available from any telephone that can make an international call. Access to the Internet can also be wireless and satellite based and therefore further removed from effective control of governments.

The above is an outline to illustrate the unique features of the Internet as an essential part of the electronic world. This reasonably exhaustive list is almost entirely copied from a publication of the Global Internet Liberty Campaign[65].

4.2. The importance of anonymity in the electronic world

According to Detweiler “anonymity is a powerful tool that can be beneficial or problematic depending on its use. Arguably absence of identification is as important as the presence of it. It may be the case that many strong benefits from electronic anonymity will be discovered that were unforeseen and unpredicted, because true anonymity has been historically very difficult to establish”.

> One can use anonymity to make personal statements to a colleague that would sabotage a relationship if stated openly (such as employer/employee scenarios). One can use it to pass information and evade any threat of direct retribution. For example, `whistleblowers' reporting on government abuses (economic, social, or political) can bring issues to light without fear of stigma or retaliation. Sensitive, personal, potentially damaging information is often posted to some USENET groups, a risky situation where anonymity allows conversations to be carried on completely independent of the identities of the participants. Some police departments run phone services that allow anonymous reporting of crimes; such uses would be straightforward on the network. Anonymity can be extremely important and potentially lifesaving diagnoses and discussions carried out on medical or therapeutic newsgroups. Unfortunately, extortion and harassment become more insidious with assurances of anonymity[66].

4.3. Threats to anonymity in the electronic world

Nowadays, there are many threats to anonymity in the electronic world. Organizations and authorities keep personal data in *information databases*. This causes a threat of unauthorised access to personal information, which is a risk for personal privacy.

Another threat arises from the significant emergence of *electronic communication* such as e-mail, newsgroups, chat, etc. The biggest privacy risk is that somebody monitors or even manipulates this communication.

A third threat to anonymity in the electronic world is *transaction monitoring* and *extraction of additional information*. Most electronic transactions are logged. In addition to this, many personal data can be stored.

Most electronic services require the user to identify him. The demands for *identification and authentication* obstruct the desire to be anonymous and thus the desire to protect privacy. Moreover, the Internet creates opportunities for identity theft, as it is easier to copy or to fake identities in the electronic world. The problem is that this causes great harm to the person whose identity is stolen.

The electronic world creates a more efficient *marketing* through the fact that marketeers and advertisers use the electronic facilities to gather personal data and to monitor prospective customers' preferences. On the basis of the gathered data, they send marketing mails, for the greatest part *spam mails*. Usually they fake the sender's address, so that it is almost impossible to trace back to the real sender.

Positioning and location based services pose an actual threat to a user's privacy. In the near future they will allow to locate all mobile communication systems[67].

4.4. Methods for improving anonymity in the electronic world

In spite of the many threats to anonymity, the new information technology also brought new methods for protecting persons who want to remain anonymous. There are both technical and non-technical methods. Below, I represent a brief list[68], given that my colleagues have specified most of these methods as part of the seminar project on 'Anonymity on the Internet'.

4.4.1. Technical methods

- *Cryptography*: to prevent unauthorized access to personal data, these data should be encrypted. Public key cryptography can be used to protect the content of messages. Digital signatures are used to guarantee the addressee from altered messages. Cryptography of data and communication channels guarantee some level of privacy but the user is not anonymous.

- *Anonymous remailers*: these enable users to send e-mails and to use news services without revealing their identity. This implies that the original message headers are altered.

- *Anonymous web browsing*: this allows the user to browse the World Wide Web without revealing the IP-number[69] or other information about the user to the web server. This provides some level of anonymity, since headers containing information about the user are removed.

- *Anonymous electronic money*: some systems or services enable anonymous payments by using blind signatures.

- *Anonymous authorisation and authorisation certificates*: public key certificates bind a public key to the name or some other identification of the key holder. The credential or accountability is based on the identity of the user.

- *Privacy-protective infrastructure*: The World Wide Web consortium has been working on a privacy-protective infrastructure called Platform for Privacy Preferences (P3P) that enables web sites to specify the use of data and disclosure practices. This platform also enables web-users to specify their expectations concerning personal data disclosure practices. Additionally, P3P enables more or less automatic negotiation of the exchange of personal data between the web site and the user. So, P3P tries to model a privacy policy negotiation mechanism, where a negotiation can be conducted for each piece of private information[70].

4.4.2. Non-technical methods

Besides the technical methods, there are also several non-technical methods to protect anonymity. By this I understand:

- the use of different identities and inconsistent misinformation;
- the indirect spread of information about existing privacy threats;
- different kinds of privacy self-regulation programs;
- regulation by laws;
- the use of different systems on different locations.

4.5. Types of anonymity

4.5.1. Agent-related types of anonymity

There are, in general, several agents in an anonymous communication or transaction system: these include the author, the addressee and the server. I address each of these agents separately, in order to try to discuss some types of anonymity. This matter is for the greater part borrowed from Roger Dingledine's explanations within the scope of his thesis on the design and deployment of an anonymous 'secure data haven'[71].

4.5.1.1. Author-anonymity

> Author-anonymity means that the original author of a given document should not be known. This characteristic of anonymity is one of the integral parts of almost any anonymous network or service. Even so-called 'anonymous remailers', which are simply anonymous forwarders and don't support persistence or storage of the data, provide author-anonymity.

4.5.1.2. Publisher-anonymity

While author-anonymity addresses the original author of the document itself, publisher-anonymity addresses the agent that originally introduces the document into the system. In some cases the author and the publisher may be the same identity, but in the general case the author may make use of a separate individual, either a third party or a server in the system, to introduce the document. Separating these two notions of 'origin' makes it clearer what protections the system provides.

4.5.1.3. Reader-anonymity

Reader-anonymity means that readers requesting a document should not have to identify themselves to anyone. In particular, this means that when a reader performs a document request at a given server, this server is unable to determine the identity or location of the reader. This class of anonymity is crucial for protecting people from disclosing that they are interested in or accessing certain types of material. Reader-anonymity ensures the privacy of the vast majority of the system users, a concern which is often ignored.

4.5.1.4. Server-anonymity

Server-anonymity means that the location of the document should not be known or knowable. Specifically, given a document's name or other identifier, an adversary is no closer to knowing which server or servers on the network currently possess this document (or shares it). This restriction implies that the retrieved documents do not provably pass through any given server that receives a request. This protection is crucial for materials where mere possession is cause for action against the server.

4.5.1.5. Document-anonymity

Document-anonymity means that the server does not know the contents of the document that is storing or helping to store. This is broken down into two scenarios. Isolated-server document-anonymity means that if the server is allowed to look only at the data that it is storing, it is unable to figure out the contents of the document. Generally this is achieved via some sort of secret sharing mechanism, either sharing the document or sharing the key for recreating the document. Generally this is achieved via some sort of secret sharing mechanism, either sharing the document or sharing the key for recreating the document (or both) across servers. On the other hand, connected-server document-anonymity means that the server is allowed to communicate and compare data with all other servers in the system, but is still unable to determine the contents of the document. Since a connected server may well be able to act as a reader and do a document request itself, it seems that connected-server document-anonymity is difficult to achieve without some trusted party acting as intermediary and authenticating and authorizing readers. Notice that merely encrypting the document before publishing it into the system is not sufficient to achieve document-anonymity: we are concerned here not with confidentiality of the published document, but instead with whether the given server can recreate the bits that were inserted into the system.

4.5.1.6. Query-anonymity

Query-anonymity refers to the notion that over the course of a given document query or request, the 'identity' of the document itself is not revealed to the server. In short, this means that although a server may have many different documents stored, which document was served for a given request is not knowable by the server.

4.5.2. Types of anonymity related to the characteristics of a communication

The agent of a communication has control on whether to publish his speech over a given channel, based on the characteristics of that particular channel. The speaker might tailor his speech, or choose not to speak at all, based on the level of protection provided by that channel and the choices he makes about his anonymity. This explanation is also based on Roger Dingledine's rather technical viewpoints.

4.5.2.1. Computational vs. information-theoretic Anonymity

The distinction between *computational* and *information-theoretic* anonymity depends on the notion of how protected a given address is: 'does it rely on computational complexity to protect its anonymity, or does it use some other technique to make the address unknowable even in the face of a computationally powerful adversary?'[72]. An alternative to computational anonymity is that an adversary has the transcript of a particular communication but is still unable to break its anonymity. This is what is called information-theoretic anonymity.

4.5.2.2. Perfect forward anonymity

Perfect forward anonymity means that when a particular transaction is done, there is nothing new that the adversary can get that helps him identify the location or identity of either of the communicating parties[73].

4.5.3. Main types of anonymity

Finally, there are types of anonymity that are not really related to the agents or the characteristics of a communication or a transaction. It concerns the main distinction between *data anonymity* and *connection anonymity*. In data anonymity, data flowing over a connection do not reveal an identity. In connection anonymity, the connection itself does not reveal an identity, and the vulnerability is traffic analysis. For more on this subject, I refer to the explanations of my colleague Peter Rigole[74].

Pfitzmann and Waidner describe three main types of anonymous communication properties: *sender anonymity*, *receiver anonymity* and *unlinkability* of sender and receiver. Sender anonymity means that the identity of the party who sent a message is hidden, while the receiver (and the message itself) might not be hidden. Receiver anonymity similarly means that the identity of the receiver is hidden. Unlinkability of sender and receiver means that though the sender and receiver can each be identified as participating in some communication, they cannot be identified as communicating with each other[75].

4.6. Levels of anonymity

The level of anonymity you have is, as mentioned above, a result of the choices you make about your privacy. Given that privacy is not the only rationale of anonymity, it is obvious that the level of anonymity is also a result of the choices made in function of other rationales.

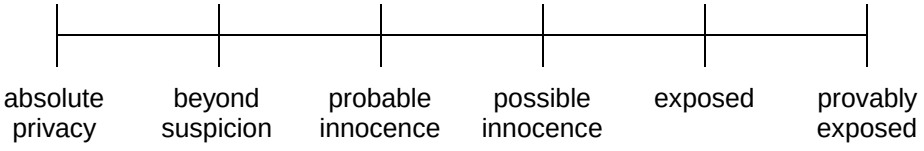
For convenience, there are as much levels of anonymity as there are levels of identity. Anonymity is one polar value of a broad dimension of identifiability versus non-identifiability. To be fully anonymous means that a person cannot be identified according to any of the seven broad types of identity knowledge discussed above[76].

4.6.1. Degrees of anonymity

Developing a system to protect privacy while browsing the World Wide Web, Mike Reiter and Avi Rubin introduced the idea of *degrees of anonymity* as an important tool for describing and proving anonymity properties. They argue that 'the degree of anonymity provided against an attacker can be viewed as a continuum, ranging from no anonymity to complete anonymity and having several interesting points in between'[77]. In addition, they informally define these intermediate points, and for their project, they refine these definitions and proofs to yield insights into proving anonymity properties for other approaches.

They describe the degree of anonymity as an informal continuum. This can obviously be extended to receiver anonymity and unlinkability as well.

> On the one end of the spectrum, absolute privacy is found: absolute sender privacy against an attacker means that the attacker can in no way distinguish the situations in which a potential sender actually sent communication from situations in which he did not. Sending a message results in no observable effects for the attacker. On the other end of the spectrum is provably exposed: the identity of the sender is provably exposed if the attacker cannot only identify the sender of a message, but can also prove the identity of the sender to others.



For the purposes of their paper, Reiter and Rubin discuss the following three intermediate points of this spectrum, listed below from strongest to weakest.

- *Beyond suspicion*: A sender's anonymity is beyond suspicion if though the attacker can see evidence of a sent message, the sender appears no more likely to be the originator of that message than any other potential sender in the system.
- *Probable innocence*: A sender is probably innocent if, from the attacker's point of view, the sender appears no more likely to be the originator than to not be the originator. This is weaker than beyond suspicion in that the attacker may have reason to expect that the sender is more likely to be responsible than any other potential sender, but it still appears at least as likely that the sender is not responsible.
- *Possible innocence*: A sender is possibly innocent if, from the attacker's point of view, there is a nontrivial probability that the real sender is someone else.

It is possible to describe these intermediate points for receiver anonymity and sender or receiver unlinkability, as well.

Which degree of anonymity applies to a particular communication or transaction depends on the agent and the context. The default degree of anonymity on the web for most information and attackers is *exposed*. All recent versions of Internet browsers are configured to automatically identify the client computer to web servers, by passing information including the IP addresses[78] and the host platform in request headers.

4.6.2. Gradations of anonymity

In an exploration of the legal implications of anonymity, Grijpink and Prins emphasize the significance of the distinction between various gradations of anonymity, which is important to evaluate these legal implications[79]. They make a distinction between:

- completely anonymous transactions, whether or not with the use of a *self-chosen* pseudonym (no traces that make it possible to establish someone's identity);
- spontaneous semi-anonymous legal transactions, whether or not with the use of a *self-chosen* pseudonym (there are traces that make it possible to establish someone's identity);
- organised semi-anonymous legal transactions with the use of a pseudonym *issued by a third party*;
- spontaneous personalised transactions using unverified or unverifiable identifying personal details;
- organised personalised transactions with the use of identifying personal details with which an authorised third party can verify the accuracy of the identifying personal details.

Grijpink and Prins state that the determinative factor of this division is first and foremost the use of a pseudonym that does or does not leave traces that make it possible to find out who is using the pseudonym[80].

Some paragraphs further in their paper, Grijpink and Prins underline that there are, in addition to *complete anonymity*, also forms of *semi-anonymity*. It is clear that these notions are analogous to the above-mentioned distinction between pseudo-anonymity and full or real anonymity[81]. However, they note that where people speak of anonymity, they essentially mean semi-anonymity. Electronic communications or transactions can, after all, be traced and verified 'if necessitated by the circumstances, the law or the court'.

Remark:

Many authors use different names for similar or analogue notions. The list below is a selection of these notions.

Full anonymity	Partial anonymity
Complete anonymity	Semi-anonymity
Real anonymity	Pseudo-anonymity
Untraceable anonymity	Traceable anonymity
Unlinkable anonymity	Linkable anonymity
Absolute anonymity	Relative anonymity
Unobservability	Observability
Unidentifiability	Identifiability

4.6.3. Traceable anonymity and untraceable anonymity

Electronic anonymity can be 'traceable' or 'untraceable'. This distinction is explained in the paper of my colleague Stacey Smits, participating in the seminar project 'Anonymity on the Internet', so that I refer to her statements[82]. Similar explanations can be read in the publications of Michael Froomkin[83].

4.6.4. Levels of anonymity

Bill Flinn and Hermann Maurer, both computer scientists, make an attempt at systematically investigating levels of anonymity required in networked computer systems. 'Applications of modern computer networks require a rethinking of how anonymous users should be for various applications'. They give an overview of six -including level 0- possible levels.

- Level 0: *No identification*

  In this level there is no identification of the user of a computer system. This involves the complete absence of the identity of the user.

- Level 1: *Anonymous identification*

  This is the level in which the user is identified by the system, but not as a specific individual and thus not 'addressable'.

- Level 2: *Pen-name identification* or pseudonym identification

  The user is known within the system by some user-name, but there is no proper identification of the user as person.

- Level 3: *Latent (potential) identification*

  Here the user is known to the system. Each user may develop a set of pseudonyms. Distinct users cannot directly identify other users using the computer system; however, the system has exact knowledge of each user.

- Level 4: *Usual identification*

  The user is known within the system by a user-name and associated password. Nowadays, most multiple user systems use this in actual practice.

- Level 5: S*uper-identification*

  The user must be authenticated[84], or in other words be identified uniquely to the system in a completely secure way. This requires in fact zero anonymity.

It is obvious that these levels are analogous to the statements on the degrees and the gradations of anonymity described above. However, some explanations involve balanced approaches to the different levels of anonymity in the main.

5. Conclusion

Anonymity is, as it is generally acknowledged, the absence of identity. It is a method of privacy protection and thus a part of privacy. The concept of anonymity becomes increasingly significant regarding privacy protection in electronic services. The fluidity of identity on the Internet simplifies anonymous communications and transactions. Many strong benefits from electronic anonymity are discovered though there are many threats to this anonymity. It is a trying task to decide what is legal or who should be held responsible for anonymous communications and transactions. The discussion on the aspects of anonymity in the electronic world may result in a good understanding of the concept, with a view to guide the development and assessment of any Internet policy regarding anonymity.

Endnotes

[1] 'Information privacy' involves the interest of an individual to control information about himself. See CLARKE, R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1997, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.
[2] FROOMKIN, M., "Anonymity and Its Enmities", *The Journal of Online Law*, 1995, article 4, par. 3, <http://www.wm.edu/law/publications/jol/froomkin.html>.
[3] However good or prestigious a dictionary, none of all dictionaries is ultimately 'authoritative': whatever 'authority' any dictionary has is attributable only to the skill and diligence of the men and women who compiled it.
[4] Webster's Ninth New Collegiate Dictionary, Springfield MA, 1991, <http://www.m-w.com/dictionary.htm>.
[5] See etymological explanation in Webster's Ninth New Collegiate Dictionary, *o.c.*, search for 'anonymity' and 'anonymous'.
[6] As stated below with regard to the concept of 'identity'.
[7] This follows obviously from the original, and even etymological, meaning of 'definition'.
[8] DETWEILLER L., *Identity, Privacy and Anonymity on the Internet*, 1993, <http://www.eserver.org/Internet/Identity-Privacy-Anonymity.txt>.
[9] Webster's Ninth New Collegiate Dictionary, *o.c.*, search for 'identity'.
[10] A recent attempt to deal with this fact of life can be found in the proposal for a Simple Distributed Security Infrastructure (SDSI) of Ronald L. Rivest; RIVEST, R., L., *A Simple Distributed Security Infrastructure*, 1996, <http://theory.lcs.mit.edu/~rivest/sdsi11.html>.
[11] As stated below, 'identity in the real world' must be distinguished from 'identity in the electronic world' or 'digital identity'.
[12] COVELL, P., *Digital Identity in Cyberspace*, 1998, <http://cyber.law.harvard.edu/courses/ltac98/white-paper.html>.
[13] Also see below: 3.1.1. Rationales for anonymity.
[14] CLARKE, R., *Computer Matching and Digital Identity*, 1993, <http://www.anu.edu.au/people/Roger.Clarke/DV/CFP93.html>.
[15] See: 2.4. Pseudonymity.
[16] For more about identity as a commodity, read COVELL, P., *Digital Identity in Cyberspace*, 1998, <http://cyber.law.harvard.edu/courses/ltac98/white-paper.html>.
[17] Its computing infrastructure must be designed to help its users spot competitive threats and opportunities, and quickly organize responses.
[18] *Knowledge management* stands for the Information flow and relationships among workers within a company; *e-commerce* is about the relationships to customers and business partners; *business operations* are the internal business processes.
[19] See COVELL, P., *o.c.*, 1998, <http://cyber.law.harvard.edu/courses/ltac98/white-paper.html>. Authentication, integrity and non-repudiation are, on further consideration, second-rate functions of digital identity. The most natural function of digital identity is identification, nuancing RIGOLE, P., *Technological*

Aspects of Anonymity on the Internet, Seminar paper, 2001, <http://www.student.kuleuven.ac.be/~m9606335/technicalside.html>.

[20] Roger Clarke is a Visiting Fellow at the Faculty of Engineering and Information Technology of the Australian National University, <http://www.anu.edu.au/people/Roger.Clarke/>.

[21] CLARKE, R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1997, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

[22] See: 2.2.3. Identity and anonymity; 2.3.1. Definition and dimensions of privacy.

[23] SMITS, S., *Anonymous E-mail?*, Seminar paper, KULeuven, 2001; DETWEILER, L., *Identity, Privacy, and Anonymity on the Internet*, 1993, <http://www.eserver.org/internet/Identity-Privacy-Anonymity.txt>.

[24] A network *protocol* is the set of very detailed rules, sequences, message formats, and procedures that computer systems use and understand when exchanging data with each other. The most fundamental protocol is called 'Internet Protocol' (IP). IP is responsible for transmitting each chunk of data from one system to another. What is of more interest is the location on the network of the systems that IP uses to send chunks of data back and forth. Each computer system uses an IP address.

[25] SMITH, R., *The IP Address: Your Internet Identity*, 1998, <http://consumer.net/IPpaper.asp>.

[26] For the analogous levels of anonymity in the electronic world, see: 4.6.4. Levels of anonymity.

[27] MARX, G. T., *What's in a Name? Some Reflections on the Sociology of Anonymity*, 1999, <http://web.mit.edu/gtmarx/www/anon.html>.

[28] All types below are listed by Gary Marx; MARX, G. T., *o.c.*, <http://web.mit.edu/gtmarx/www/anon.html>.

[29] See: 2.4. Pseudonymity.

[30] See: 2.4. Pseudonymity.

[31] See: 2.2.1. Definition of ‘identity’.

[32] Information privacy involves the interest of an individual to control information about himself.

[33] CLARKE, R., *o.c.*, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

[34] These distinctions between the dimensions of privacy are described by Roger Clarke, CLARKE, R., *o.c.*, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

[35] KORKEA-AHO, M., *Anonymity and Privacy in the Electronic World*, 1999, <http://www.hut.fi/~mkorkeaa/doc/anonpriv.html>.

[36] CLARKE, R., *o.c.*, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

[37] Also see: 2.2.3. Identity and anonymity.

[38] CLARKE, R., *o.c.*, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

[39] For more about this read STONE, A., R., *The war of desire and technology*, Cambridge, MA, MIT Press, 1996; TURKLE, S., *Life on the screen: identity in the age of the internet*, New York, Touchstone, 1995.

[40] WALLACE, P., *The psychology of the Internet*, Cambridge, UK, Cambridge University Press, 1999.

[41] CHAUM, D., “Untraceable electronic mail, return addresses, and digital pseudonyms”, *Communications of the ACM*, 1981, 24/2 84-88;

<http://world.std.com/~franl/crypto/chaum-acm-1981.html>.
[42] Also see: 2.2.3. Identity and anonymity.
[43] DINGLEDINE, R., *The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven*, MIT Master's Thesis, 2000, <http://www.freehaven.net/papers.html/doc/freehaven.ps>.
[44] See above: 2.3.3. Anonymity and privacy.
[45] Cf.: 2.2.3. Identity and anonymity; MARX, G. T., *o.c.*,<http://web.mit.edu/gtmarx/www/anon.html>.
[46] Cf. 'privacy protection' explained in: 2.3.2. Privacy in the electronic world.
[47] Also see: 2.2.1. Definition of 'identity'.
[48] FROOMKIN, M., "Anonymity and Its Enmities", *The Journal of Online Law*, 1995, article 4, par. 3, <http://www.wm.edu/law/publications/jol/froomkin.html>.
[49] Also read LE BON, G., *The crowd: A study of the popular mind*, Macmillan, New York, 1896.
[50] See ZIMBARDO, P. G., *The human choice: individuation, reason and order versus deindividuation, impulse, and chaos*, Arnold, W. J. & D. Levine, eds, *Nebraska Symposium on* Motivation, University of Nebraska Press (Lincoln), 1969.
[51] RUSSELL, J. J., 'The new menace on the road', *Good Housekeeping*, 224(4):100-10, 1997.
[52] See ZIMBARDO, P. G., *The human choice: individuation, reason and order versus deindividuation, impulse, and chaos*, Arnold, W. J. & D. Levine eds, Nebraska Symposium on Motivation, University of Nebraska Press (Lincoln), 1969.
[53] See WATSON, R., I. Jr, "Investigation into deindividuation using a cross-cultural survey technique", *Journal of Personality and Social Psychology*, 1973, 25:342-345.
[54] To know more about the *theory of deindividuation*: ZIMBARDO, P. G., *The human choice: individuation, reason and order versus deindividuation, impulse, and chaos*, Arnold, W. J. & D. Levine, eds, Nebraska Symposium on Motivation, University of Nebraska Press (Lincoln), 1969; to know more about *honesty in the electronic world* see MARX, G. T., *o.c.*, 1999, <http://web.mit.edu/gtmarx/www/anon.html>.
[55] Their papers include "Nameless in Cyberspace: Anonymity on the Internet", a briefing paper addressing anonymous speech on the Internet. WALLACE, J., D., *Nameless in Cyberspace: Anonymity on the Internet*, 1999, <http://www.cato.org/pubs/briefs/bp-054es.html>.
[56] See website at http://www.eff.org.
[57] MARX, G. T., *o.c.*, 1999, <http://web.mit.edu/gtmarx/www/anon.html>.
[58] RIGOLE, P., *Technological Aspects of Anonymity on the Internet*, Seminar paper, 2001, <http://www.student.kuleuven.ac.be/~m9606335/technicalside.html>.
[59] See: 3.2.4. Anonymity and pro-social behaviour.
[60] See DETWEILER, L., *o.c.*,<http://www.eserver.org/internet/Identity-Privacy-Anonymity.txt>.
[61] CLARKE, R., *o.c.*, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.
[62] DETWEILER, L., *o.c.*, <http://www.eserver.org/internet/Identity-Privacy-Anonymity.txt>.
[63] See: 2.2.2. Identity in the electronic world.
[64] See FROOMKIN, M., "Anonymity and Its Enmities", *The Journal of Online Law*, 1995, article 4, par. 7, <http://www.wm.edu/law/publications/jol/froomkin.html>.

[65] DEMPSEY, J., *Regardless of Frontiers*, <http://www.gilc.org/speech/report/>.
[66] DETWEILER, L., *o.c.*, <http://www.eserver.org/internet/Identity-Privacy-Anonymity.txt>.
[67] Cf. the FCC E911 mandate in the U.S., put into practice in case of an emergency as from October 2001.
[68] Based on the enumeration of methods by KORKEA-AHO, M., *o.c.*, <http://www.hut.fi/~mkorkeaa/doc/anonpriv.html>.
[69] See: 2.2.2.2. Forms of digital identity; also read endnote 24.
[70] Quoting KORKEA-AHO, M., *o.c.*, <http://www.hut.fi/~mkorkeaa/doc/anonpriv.html>.
[71] DINGLEDINE, R., *o.c.*, <http://www.freehaven.net/papers.html/doc/freehaven.ps>.
[72] DINGLEDINE, R., *o.c.*, <http://www.freehaven.net/papers.html/doc/freehaven.ps>.
[73] DINGLEDINE, R., *o.c.*, <http://www.freehaven.net/papers.html/doc/freehaven.ps>.
[74] RIGOLE, P., *Technological Aspects of Anonymity on the Internet*, Seminar paper, 2001, <http://www.student.kuleuven.ac.be/~m9606335/technicalside.html>.
[75] PFITZMANN, A., and WAIDNER, M., "Networks without user observability", *Computers & Security 2*, 1987, 6, 158-166.
[76] MARX, G. T., *o.c.*, 1999, <http://web.mit.edu/gtmarx/www/anon.html>.
[77] REITER, M., RUBIN, A., *Crowds: Anonymity for Web Transactions*, 1999, <http://www.research.att.com/projects/crowds/papers/j8.ps.gz>.
[78] See: 2.2.2.2. Forms of digital identity; also read endnote 24.
[79] GRIJPINK, J. and PRINS, C., *New legal rules for anonymous electronic legal transactions? An exploration of the legal implications of digital anonymity*, unpublished translation of the dutch text entitled *Nieuwe rechtsregels voor anoniem elektronisch rechtsverkeer? Een verkenning van de privaatrechtelijke gevolgen van digitale anonimiteit*, 2001, <http://rechten.kub.nl/prins/Publicatnl/ntbr1.pdf>.
[80] See: 2.4. Pseudonymity.
[81] See: 2.4.3. Pseudonymity and anonymity.
[82] SMITS, S., *Anonymous E-mail?*, Seminar paper, KULeuven, 2001.
[83] FROOMKIN, M., "Anonymity and Its Enmities", *The Journal of Online Law*, 1995, article 4, par. 7, <http://www.wm.edu/law/publications/jol/froomkin.html>; FROOMKIN, M., "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases", *Pittsburgh Journal of Law and Commerce*, 1996, 395, <http://www.law.miami.edu/~froomkin/articles/ocean.htm>.
[84] For 'authentication' see: 2.2.2.1. Functions of digital identity.