Distributed Anonymising Networks: introduction to Tor

When you send something over the internet (an e-mail, a picture, a web page, etc.), the information travels in the form of “packets”. Internet packets have two parts: the data (the thing you are sending) and a header used for routing. The data can be hidden by encryption, but the header will still contain information about the source (your IP address), destination, size, times, etc. The header can be analysed by the bad guys to try to identify you and the people you are corresponding with.

A basic problem for the privacy minded is that the recipient of your communication can guess that it was you who sent it just by looking at the packet header. When you send a comment to a blog “anonymously”, the blog owner can look at your submission and find out where you are, and much more. With some work you could be identified by name.

A common form of Internet surveillance is known as "traffic analysis”. A very simple form of traffic analysis might involve tapping into the internet somewhere between sender and recipient, and looking at headers. Internet service providers can do this more or less legitimately (and sell the information) but unauthorized intermediaries can also analyse your headers. When a repressive government owns the service provider, you may be more at risk.

There are also more powerful kinds of traffic analysis. Some attackers spy on multiple parts of the Internet and use sophisticated statistical techniques to track the communications patterns of many different organizations and individuals. Encryption does not help against these attackers, since it only hides the content of Internet traffic, not the headers.

The bad guys trying to get you could stage an end-to-end timing attack. If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to confirm that they are part of the same circuit. Protecting yourself from this technology is a major challenge in safe internet communications.

There are various ways to hide your identity while surfing the internet. One is to subscribe to a web proxy service that will do this for you for a fee. Of course you don't know who owns the proxy server: if the bad guys have something to do with it then you are even more exposed than before.

One practical way to hide your identity is to use a distributed anonymising network such as Tor (free of charge). The following paragraphs are taken from Tor's website.

“Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.”

“To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.”

“Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support.”

You can try a version of Tor that runs off a USB flash memory stick, without installation and without leaving any traces in your computer. It is called the Tor Browser Bundle, and contains a stand-alone version of Firefox. There is a tutorial at http://www.youtube.com/watch?v=nq_dOsAAQ8A It will be a little slower than your normal browser, but if you are concerned about security...