

Anonymity on the Internet

By Jacob Palme <jpalme@dsv.su.se> and Mikael Berglund¹

Abstract

How is anonymity used on the Internet? How anonymous is an Internet user, and how can an Internet user achieve anonymity? What are the pros and cons of anonymity on the Internet? Is anonymity controlled by laws specially directed at regulating anonymity? How should laws on anonymity in the Internet be constructed? Should the EU establish a common directive on how anonymity is to be handled in the member states?

File name: anonymity.pdf

This document in HTML format:

<http://dsv.su.se/jpalme/society/anonymity.html>

This document in PDF format:

<http://dsv.su.se/jpalme/society/anonymity.pdf>

Latest change: 04-12-22 10.47

Types of Anonymity

In this paper, the word “message” is used to designate any communication unit (e-mail, newsgroup article, web page, pamphlet, book, rumour, etc.)

Anonymity means that the real author of a message is not shown.

Anonymity can be implemented to make it impossible or very difficult to find out the real author of a message.

A common variant of anonymity is pseudonymity, where another name than the real author is shown. The pseudonym is sometimes kept very secret, sometimes the real name behind a pseudonym is openly known, such as *Marc Twain* as a pseudonym for *Samuel Clemens* or *Ed McBain* as a pseudonym for *Evan Hunter*, whose original name was *Salvatore A. Lombino*. A person can even use multiple different pseudonyms for different kinds of communication.

An advantage with a pseudonym, compared with complete anonymity, is that it is possible to recognize that different messages are written by the same author. Sometimes, it is also possible to write a letter to a pseudonym (without knowing the real person behind it) and get replies back. It is even

¹ This paper was written by Jacob Palme, using much material from the paper “Usenet news and anon.penet.fi” by Mikael Berglund.

possible to have long discourses between two pseudonyms, none of them knowing the real name behind the other's pseudonym. A disadvantage, for a person who wants to be anonymous, is that combining information in many messages from the same person may make it easier to find out who the real person is behind the pseudonym.

A variant of pseudonymity is deception [Donath 1996], where a person intentionally tries to give the impression of being someone else, or of having different authority or expertise.

Anonymity before the Internet

Anonymity is not something which was invented with the Internet. Anonymity and pseudonymity has occurred throughout history. For example, William Shakespeare is probably a pseudonym, and the real name of this famous author is not known and will probably never be known.

Anonymity has been used for many purposes.

A well-known person may use a pseudonym to write messages, where the person does not want people's preconception of the real author color their perception of the message.

Also other people may want to hide certain information about themselves in order to achieve a more unbiased evaluation of their messages. For example, in history it has been common that women used male pseudonyms, and for Jews to use pseudonyms in societies where their religion was persecuted.

Anonymity is often used to protect the privacy of people, for example when reporting results of a scientific study, when describing individual cases.

Many countries even have laws which protect anonymity in certain circumstances. Examples:

A person may, in many countries, consult a priest, doctor or lawyer and reveal personal information which is protected. In some cases, for example confession in catholic churches, the confession booth is specially designed to allow people to consult a priest, without seeing him face to face.

The anonymity in confessional situations is however not always 100 %. If a person tells a lawyer that he plans a serious crime, some countries allow or even require that the lawyer tell the police. The decision to do so is not easy, since people who tell a priest or a psychologist that they plan a serious crime, may often do this to express their feeling more than their real intention.

Many countries have laws protecting the anonymity of tip-offs to newspapers. It is regarded as important that people can give tips to

newspapers about abuse, even though they are dependent on the organization they are criticizing and do not dare reveal their real name.

Advertisement in personal sections in newspapers are almost always signed by a pseudonym for obvious reasons.

Is Anonymity Good or Bad?

In summary, anonymity and pseudonymity can be used for good and bad purposes. And anonymity can in many cases be desirable for one person and not desirable for another person. A company may, for example, not like an employee to divulge information about improper practices within the company, but society as a whole may find it important that such improper practices are publicly exposed.

Good purposes of anonymity and pseudonymity:

- + People dependent on an organization, or afraid of revenge, may divulge serious misuse, which should be revealed. Anonymous tips can be used as an information source by newspapers, as well as by police departments, soliciting tips aimed at catching criminals. Everyone will not regard such anonymous communication as good. For example, message boards established outside companies, but for employees of such companies to vent their opinions on their employer, have sometimes been used in ways that at least the companies themselves were not happy about [Abelson 2001]. Police use of anonymity is a complex issue, since the police often will want to know the identity of the tipper in order to get more information, evaluate the reliability or get the tipper as a witness. Is it ethical for police to identify the tipper if it has opened up an anonymous tipping hotline?
- + People in a country with a repressive political regime may use anonymity (for example Internet-based anonymity servers in other countries) to avoid persecution for their political opinions. Note that even in democratic countries, some people claim, rightly or wrongly, that certain political opinions are persecuted. [Wallace 1999] gives an overview of uses of anonymity to protect political speech. Every country has a limit on which political opinions are allowed, and there are always people who want to express forbidden opinions, like racial agitation in most democratic countries.
- + People may openly discuss personal stuff which would be embarrassing to tell many people about, such as sexual problems. . Research shows that anonymous participants disclose significantly more information about themselves [Joinson 2001].

- + People may get more objective evaluation of their messages, by not showing their real name.
- + People are more equal in anonymous discussions, factors like status, gender, etc., will not influence the evaluation of what they say.
- + Pseudonymity can be used to experiment with role playing, for example a man posing as a woman in order to understand the feelings of people of different gender.
- + Pseudonymity can be a tool for timid people to dare establish contacts which can be of value for them and others, e.g. through contact advertisements.

There has always, however, also been a dark side of anonymity:

- Anonymity can be used to protect a criminal performing many different crimes, for example slander, distribution of child pornography, illegal threats, racial agitation, fraud, intentional damage such as distribution of computer viruses, etc. The exact set of illegal acts varies from country to country, but most countries have many laws forbidding certain “informational” acts, everything from high treason to instigation of rebellion, etc., to swindling.
- Anonymity can 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 disruptive communication. For example, some people use anonymity in order to say nasty things about other people.

The border between illegal and legal but offensive use is not very sharp, and varies depending on the law in each country.

Anonymity on the Internet

Even though anonymity and pseudonymity is not something new with the Internet, the net has increased the ease for a person to distribute anonymous and pseudonymous messages. Anonymity on the Internet is almost never 100 %, there is always a possibility to find the perpetrator, especially if the same person uses the same way to gain anonymity multiple times.

In the simplest case, a person sends an e-mail or writes a Usenet news article using a falsified name. Most mail and news software allows the users to specify whichever name they prefer, and makes no check of the correct identity. Using web-based mail systems like Hotmail, it is even possible to receive replies and conduct discussions using a pseudonym.

The security for the anonymous user is not very high in this case. The IP number (physical address) of the computer used is usually logged, often also the host name (logical name). Many people connect to the Internet using a temporary IP number assigned to them for a single session. But also such numbers are logged by the ISP (Internet Service Provider) and it is possible to find out who used a certain IP number at a certain time, provided that the ISP assists in the identification. There are also other well-known methods for breaking anonymity, for example elements can be included on a web page, which communicates information without knowledge of the person watching the web page. Some ISPs have a policy of always assisting such searches for the anonymous users. In this way they avoid tricky decisions on when to assist and not assist such searches.

In the case of e-mail, the e-mail header itself contains a trace of the route of a message. This trace is not normally shown to recipients, but most mailers have a command named something like *full headers* to show this information. An example of such a trace list is shown in Figure 1.

```
sentto-1119315-3675-1008119937-jpalme=dsv.su.se@returns.groups.yahoo.com
Received: from n12.groups.yahoo.com (n12.groups.yahoo.com
  [216.115.96.62])
  by unni.dsv.su.se (8.9.3/8.9.3) with SMTP
  id CAA21903 for <jpalme@dsv.su.se>;
  Wed, 12 Dec 2001 02:19:32 +0100 (MET)
X-eGroups-Return: sentto-1119315-3675-1008119937-
jpalme=dsv.su.se@returns.groups.yahoo.com
Received: from [216.115.97.162] by n12.groups.yahoo.com with NNFMP;
  12 Dec 2001 01:19:00 -0000
Received: (qmail 11251 invoked from network); 12 Dec 2001 01:18:56 -0000
Received: from unknown (216.115.97.167)
  by m8.grp.snv.yahoo.com with QMQP; 12 Dec 2001 01:18:56 -0000
Received: from unknown (HELO n26.groups.yahoo.com) (216.115.96.76)
  by mta1.grp.snv.yahoo.com with SMTP;
  12 Dec 2001 01:18:59 -0000
X-eGroups-Return: lizard@mrlizard.com
Received: from [216.115.96.110] by n26.groups.yahoo.com with NNFMP;
  12 Dec 2001 01:12:56 -0000
X-eGroups-Approved-By: simparl <simparl@aol.com> via web;
  12 Dec 2001 01:18:15 -0000
X-Sender: lizard@mrlizard.com
X-Apparently-To: web-law@yahoogroups.com
Received: (EGP: mail-8_0_1_2); 11 Dec 2001 20:50:42 -0000
Received: (qmail 68836 invoked from network); 11 Dec 2001 20:50:42 -0000
Received: from unknown (216.115.97.172)
  by m12.grp.snv.yahoo.com with QMQP; 11 Dec 2001 20:50:42 -0000
Received: from unknown (HELO micexchange.loanperformance.com)
  (64.57.138.217) by mta2.grp.snv.yahoo.com with SMTP;
  11 Dec 2001 20:50:40 -0000
Received: from mrlizard.com (IAN2 [192.168.1.119]) by
  micexchange.loanperformance.com with SMTP
  (Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
  id W11PL97B; Tue, 11 Dec 2001 12:53:11 -0800
```

Figure 1: An example of the trace headers on an e-mail message, which in this case has passed many servers on its route from the original sender to the final recipient. Headers are added at the top, so the last header in the list represents the original submission of this message.

To gain higher protection of anonymity, a clever impostor can use various techniques to make identification more difficult. Examples of such techniques are:

- IP numbers, trace lists and other identification can be falsified. Since this information is often created in servers, it is easier to falsify them if you have control of one or more servers.
- Communication is done in several steps. The impostor first connects to computer A, then from this computer to computer B, then from this to computer C, etc. To find the real person, all the steps must be followed backward. The trace needs transaction logs, and such logs are not always produced automatically. Logging may have to be switched on. So by co-operating with the owner of computer C, it is possible to switch on logging so that the next time the impostor appears, he is traced back to computer B. In the next step, the owner of computer B is asked to help trace the impostor further. Thus, through a tedious process, including the co-operation of all the used computers in the chain, the real person can be found. A famous example is described in the book [Stoll 1989], which describes the tracing of a hacker which used a series of servers, without permission, to conceal the route from the user to the final anonymous activity.

Anonymity servers

Since anonymity has positive uses (see above) there are people who run anonymity servers. An anonymity server receives messages, and resends them under another identity. There are two types of anonymity servers:

- Full anonymity servers, where no identifying information is forwarded.
- Pseudonymous servers, where the message is forwarded under a pseudonym. The server stores the real name behind a pseudonym, and can receive replies sent to the pseudonym, and transmit them back to the originator.

Anonymity servers often use encryption of the communication, especially of the communication between the real user and the server, to increase the security against wiretapping.

There are companies which market anonymity servers and there is a research area on improving the techniques of such software [McCullagh 2001].

People who want to achieve high security against being revealed, often use several anonymity servers in sequence. To trace them, each of the servers must assist or be penetrated (see Figure 2). If the servers are placed in different countries, tracing them becomes even more difficult.

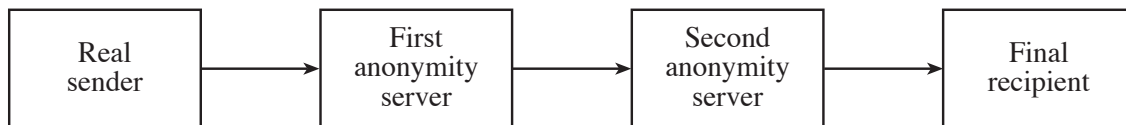


Figure 2: Steps to hide the real identity through several servers

A user might send a message to the first anonymity server, instructing it to send the message to the second anonymity server, which is instructed to send the message to the final recipient.

An example: Anon.penet.fi

Anon.penet.fi was a pseudonymity server started by Johan Helsingius in Finland in 1992. It was very popular by people in other countries, since they thought that relaying messages through an anonymity server in Finland would reduce the risk of their real identity being divulged. At its peak, it had 500 000 registered users and transferred 10 000 messages per day.

There was a lot of controversy regarding this server.

Example 1: Some people claimed that the server was used to distribute child pornography. This was both true and false. The server had been used to communicate between providers and consumers about child pornography. The actual pictures, however, had not been transmitted through the server, even though they had been wrongly marked-up as coming from the server. The server, in fact, had such a low limit on the maximum size of messages, that only very small pictures (less than 48 kbyte) could be sent through it.

Example 2: The server was used by a former member of the American quasi-religious organization “Scientology Church” to distribute secret documents from this organization to the public. The organization asked American police for help, claiming that the messages infringed on their copyright. The American police contacted the Finnish police in the spring of 1996, and the Finnish police forced Helsingius to tell them the real name behind these messages. The way in which the police in the U.S.A. and Finland treated this issue has been criticized afterwards.

As a result of these and other cases, Helsingius stopped his server in August 1996.

The Scientology Church has also attempted to stop newsgroups discussing the Church on the Internet using various technical means such as falsified CANCEL commands.

Statistics on the Use of Anonymity

Mikael Berglund made a study on how anonymity was used. His study was based on scanning all publicly available newsgroups in a Swedish Usenet News server, which downloaded almost everything written in Usenet News internationally in September 1995. He randomly selected a number of messages, which were pseudonymous and were shown as coming from anon.penet.fi (they may not always in reality have passed through anon.penet.fi), and classified the topic of these messages. His results were as follows:

Percentage	Type of message
30,0 %	Discussion Common topics: Sex, hobby, work, religion, politics, ethics, software.
23,1 %	Advertisements Common topics: Sexual/romantic contact advertisements dominated, a few other advertisements also used anonymity, for example ads searching for friends with a particular interest. The authors of contact ads were mostly male.
16,5 %	Questions and answers Common topics: Computer software issues, sex, medicine and drugs.
13,2 %	Texts Common topics: Pornographic texts, about 50 % heterosexual and 50 % homosexual (purported to be written by both men and women), jokes, sometimes nasty.
9,9 %	Test messages To try out if the anonymity server works.
3,7 %	Pictures Mostly erotic/pornographic.
0,4 %	Computer software
3,3 %	Unclassifiable Written in a language the researcher could not read, such as several messages in Chinese. Note the repressive political regime in China, which may be a reason why there were several people who needed to use an anonymity server in discussing issues in that language.

A classification of the contents of the messages shows (the total is more than 100 since some messages had more than one topic):

Percentage	Topic
18,8 %	Sex
18,5 %	Partner search ad
9,4 %	Test
8,7 %	Software
5,8 %	Hobby, work
4,7 %	Unclassified
4,3 %	Computer hardware
4,0 %	Religion
3,6 %	Picture
2,5 %	Races, racism
2,5 %	Politics
2,2 %	Internet etiquette (people complaining of other people's misuse of the net sometimes wrote anonymously)
1,4 %	Personal criticism of identified person
1,4 %	Internet reference
1,4 %	Ads selling something
1,4 %	Psychology
1,1 %	War, violence
1,1 %	Drugs except pharmaceutical drugs)
1,1 %	Ethics
1,1 %	Contact ad which was not partner ad
0,7 %	Poetry
0,7 %	Celebrity gossip
0,7 %	Pharmaceutical drugs
0,4 %	Fiction
0,4 %	Censorship

The most commonly used newsgroups were

Percentage	Newsgroup
21,7 %	Alt.sex.fetish.hair
19,5 %	alt.personals.bi
17,4 %	alt.sex.stories
16,4 %	alt.personals.poly
15,9 %	alt.sex.stories.gay
13,5 %	alt.suicide.holiday
13,4 %	alt.personals.bondage
12,6 %	alt.sex.wanted
11,8 %	alt.recovery.addiction.sexual
11,7 %	alt.personals.spanking.punishment

Percentage	Newsgroup
11,3 %	alt.personals.spanking
10,9 %	alt.binaries.pictures.boys
10,7 %	alt.personals.ads
10,2 %	alt.test
10,0 %	alt.personals.intercultural
9,7 %	alt.personal.motss
9,1 %	alt.sex.intergen
8,7 %	alt.testing.testing
8,5 %	alt.personals.fat

Legal View of Anonymity

Since anonymity can both be used for good and bad purposes (see the section “Is Anonymity Good or Bad?” above), various countries have laws both protecting and forbidding anonymity.

For example, many countries have laws protecting the anonymity of a person giving tips to a newspapers, and laws protecting the anonymity in communication with priests, doctors, etc. are also common.

On the other hand, the obvious risk of misuse of anonymity , has caused some countries (for example France) to try special legislation concerning anonymity, especially on the Internet, for example laws requiring that all messages on the Internet must be identified with the real identity of their source. Prosecutors and judges often are negative to all kinds of anonymity. For example, U.S. Supreme Court Justice Scalia said “The very purpose of anonymity is to facilitate wrong by eliminating accountability” (quoted in [Frankin 1995]).

The responsibility for messages has also been treated, for example my home country, Sweden, has a law [Sweden 1998] which (simplified) says that a service provider has responsibility for certain kind of illegal messages which are stored and downloadable from his service. However, if the service provider uses certain procedures to stop abuse, the service provider is not any more responsible. Such procedures are to accept complaints to a complaint board, and to remove messages which are obviously illegal, if notified of this to the complaint board. The wordings of this law shows that the lawmakers seriously tried writing a law which reasonably well stops misuse without preventing the free flow of information on the Internet. For example, the words “obviously are illegal” in the law means that the service provider need not investigate the legality in doubtful cases. For areas where illegal messages are common, the service provider has to scan or censor them regularly, and this has caused many Swedish service providers to ban certain newsgroups in which illegal

messages are common (such as “white supremacy” newsgroups and certain pornography newsgroups).

Lobbying

Legal authorities, such as police and prosecutors often lobby for laws forbidding anonymity on the Internet, for example, a group of prosecutors from different EU countries recently urged the EU to issue a directive which forbids anonymity on the Internet. Their main argument was that this was needed to stop illegal racial agitation. Civil liberties organizations, on the other hand, often lobby for protection of anonymity on the Internet, for example the American Civil Liberties Union (ACLU) [ACLU 2000].

How to Regulate Anonymity on the Internet

Since these issues are difficult and sensitive, it is not easy to decide how to lawfully regulate anonymity on the Internet. It is, however, important not to let the lobbying from police and prosecutors determine this.

Here is an excerpt from an EU report [EU 1999], which shows that the authorities are aware of the issues of anonymity:

In accordance with the principle of freedom of expression and the right to privacy, use of anonymity is legal. Users may wish to access data and browse anonymously so that their personal details cannot be recorded and used without their knowledge. Content providers on the Internet may wish to remain anonymous for legitimate purposes, such as where a victim of a sexual offence or a person suffering from a dependency such as alcohol or drugs, a disease or a disability wishes to share experiences with others without revealing their identity, or where a person wishes to report a crime without fear of retaliation. A user should not be required to justify anonymous use.

Anonymity may however also be used by those engaged in illegal acts to complicate the task of the police in identifying and apprehending the person responsible. Further examination is required of the conditions under which measures to identify criminals for law enforcement purposes can be achieved in the same way as in the “off-line” world. Precedents exist in laws establishing conditions and procedures for tapping and listening into telephone calls. Anonymity should not be used as a cloak to protect criminals.

Below is my personal idea how such a law or EU directive might be written. I am sure others have other ideas!

1. A law should allow for anonymity and pseudonymity on the Internet.

2. The law might however require, that the real identity behind anonymous messages should be available for retrieval, but if so only in accordance with the privacy policy of the web server distribution the message.
3. Every site which allows anonymity must publish a privacy policy, which explains exactly in what cases they will break the anonymity. For example, such a policy may say that they will break the anonymity only if ordered by the police, by a prosecutor or by a court of law in the country of the site. The site must then adhere to its own privacy policy and not look up the real name behind a pseudonym except when specified in the privacy policy. Different servers may have different such policies, but important is that they are known to their users and adhered to by the server.

As an example, I am at present working on a web site which will allow people with eating disorders to discuss their problems. Our privacy policy will probably allow people with eating disorders, their relatives and friends, to participate anonymously.

4. Since some people are afraid that means for the police to find the real person behind anonymity will be misused by some authorities, it should be allowed to communicate through a series of anonymity servers as described above, provided that each server follows the law on anonymity on the Internet. This means that co-operation of the police in several countries is needed to trace the person behind an anonymous message. Police should be instructed not to blindly follow requests from police in other countries to break anonymity, they should evaluate the correctness of the request before giving such assistance to police from other countries.

References

- [Abelson 2001] By the Water Cooler in Cyberspace, the Talk Turns Ugly, by Reed Abelson, New York times, 29 April 2001.
<http://www.nytimes.com/2001/04/29/technology/29HAR A.html?searchpv=site14>
- [ACLU 2000] PA Court Establishes First-Ever Protections For Online Critics of Public Officials,
<http://www.aclu.org/news/2000/n111500a.html>
November 2000.
- [Berglund 1997] Usenet News and anon-penet.fi. Master's thesis, in Swedish, DSV, Stockholm.
- [Donath 1996] Identity and Deception in the Virtual Community by Judith Donath, in Kollock, P. and Smith M. (eds): Communities in Cyberspace, Routledge, London, 1999.
<http://smg.media.mit.edu/people/Judith/Identity/IdentityDeception.html>.

- [EU 1999] Working party on illegal and harmful content on the internet, EC Report, May 1999,
<http://europa.eu.int/ISPO/legal/en/internet/wpen.html>
- [Froomkin 1995] Anonymity and its enemies. Journal of Online Law, art. 4, by A. Michael Froomkin,
http://www.wm.edu/law/publications/jol/95_96/froomkin.html
- [Joinsson 2001] Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. European Journal of Social Psychology, 31, 177-192.
<http://iet.open.ac.uk/pp/a.n.joinson/papers/self-disclosure.PDF>
- [McCullagh 2001] You Can Hide From Prying Eyes, by Declan McCullagh, Wired News, April 27, 2001
<http://www.wired.com/news/politics/0,1283,43355,00.html>.
- [Stoll 1989] The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, by Clifford Stoll, Doubleday, New York 1989.
- [Sweden 1998] Act (1998:112) on Responsibility for Electronic Bulletin Boards, in Swedish at
<http://www.notisum.se/rnp/sls/lag/19980112.HTM> and in English translation at
<http://dsv.su.se/jpalme/society/swedish-bbs-act.html>
- [Wallace 1999] Nameless in Cyberspace, Anonymity on the Internet, by Jonathan D. Wallace, CATO Institute Briefing Papers,
<http://www.cato.org/pubs/briefs/bp-054es.html>.