How To Avoid Being Logged

Basic ways of protecting privacy in a world with a data retention law

Łukasz Jachowicz
<lukasz @ jachowicz . com>

Bruxelles 2005

How To Avoid Being Logged
Basic ways of protecting privacy in a world with a data retention law

The data retention directive, presented as panacea to the terrorism, has some basic design errors. These errors put the ordinary citizens' privacy at risk and, at the same time, make it easy to circumvent restrictions by any person with basic technical skills or just a simple ability to use Google. Below you can find most basic techniques used to avoid logging connection information by internet or cell phone operators. All of them are easy to implement, most of them is already used to create secure subnetworks and software that automates the whole process is freely available in the internet. These are not all existing ways to avoid being logged, just the easiest ones. Anyone can use most of them to protect its privacy without breaking any law. Forbidding these techniques would decrease the security of the whole internet and would be a big step back in the evolution of this network.

Tunnelling (**VPN**) is a common technique used to securely connect over internet two or more local computer networks (ie. office networks), physically located in different locations. All the connections from one network are encrypted and packed together into single connection that goes straight to the gateway server of a second network. Gateway server decrypts it and unpacks it. For user of such network the whole process is completely transparent.

The same technique can be used to avoid logging connection information by Internet Service Providers (ISP). The computer used by a person who wants to keep his or her privacy packs and encrypts all the data, create a tunnel to the server outside of European Union (for example, to the USA, Russia or Cuba) and send all the connections through this tunnel. Internet provider of this person would log only one, long lasting connection to USA/Russia/Cuba, in spite of this that the person using the computer would connect to hundreds of servers at this time. It would stay completely invisible for anyone trying to log the internet traffic.

Mail anonymizers and secure **proxy servers** are the tools used to remove any data that would help to identify an e-mail sender or the computer used to browse the web.

The mail anonymizer is usually a server that removes data hidden in the header of every e-mail message. Each e-mail message has hidden lines that show, for example, real time of sending and the list of servers used to transmit the e-mail. If the email gets to the mail anonymizer, it would remove these data and put its own address instead of the real sender address. Anonymizers can be connected in networks, so the e-mail message that comes to the first server is anonymized, sent to the second server, then anonymized again and sent to the next anonymizer server and so on. When a mail is delivered to the final recipient, the only server he could trace is the last server in the network of anonymizers. The rest of sender's data is lost forever. Also the internet operator of sender cannot trace the real recipient of the e-mail message as he would see only the address of first anonymizing server as a recipient.

The secure proxy server works in similiar way but is used to hide the identity of a web browsing person. Internet operator would be able to record only the address of used

proxy, the final website operator would see only the proxy address instead of the real browser's address.

Wireless networks (WiFi) are getting more and more popular all over the Europe. Unfortunately, the standard security technique used to protect this kind of networks is poorly designed and allows anyone to connect even to protected networks without any effort. Moreover, the security systems are usually turned off as they seriously slow down a network without providing any serious security.
In many places (like railway stations, city markets, restaurants, shopping malls or just whole cities) the WiFi network is provided for free to anyone with WiFi capable device. It means that anyone with a laptop or palmtop could connect to internet completely anonymously. In case he or she commits a crime, the address recorded by internet operator will be the address of the WiFi gateway, not the real address of the criminal. If such a crime were committed using publicly available network, it's easy to prove that its owner has nothing to do with it. If a cracker connects to the private WiFi network, the owner of such network won't be able to prove he is not the one that committed the crime and innocent victim would be convicted.

IMEI and **MAC** numbers, presented in a draft directive as unique and invariable identifiers of each device are in fact easy to change. The IMEI number (the unique number of a cell phone) can be changed using the specialised software available in internet. The MAC address - the unique address of the network device - can be changed using one simple command of any modern operating system. Moreover, some producers accidentally gave the same MAC number to many network devices so that even the "brand new" MAC number doesn't necessary have to be unique.

MAC numbers are not transmitted during the internet communication so the internet operators won't be able to record them.

Phone connections can also be hard to trace thanks to Voice over IP (VoIP) telephony. This technique allows making phone calls using internet connection instead of fixed phone lines. Because of low prices, a lot of VoIP users choose USA-based phone operators. If any person wants its VoIP connection completely secret for its internet operator, he or she can create a secure tunnel (technique described earlier) to outside of the European Union and using the tunnel connect to his VoIP operator. Even if he or she calls someone in EU, the recipient's phone operator would be able to log that someone from USA called European phone number, he wouldn't be able to find out that the call in fact was made from within EU.

Non-traceable cell phone connections are also easy to make from within European Union. The easiest, and by the way - most expensive way - is to buy a new pre-paid phone. The more secure way is to use the 3G phone. So called third generation cell phones provide its users very fast connection to internet. At the same time, these cell phones are powerful computers with its own operating systems. It means that any software, not only the one provided by manufacturer, can be loaded on to such phones. To make an non-traceable call from 3G phone it is enough to run a tunnelling software that would hide real internet connections from being logged by cell phone

operator. Then the VoIP software must be run on such device. After that, any connection made using the VoIP software would be untraceable for loggers.

Hotmail and **Google mail** accounts are the simplest way to avoid logging the information on the sender and recipient of the mail. As Hotmail and GMail servers are usually located outside of European Union, its operators are not obligated to log their users' activities. It means that European operator will be able to log only the connection to the web server of webmail operator but will not be able to find out to whom or from whom is the mail sent - or does an user send or read any mail message. If both mail users use webmails located outside of the European Union, European internet operators will not be able to record any mails send or received by any of these users.