Who Owns Cyberspace?

> *When you step into cyberspace, you are in somebody else's territory. You walk naked before his all-seeing eye. Over him you have no power. Even your inner secrets - if you have been stupid enough to put them on the hard drive of your personal computer - are open to his gaze.*

For me, the word *cyberspace* has a dubious etymology. It is a shortened form of the word *cybernetics*, concatenated with the word *space*. The word *cybernetics* is derived from a Greek word which, depending on its context, can mean rudder, steersman, pilot or governor. The word *space* refers to a multi-dimensional medium through which conscious entities like humans may become aware of each other and interact. By consequence, the word *cyberspace* must refer to a multi-dimensional medium which some conscious entities use as a rudder or steering device through which to govern or control the rest of us. To my mind, this is pretty close to the truth.

The multi-dimensional medium of cyberspace must therefore include, first and foremost, *terraspace* - the physical biosphere of our planet. After all, our primary means of communicating is by travelling to meet and converse with others face-to-face. The biosphere is filled with air, which conducts the sound of the human voice. It is thus a medium through which human beings may converse. This medium is an ideal channel for human communication. Through it, normal human speech offers a channel of communication with a very high bandwidth over a conveniently limited distance. This facilitates the rapid interchange of knowledge, thoughts and ideas with safe and easy control between privacy on the one hand and and publicity on the other.

Cyberspace must also include *radiospace* - what we know as the electromagnetic spectrum, comprising the full range of radio waves, through which we are able to communicate at a distance almost as if face-to-face. And finally, of course, it includes the Internet. Personally, I question whether or not these relatively recent technical advancements really offer any advantage to the well-being of humanity. My reluctant perception is that humanity certainly has yet to gain the necessary and sufficient wisdom to use them in an appropriate and constructive way rather than as a tool for conditioning, tranquilizing and exploiting gullible populations.

The following discourse is about all three of these aspects of cyberspace and what goes on within them, as perceived by me from where I stand within time, space and the social order.

Who Owns Terraspace?

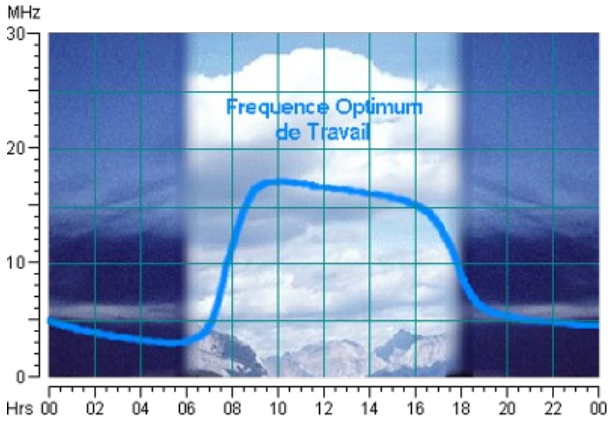
Perhaps in the misty beginnings of humanity, individuals wandered unhindered across the bountiful surface of their native planet, able freely to communicate and interact with their peers. But it was not long before kings began to annex the Earth's habitable land, and the resources it contains, as a means to govern and control the majority of mankind and thereby command his labour. This was done firstly by force of arms then by legal instruments such as the "Inclosure Acts" (1604 to 1914) in the United Kingdom.

Nowadays, the only way the individual may move across the surface of our planet is via a transport infrastructure, which is far from free, and within which, the individual's movements are severely restricted, regimented and controlled. The Earth is no longer free to wander.

Today, individuals may communicate and interact across the physical surface of the planet, but only by the leave of its State and corporate owners. And these require payment for their leave. They also impose the rules as to which restrictive routes the individual may use and how and when and under what conditions he may use them. They control all land. Control is ownership. Even in the prosperous First World economies, the individual has no allodial claim over any part of Planet Earth. He even has to pay for the privilege of "owning" his little brick box parked on its postage stamp lot in suburbia.

In my opinion, this is not an idyllic state for the human species. Each individual is an independent sentient being. Collectively, humanity is not a conscious entity. Neither is a family, a State or a corporation. These have no personal fear or feeling. Consequently it is the well-being of each conscious individual that matters. Each individual should therefore rightly have free and unencumbered economic use of his fair share of *terraspace*, and the right of free passage through all *terraspace* on the understanding that he not disturb its economic use by its allotted user. No collective has the moral power to take these rights from the individual.

Who Owns Radiospace?



In 1867, James Clark Maxwell formed his mathematical prediction of the existence of radio waves. Two years later, Heinrich Hertz managed to generate them artificially. Subsequent experiments revealed that these waves could be made to bounce between the ground and the ionospheric layers high above and thereby propagate around the world. Before these events, nothing was known about these waves, or about the dimensions of space-time through which they travelled. And what is unknown can be commandeered by neither king nor corporation. Consequently, upon its discovery, the radio spectrum was an untouched virgin land, wild, unclaimed, free. Anybody could build his own apparatus and experiment to his heart's content.

But not for long. As with the open continents of the New World, kings and emperors, enterprises and corporations, soon looked upon the radio spectrum with possessive eyes. Each mustered his mighty power to divide and conquer it for lucrative gain. The kings of the Earth each soon declared his allodial possession, within his respective jurisdiction, of the newly revealed dimensions of space-time through which travelled the electromagnetic wave. Common man could no longer venture therein, except by the leave of his king. Thus, like land, the radio spectrum had become subjected to what could be viewed as another form of "Inclosure Act".

For king or State, radiospace is invaluable for administration, defence and as a source of common revenue. Thus, today, the king (as an embodiment of the State) reserves some of the radio spectrum for use by his military and civil services. He licenses the use of what remains to his subjects, in return for a fee. He licenses some of it to broadcasters, some to the merchant marine, some to aircraft operators, some to commercial communications carriers, some to private communication, and even some to amateur radio enthusiasts.

As always when a king grants his leave, it comes with terms and conditions. In the case of licence to use the radio spectrum, it comes with *very restrictive* terms and conditions. The licence holder is restricted not only as to what frequency range and power he may use, but also as to what kind of information he may send and receive.

The restrictions placed upon radio amateurs are simply Draconian. Political, religious and commercial comments or discussions are specifically prohibited. It is probably unsafe even to discuss philosophy. In fact, the only topics that radio amateurs are safely able to discuss are their equipment, the weather and signal conditions. This makes for tediously boring conversation. Furthermore, however boring it may be, a chat between radio amateurs can never be private. Section 2, Clause 11(2)b of the "Terms, conditions and limitations" of the UK's Amateur Radio Licence states that "Messages sent from the station shall not be encrypted for the purposes of rendering the Message unintelligible to other radio spectrum users."

Radiospace is thus strictly off-limits to any lowly individual who may wish to discuss - either privately or openly - his own philosophical, political, religious or commercial ideas and opinions with his fellow human beings. I sometimes vainly try to imagine what it would be like to be a member of a group of fictitious egalitarians who alone knew of the existence of radio waves and how to use them to communicate. We would have the unencumbered freedom, without cost, to discuss whatever we liked, unhindered by any restrictions and regulations imposed by king or State. Even if my friends and I had discovered a secret technique, such as chipped digital spread-spectrum transmission, way back in the 1950s, we could have communicated by radio among ourselves without any authority of the time even being aware of our signals.

No State wants individuals to have the unlicensed and uncensored freedom to be able to discuss any and all topics with any other arbitrary individual within its realm. If they could, like minds may connect. Connected they would become united. United they could not be divided. Undivided they could not be ruled. And that would pose a real and present threat to the established order.

Unlike terraspace, radiospace is three-dimensional and is not confined to the surface of the Earth. It occupies the entire universe. So, to what extent can a sovereign state lay claim to it? It cannot be fenced like land. A State cannot stop radio waves from crossing its national frontiers. The only extent to which a State can lay claim to the possession of radiospace is to control its use by its subjects. The only way it can do this is by imposing a legal penalty upon any individual who uses radiospace, from within its territorial boundaries, without licence or in a manner or for a purpose that its law forbids. The State polices its radiospace, to see who may be violating this aspect of its "sovereign territory", simply by monitoring the radio spectrum from official listening stations.

Having imposed rigorous control over who may or may not transmit signals from within their territories, some sovereign states even forbid their subjects even from passively receiving radio signals without having paid a licence fee. This was abolished in the United Kingdom in 1971, but it still remains for receiving television programmes.

The licence fee money is purportedly used for creating programmes and running the transmission services. Notwithstanding, it places the State's broadcasting authority in the position of receiving unconditional finance to produce what the authority wants the people to see and hear, which is not necessarily what the people want to see or hear. More disturbingly, it creates a facility by which the State and its broadcasting authority may steer and manipulate the public mind, making it an effective means of controlling society to conform to the will of the State and the elite minority who actually influences and controls it.

A sovereign state cannot stop radio waves from other sovereign states from entering its territory. Neither can it stop radio waves emanating from within its jurisdiction from leaving and entering the territories of other sovereign states. A particular State may wish to prevent foreigners listening to its domestic broadcasts. It can try to do this by limiting power and/or using line-of-sight frequency bands. More likely, though, it may wish to prevent its subjects from receiving broadcasts from certain

other foreign States, for conflicting political reasons. This it can achieve by transmitting jamming signals on the same frequency as the offending broadcast, as happened during the Cold War. Nowadays, with digital transmission, complete control of who may or may not receive a broadcast can be effected by encrypting the signal.

So, having discovered it, how should mankind use radiospace? The answer, in my opinion, is in a way that is fair to every individual. Every individual, should he wish to, must be free to use radiospace to seek and find like minds and discuss openly and freely his ideas with them. He should also be free to broadcast his ideas to any who may wish to listen. He must also be free to contact anybody casually or for some specific reason. Equally, he must have the right to privacy from being pestered by persistent callers, such as with the present unwelcome epidemic from telesales call centres.

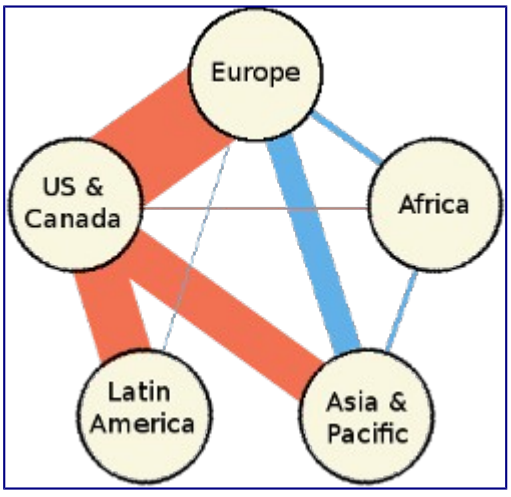
Technology exists whereby all this could be easily implemented without common infrastructure. However, for it to work equitably, there must be some form of central coordination. A single entity must exist to allocate spectrum usage and session channels and to maintain search indexes. But such an entity must not be an active authority. It must have no coercive power. Neither should it ever be allowed to fall into the hands of private commercial interests. It must be a passive system, implemented as a distributed technology within the equipments of all its users.

Who Owns The Internet?

Radiospace is an aspect of the natural universe. The Internet is not. Two radio amateurs, in different parts of the world, may communicate with each other over HF radio, using transceivers designed, built and owned entirely by themselves. In this case, their two transceivers are connected by entirely natural means. Two geeks, in different parts of the world, may communicate with each other over the Internet, using personal computers designed, built and owned entirely by themselves. In this case, however, what connects their two personal computers is a vastly complicated and expensive artificial infrastructure.

The justification for the extreme cost of the Internet's infrastructure is that radiospace simply does not have the capacity for the data transfer speeds demanded by all the Internet's users. At least, not the way the Internet is currently implemented. And the way it is implemented has a lot to do with how the Internet was born, developed and evolved.

One part, of what became the Internet, started from the wish of scientists and academics in research centres and universities around the world to be able to rapidly exchange scientific papers and experimental data. They opted for the quick solution of renting the use of cables or packet services from national telecommunications authorities and corporations. Another part started as networks linking government centres in various countries, again using rented cables. A third part started as separate private international data communications networks, also operated across rented cables, by various large multinationals. These three parts and their various elements all finally, by mutual agreement, became interconnected to form the Interconnected Networks or Internet.



Consequently, the connecting cables are owned by national telecommunications authorities and licensed private telecommunications corporations, each within its

designated geographical jurisdiction, throughout the world. These may also own the switching nodes (or routers), at the various junctions in the cable routes. Switching (or routing) equipment may, however, also be owned by private corporations who rent the use of the cables connecting their private switching nodes. All these together form what is called the Internet Backbone, which spans the entire globe.

A broad-brush logical view of the global backbone is shown on the left. The width of each coloured line depicts the relative amount of data traffic flowing between each pair of the 5 main regions of the world. By far the busiest route is between the USA and Europe. Practically 100% of Latin America's traffic, bound for the rest of the world, flows via the USA. The one glaring omission is a route linking Latin America with Africa. With practically all the world's data traffic flowing via the USA, the USA is effectively able to intercept, monitor, record, interrupt or stop all data flowing around the world.

All private interests operating within the USA, including all owners and operators of Internet cables and routers, through which practically all the world's Internet traffic passes, are subject to US law. Consequently, the government of the United States of America - through its various agencies - is able to control the flow of traffic within the physical infrastructure of the Internet worldwide.

An Internet Router sits at each junction of the Internet. Its job is to forward each arriving data packet, down the next appropriate leg of its route, to its final destination. Each data packet contains information about its origin and destination addresses. Most routers are located in US territory and are therefore under the jurisdiction of US law.

The US government is therefore in a position to be able to issue a legal instrument to a router administrator forbidding the forwarding of data packets travelling between a specified [home or foreign] origin and a specified [home or foreign] destination. With appropriate software or chip firmware covertly embedded within a router computer, a US government agency could effect the blocking remotely, without the router administrator even being aware of it.

I am not suggesting that they do this. But the general adage is that: if they can, they will. They may be thus able, at will, to determine whether or not a web site in one foreign country be visible or not in a different foreign country.

Notwithstanding, effective ownership of the Internet's physical infrastructure does not procure control over what kind of information it carries, and between who and whom. The Internet is internationally open. Hence, the *semantic content* of the data traffic flowing through it is outside the direct control of any one sovereign state or legal jurisdiction. To truly control the Internet, it is necessary to construct some means of controlling what kind of semantic content may pass through the Internet and who may and who may not access it.

Because of its central position, within the worldwide infrastructure of the Internet, the USA has, through active selective encouragement, managed to establish multiple means of achieving total control of Internet content - or, at least, world public access to it. These means are, for all practical purposes, exclusively concentrated within United States jurisdiction, where, again, they can be regulated by US law. The government of the United States has thereby effected a worldwide "Inclosure Act" upon cyberspace.

Control of The World-Wide Web

Any scientist or academic - or indeed, anybody who may want to - can publish his observations, experiences, sufferings and opinions on the worldwide web, as in the example of my own web site shown below on the right. All he needs to do is write his thoughts in a text file, mark it up in HTML

[the hypertext mark-up language] and upload it to a web server. He can include, within his text, diagrams, photographs, animations and even running programs called applets. But how do others get to see what he has thus published?

Within the hypertext mark-up language is a container for a list of keywords. It is called the keywords meta tag. The author of the document places relevant keywords into the keywords meta tag of his document. These are words, which he thinks are likely to spring to people's minds, when they are searching for material on the subjects or ideas that his article covers. The words which actually spring into people's minds, when they are thinking of a particular subject or idea, are not necessarily very likely to appear in the actual texts of the most relevant documents. So choosing effective keywords is quite an art.

Certain computers, connected to the Internet, contain running programs called search spiders. These continually trawl through all the documents on all the servers on the worldwide web. Each spider looks in the keywords meta tag of each document. It then places references to that document against all the relevant keywords in its vast search index.

Running on these certain computers also is another kind of program called a search engine. This is accessed via a web page, which looks something like as shown on the left.

A person looking for documents on a particular subject types the relevant keywords that come to mind into the search engine's entry field and then clicks "Go". The search engine then looks in its vast index for relevant documents. It then displays a list of the titles of the relevant documents it has found, together with a short summary under each title. The searcher then clicks on a title which interests him in order to display that document in his browser.

Search engines and their spiders were free ancillary services running within large computers operated by academic institutions and other non-commercial establishments. Documents were listed strictly according to relevance and nothing else. People could find exactly what they wanted within all that was available. And everybody lived happily ever after. That is, until business and commerce got their dirty devious hands on the worldwide web and corrupted the whole process.

The natural motive of academics and other thinkers is to make their material available to people who are genuinely interested in the subjects concerned. They have no desire whatsoever to push their material down the throats of people who are not interested in it. Not so the businessman. He wants to attract anybody and everybody to his web site in order to beguile them, by all means possible, into buying his products. And he quickly found an effective way of doing this.

He compiles a list of the most popular search words that people enter into search engines. These are, for the most part, words with sexual, sportive or financial connotations. Then he places these words - along with keywords that are relevant to his own business - into the keywords meta tag of his web site's home page. So not only do people specifically seeking his products end up at his site, but also a vast number of other people who were searching for something quite different. His hope is that these other people, having arrived at his site, will be beguiled by his eye-candy presentation into buying his merchandise.

The overloading of the HTML keywords meta tag with false attractors eventually became such an overwhelming nuisance to Internet users that traditional search engines became almost useless for

serious searching. Something drastic had to be done. The solution was to abandoned the keywords meta tag as the means for search spiders to classify web pages. Search engines eventually ignored the contents of keyword meta tags altogether and instead extracted keywords directly from the main body text of the document.

Of course, this practice does not lend itself to the compilation of the most effective keywords. Most words people think of when looking for a document are unlikely to appear as such within the document's text. Keywords are generally big highly specific words. The thought such a keyword embodies is usually expressed much more powerfully within the actual text by a phrase comprising a succinct combination of much smaller words. Thus the process has already lost some of its original effectiveness. But this is only the beginning of woes.

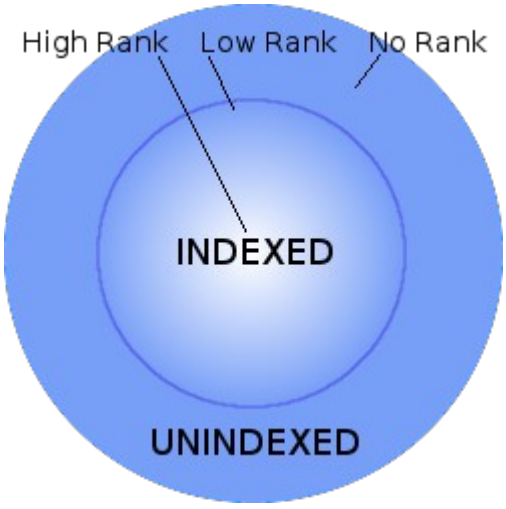
To compensate for this problem of less effective keyword harvesting, web page authors began to write text that was deliberately force-populated with what they considered to be relevant keywords. This naturally resulted in bland text that was much less interesting and expressive, and indeed much more irksome and tiring to read. So it had to be kept short. The quality of web content thus began to diminish and so viewer interest had to be evermore held by quirky artwork. Web content thus became increasingly trivial.

At this juncture, by powerful marketing, US search engines began to attract the greatest number of web users. European and other search engines quickly fell from popularity and eventually disappeared. But the major players among the US search engines began to think commercially. Before, they had been ancillary services provided internally by academic institutions and large corporations.

But now they wanted to make a profit. Charging the individual searcher was essentially impractical. So they adopted a policy for charging commercial web site owners. One popular way was to charge for ranking sites within search lists. The more you paid to the search engine provider, the nearer the top of the relevant search list your site would appear. This meant that non-commercial web sites all but disappeared from all search lists.

In all this confusion, I found that a small search engine called Google still returned good relevant results. I think that perhaps at the time it did not charge for ranking. I don't know. All I know is the results I got were good. Finally, for whatever reason or by whatever means, Google grew and became the *de facto* means by which practically all the web users in the world searched for sites and pages on the worldwide web. Thus Google has become the single exclusive access point, for everybody in the world, to information within the worldwide web.

This means that Google alone can determine how the entire worldwide web is indexed from the point of view of almost all the web users in the world. Its indexing policy can determine whose web sites can be seen and whose cannot; whose appears in search lists and whose does not. It can use arbitrary criteria to rank web pages by relevance, and indeed to exclude vast swathes of websites from its index altogether. Thus, one single commercial entity, within the jurisdiction of one single sovereign state, has almost total control over the flow of intellectual material among all the inhabitants of Planet Earth.



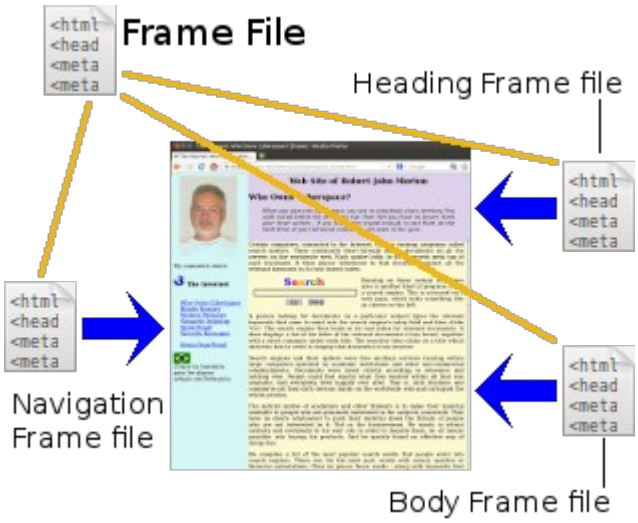
My web site has been on-line since April 1998. That's before Google came to power. Up until around 2004, my site had thousands of unique visitors a month. I received hundreds of emails in feedback from viewers. Now, looking in the access log, I see that this entire vast web site, of articles amounting to about 1·2 million words, receives about half a dozen meaningful hits a month if I'm lucky. And these hits are exclusively to pages about odd technical topics, which are of only ancillary significance. Searching for major topics within this website using any public search engine reveals nothing. Yet I have complied, as best I can, with all the technical standards that search engines currently demand. Why should this be? Statistically, it makes no sense.

The Spider That's Too "Clever"

I speculate that one reason for the dramatic fall in hits to my website is Google trying to make its search spider a bit too "clever" for the good of writers like myself. What is known as the *three-frame set* has been a standard way of presenting documents of the kind that I write since Internet antiquity.

Each of my documents is presented, within the browser window, in three distinct areas called frames. The top frame, shown in pink, is the Heading Frame. It contains the document's title plus a 4-line extended heading or mission statement. To the left is the Navigation Frame shown in cyan (light blue). This contains hyperlinks to the group of documents of which this document is a part. The remaining frame, shown in yellow, is the Body Frame. It contains the main text.

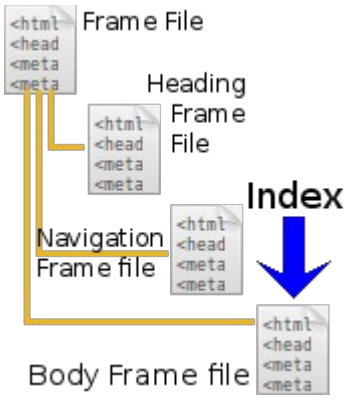
The content of each of the three frames is contained in a separate file: a Heading Frame file containing the tile and extended heading of the document, a Body Frame file which contains its text and a Navigation Frame file containing the navigation links. A fourth file (called the Frame File) acts as an organiser to load the contents of each of the other three files into its appropriate area of the browser window. The document is displayed by simply requesting that the Frame File be displayed. The Frame File itself does the rest.



The browser window should be ideally 840 pixels wide: 200 for the Navigation Frame and 640 for the Heading and Body frames. The window height should ideally be about the same or a little more. With these minimal dimensions, the Heading and Navigation frames will not scroll. Only the Body Frame should contain a vertical scroll bar. This arrangement allows the reader to scroll down the Body text while the title and mission statement stay permanently in view at the top as a semantic anchor for the reader's mind while reading a long discourse. The Navigation Frame stays put also,

keeping the reader always aware of where the document he is currently reading fits into the big picture.

This arrangement is ideal for presenting large documents on intellectual subjects. It is not, however, what they call "Google-friendly". Google seems to be completely flummoxed by frames. Initially, as I understood it, the Google spider could not read JavaScript. I therefore adopted the following strategy to induce Google to index my documents, which exploited the Google bot's inability to see JavaScript.



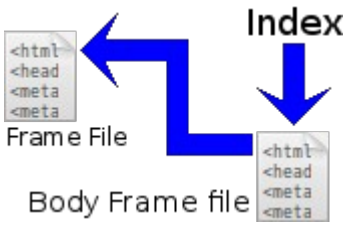
I needed to induce the Google bot to trawl the Body Frame file of my document for keywords. I therefore pointed all links that referred to the document concerned to the frameset's Body Frame file. In the Navigation Frame file, the Heading Frame file and the Frame File I put an HTML meta tag to tell search spiders not to index them but to follow the links within them onwards to other files. I put a different meta tag in the Body Frame file telling the spiders to both index the document and follow the links within it onwards to other documents.

What would appear in Google's index would therefore be references to each of my Body Frame files. If a searcher clicked on a link in a Google search results list, my Body Frame file alone would be displayed - without a heading, mission statement or contents list. That would look very frumpy and would not be much use. I therefore included, in the header section of my Body Frame file, the following JavaScript statement:

```
if(window==top){top.location.replace("cyberspace_frame.htm");}
```

This tells the browser that if it is being asked to load my Body Frame file as the only document to be displayed in the browser window, then it must load the document's corresponding Frame File instead. The Frame File then presents the three frames in their respective areas of the browser window. And all is well.

That is, until Google decided to make its bot a bit too "clever". It seems they made it able to read JavaScript. The problem is that, although the Google bot may be able to determine what a JavaScript statement is doing, it does not know why it is doing it. And in its ignorance, it assumes the worst. If it could not read the JavaScript, it would blindly continue on through the Body Frame file and extract keywords. But it does not do this.



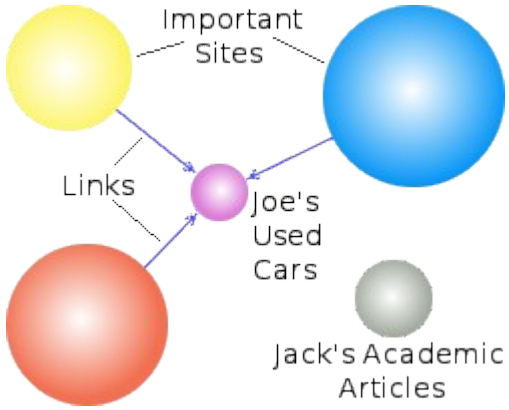
When it encounters the above JavaScript statement at the beginning of my Body Frame file, it sees that it is immediately being redirected to another page. It assumes that because I am immediately redirecting it to a different page, I must be doing something "sneaky" (Google's terminology). What is "sneaky" about presenting my document in a standard frameset, I can't imagine. Nonetheless, the Google bot, because it wrongly interprets what I am doing, refuses to index my document. Hence, from thousands of hits a month from interested viewers, my pages began to receive practically none.

If the spider had just stuck to ignoring JavaScript, all would have been well. If it had simply obeyed the JavaScript, executed the Frame File to assemble the frameset as a complete document the way a browser does and then indexed it, then again, all would have been well. But only half-doing the job, the way it does, has caused nothing but trouble for web writers like me.

My only way out of this was to create a parallel web site in which all my 1·2 million words of articles were re-formatted as single boring documents with no global site navigation. So I had one website for my readers and another for Google to index. What a pain. Hopefully, when a Google searcher finds one of my articles in Boring Format, he will click on a link somewhere within it, which will take him to the properly presented version of my website. This, however, proved not to be an effective solution. So eventually, I had to resort to using non-web networks as a means of providing "back-door" indexing for my website.

A Dysfunctional Indexing Policy

Notwithstanding the above exasperating annoyance, the dominant reason for websites such as mine disappearing from search listings is that all the major search engines have followed suit and changed their criteria for indexing websites. Any little website promoting a commercial entity, right down to a corner shop, gets pride of place in search listings. For anything of an intellectual nature, however, only globally-known high profile web sites seem to get listed. Others appear to be classified as being of interest only to their owners and are consequently not considered worth including on a search list. Of course, another possibility could be that the programmers of search-engine algorithms have suddenly become extremely inept. However, I do not think this to be likely.



From what I understand, from what I am able to glean from the web, the main criterion now for ranking a web page is the number of links there are to it from other web pages multiplied by the "importance" rankings of the web pages containing those links. This policy systemically guarantees that the high ranking of web sites that are already established is preserved and that nothing new will ever see the light of day. And this is exactly what appears to happen.

I painstakingly research and write a new document on what must be, at least to some people in the world, an interesting topic. I upload it to my web site. I link it into my site index and arrange for appropriate pages already on my site to link to it where relevant. My new document has no links pointing to it from external web sites. It therefore does not have any search ranking whatsoever. It will therefore never appear in any search listings. Consequently, nobody will ever see it. Consequently, nobody important will ever link to it from their important site. It will remain forever excluded. So those "at least some people in the world" will never be able to find it, no matter how well tuned a set of keywords they may enter into the search engine. *Quod erat demonstrandum*.

Notwithstanding the above, suppose I already know somebody who is very interested in the topic upon which I have written. I give him the URL of my new document so that he can access it directly without needing to use a search engine. He reads it. He likes it. He tells other people about it. But why should he put a link to it from another web site? He can simply bookmark it in his browser. So even if people get to know about my new document by means that are outside of the worldwide web, it is still not very likely to be linked-to from any "important" sites.

Thus, for the purpose of revealing to everybody the goldmine of information that is available on the worldwide web, this indexing policy is systemically dysfunctional. It simply preserves the popularity of what has already been made popular through other means. But perhaps this is deliberate. Perhaps the intention behind the change in the search algorithm around 2004 was for the very purpose of creating, strengthening and preserving a worldwide web establishment, while minimalizing or

excluding everybody else. Before 2004, I could search the web and find a vast diversity of interesting stuff. Now my searches end up at the appropriate established mega-site, which shows me only the bland sanitized content that I am meant to see.

The worldwide web has thus become subjected to a passive or inductive form of censorship, effected by the fact that a search engine places references to large established sites at the top of any search results list, leaving other "also ran" sites way down the list where only the very diligent searcher will bother to look.

The Cease and Desist Order

But there is yet another form of censorship, which the US government - or any other US-based authority, agency or interested party - can impose on web sites. That is a legal instrument called the *Cease and Desist* order.

Google, which is based in the US at the confluence of all major routes within the worldwide Internet infrastructure, is exclusively subject to, and regulated by, US law. If the *powers that be* [whoever they are] do not like something that has been written in a web page, they can issue a *Cease and Desist* order. Not to the purported offender [i.e. the author of the page], but to the search engine operator.

The demand of the *Cease and Desist* order is not to take down the web page concerned or to delete the "offending" content from it, but to cease and desist from placing the page in a search index. Thus it will never feature in any search results. This way, the location of the site's web server, the nationality of the author of the web page and the particular sovereign jurisdiction within which he may currently reside are all irrelevant. The search engine is located in the US and is therefore bound by US law, so the execution of the *Cease and Desist* order is easy and straightforward.

I once saw a document that was titled as a *Cease and Desist* order within a search list of my web site. Strangely, it seemed to be nothing more than a template. The reference to the offending web page and the offending content within it were both blank. It had the name and address of what I presume was an American law firm. Apart from this, it seemed to be a complete non-entity. Shortly afterwards it disappeared. I have never been any the wiser. I presume that somebody somewhere got their legal knickers in a twist.

The upshot of all this is that general public access to content on the worldwide web appears to be inductively steered, by a single political interest, towards approved parts only of the total content that exists. And the content of those approved parts seems to be becoming more and more trivial. I am neither for or against the United States of America. I would have the same gripe were any other sovereign power in the same singular position. Nonetheless, a situation exists in which one sovereign power alone is able to exert almost total control over something which pertains to the entire world. And it is my firm opinion that any such situation is fundamentally against the best interests of mankind.

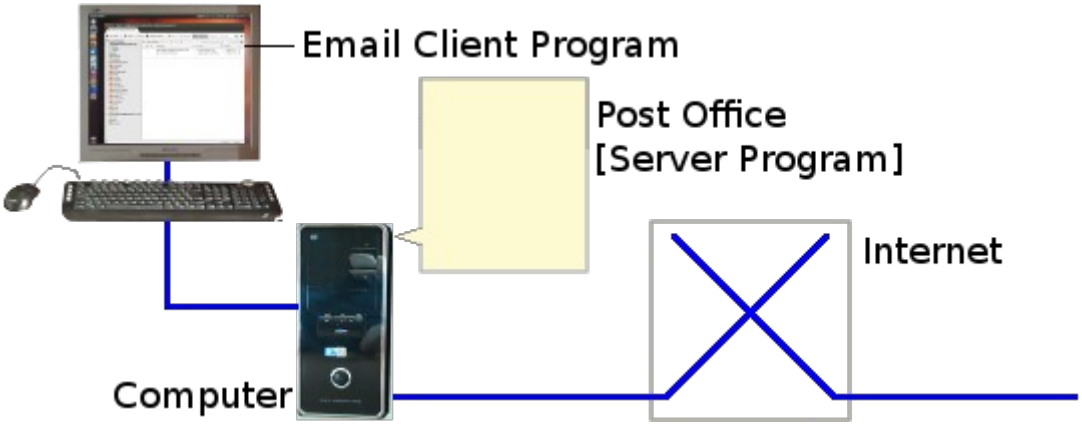
Graded Access Speed

Finally, on top of all the above impositions, there is a further inductive form of censoring that may soon be imposed by the major Internet Service Providers. They propose to provide higher data transfer speeds for the websites of those who are able to pay higher fees. These will effectively promote the dominant commercial websites backed by large corporations, burying websites - no matter how high the quality of their content - of individuals and smaller groups who simply cannot afford these higher fees.

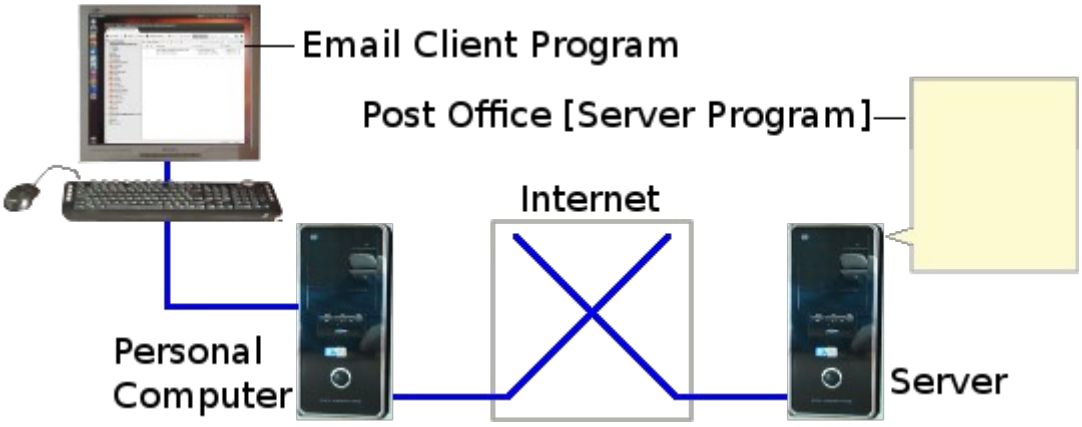
But this turn of events should be of no surprise to anybody. After all, it is simply capitalism in action. Once the Internet opened itself to commerce, its old egalitarian vision of universal freedom to exchange information was destined never to last. It had eventually to enter the real world in which the interests of the many are outweighed by the interests of the favoured few.

Web-Based Email Sites

Originally, each computer connected to the Internet had a Post Office server running all the time. People from all over the world could send an email at any time to the server. The server displayed an alert on the screen of the appropriate recipient when an email arrived for him. He then accessed it and read it. Thus the email system of the Internet was distributed and, by consequence, was reasonably private.

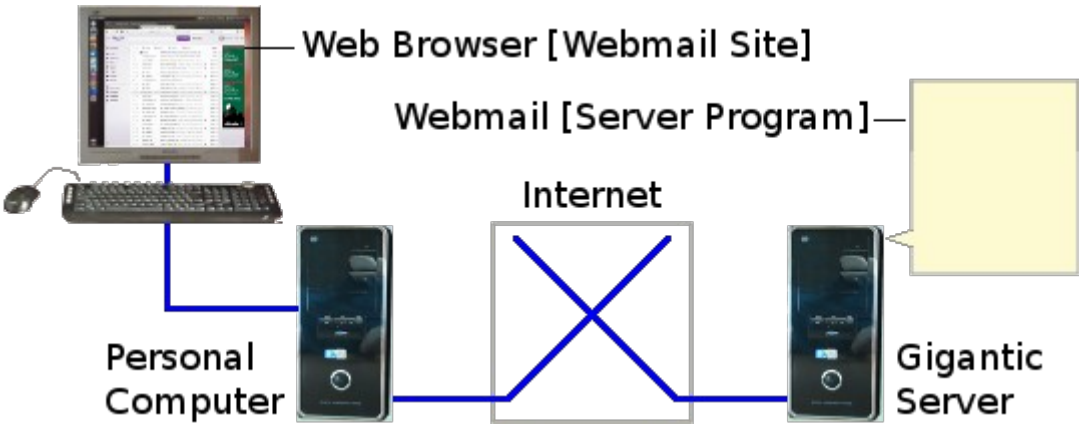


Running an email server requires the recipient's computer to be permanently on-line. This was fine in the day when the clients of the Internet were large Unix machines. Soon, however, small personal computers became the norm for the majority of Internet users. It is not normal, nor is it desirable, to keep these switched on all the time, so they do not lend themselves to running mail servers. The solution is to have a distribution of large computers permanently on-line running email servers. Each personal computer then runs an email client program, which can access its local email server from time to time to download any new mail. This is still a reasonably well distributed system.



Distributed systems are anathema to authorities. This is because they are difficult to monitor and control. The solution is to lure people to large web-based email sites. These provide an attractive user interface, which is served through a web browser. A user of a small personal computer logs on to his account at a web-based email site to send and receive his email. The US email site providers

dress up their user interfaces with lots of attractive artwork and advertise their "free" services. Whereupon, the vast avalanche of new Internet users flock to them from all over the world, like moths to a candle flame.



Email had originally been a channel for serious communication. With the advent of the web-based email giants, this abruptly ended. An ethos of total trivia quickly established itself. Now, people who have no real interest in email adopt a habit of forwarding endless jokes and stupidity to all and sundry. The result is that people's mailboxes become choked each day with truckloads of utter rubbish. Each has to spend ages getting rid of all this unwanted material and seeking out the few proper emails buried within it. This phenomenon is greatly exacerbated by the endless avalanches of unwanted and utterly abhorred junk advertising.

Many people cannot keep up with the necessary daily purging of junk from their email in-boxes. Vast numbers of email boxes therefore become abandoned as giant pus-balls of junk festering within these megalithic webmail servers. The abandoners then have no alternative but to establish a new email address. And the cycle repeats. What a stupid waste of resources!

Against this stressful backdrop is the perilous situation in which a statutory communication, such as a payment demand, can legally be sent by email and that its having been sent means that the recipient is deemed to have received it. Consequently, if the recipient accidentally deletes it along with the hundreds of junk emails among which it is buried, or if the email becomes misrouted, or if his Internet connection is down, or if his computer fails, then he is penalized. To my mind, this situation is an impractical absurdity, apart from being thoroughly unjust.

Unlike with the PC-based email client, the user of web-based email does not download his email into his own computer. Instead, it is left in his email account on the giant server of the web-based email service provider. Here, it is stored in supposed privacy. This privacy, however, is private so long as US law allows it to be so - either in general, or as may pertain to a specific user at a particular time. So, no matter what your nationality or country of abode, if an agency of the US government issues a legal instrument to the a US-based webmail service provider, to reveal to it your email archives, then it shall be done.

It is well evinced, by the nature of advertisement applets at the edges of my browser window, that the web-based email service provider trawls the content of my emails for clues as to what he is most likely to be able to sell to me. Notwithstanding, it is but a small step from here to trawling the content of my emails to see what political opinions or allegiances I hold and whether these be in or out of line with US government interests.

I find the monitoring and surveillance of the meta-data (such as the sender, recipient, subject and date) of an email disturbing. In the United Kingdom, so I am led to believe, the actual content of an

email is also monitored. I find this is even more disturbing. Monitoring, however, is a passive activity. It does not actively interfere with or disrupt the transit of emails.

Active intervention, on the other hand, definitely does interfere with and disrupt the transit of email. I used to write frequently to somebody on the other side of the Atlantic. Recently, however, Microsoft decided to block my emails from its network. Since my correspondent has a Hotmail account, my emails can no longer be received by him, although I can still receive the emails he sends to me. I also used to correspond with another person across the Atlantic. The subject matter we discussed necessitated that we exchange files attached to our emails. My correspondent has a Google mail account. We soon discovered that Google blocks the exchange of attachments of the kind we needed to exchange. This is direct and unauthorized interference with personal mail. I believe it would be classed as a crime if it were perpetrated by an individual. It would appear, however, that corporations are above the law.

Notwithstanding, the original email facilities of the Internet are still alive and well. Furthermore, I think the time is nearing when each home will be equipped with a domestic local area network. This will be connected to the Internet probably by a small, low-consumption server, which operates continuously. This server can then run the old-fashioned post office mail server, which can receive and send the home's emails, independently of any megalithic web-based service. This, however, will only work provided the Internet service providers (ISPs) leave open the listening ports required by post office mail servers. Disturbingly, there has been an increasing trend, over the past decade, for ISPs to close these listening ports.

Social Network Sites

Social networking can be done most simply and effectively through open websites and email. This, however, is outside corporate or state control or influence. And this will not do. The powers that be - commercial or political - therefore set their goal to induce the vast majority of Internet users to interact exclusively through a small clique of dominant social-networking sites.

I remember the early social networks as being quite useful. In the early days (around 2003), I could search MSN for - and find - other people in the world who shared my values, interests and aspirations. But not any more. The dominant social networking sites today such as Facebook stubbornly inhibit any attempt I may make to link with people of similar values, interests and aspirations. I quickly found that entering my interests on my Facebook page was not to help other people with those interests to find me. On the contrary, it was exclusively to help commercial advertisers target me with products based on my published interests. Understandably, I no longer have a Facebook presence.

The only people with whom I was ever able to link up with on a modern social network were people I already knew and people whom they already knew. These only knew each other through family or casual connections. Of all the "friends" I accumulated via social networking, none shared any of my values, interests or aspirations. Their conversations, to me, were always trivial, inconsequential and supremely boring. For common man, the exchange of information via the Internet has thus become impotent, relegating any serious grass-roots thinker to a voice crying in the wilderness where none can hear.

This has left television and other mass-media, once again, free to brainwash the public mind into forsaking its own well-being to serve the self-interest of the global elite. Once again, only those with lots of money - namely the state and the corporate - can make their voices heard.

This situation is not surprising. For thinking like-minded people throughout the world to be able to link up via the Internet, to exchange and develop ideas, is inherently dangerous for any global elite. So, through social networks, the Internet elite have managed to kill two birds with one stone. They have reduced to triviality practically all inter-personal communication between common people, while, at the same time, turning them into a captured audience for their highly-targeted commercial advertising.

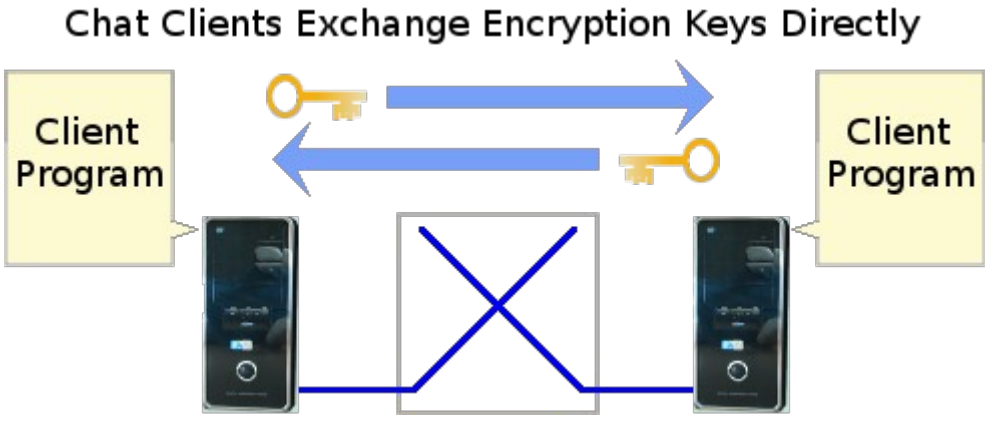
Centralised Chat Sites

Almost from the beginning, a method of encoding the human voice into discrete Internet Protocol packets was commonly available through a facility called Internet Relay Chat (IRC). There are many free open-source IRC client programs, which can be downloaded and run on practically any computer - at least any running a version or derivative of Unix. These operate in what is termed peer-to-peer mode. An IRC conversation is conducted actively by only the computers belonging to those who are parties to the conversation. Other computers en-route between them are only ever *passively* involved.

This allows any two people, each located anywhere in the world, to hold a private conversation, without the data packets carrying that conversation passing through any central server. Neither the identities of the parties to the conversation, nor the content of what they say, can be intercepted, monitored, recorded, interrupted or blocked by any third party interest such as a corporation or government agency. And for the powers-that-be, this again, simply would not do.

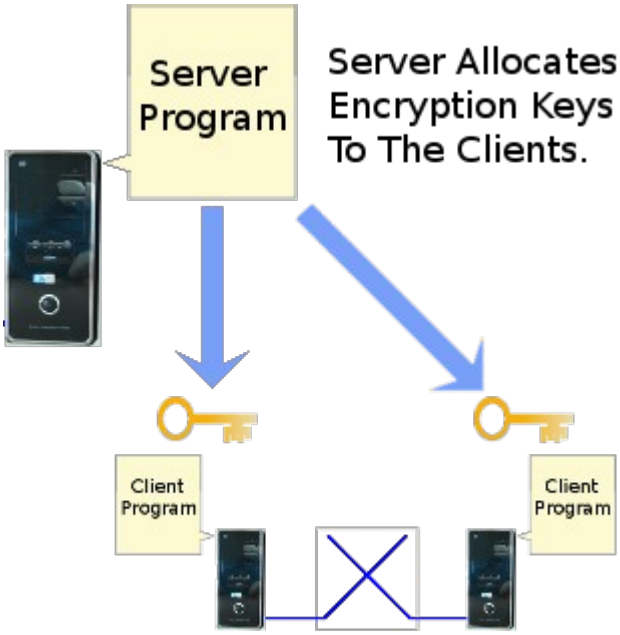
Consequently, as with personal web sites and email, large US corporations soon sprang up and pro-actively attracted the exploding base of worldwide Internet users to establish free accounts on their servers. The declared motive of these corporations was, again, to turn all the people of the world into a captured audience for their highly-targeted commercial advertising.

On these commercially-based services, at least the initiation of the connection between the two parties to a conversation is done via a corporate server. Thus, the metadata - the identities and Internet addresses - of the parties to the call are known. Information regarding who conversed with whom and when, for subscribers all over the world, is thus available on the corporate server. While this is very useful for marketing products, it is perhaps even more useful for surveillance. And being based in the US, all these corporate servers are subject to US law and so can be forced at any time, by any agency of the US government, to hand over this information.



The operators of these Internet chat services assure us that our privacy is their priority and that we need not be concerned because all our conversations are protected by strong encryption. Notwithstanding, the session encryption key for each call isn't created by the parties to that call. It is created by the service provider's client software installed in each party's computer. There is therefore

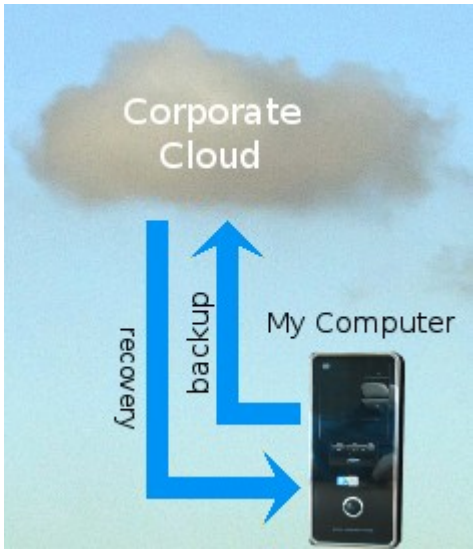
nothing to stop the service provider building in to his client program the capability of sending that key to his server if requested.



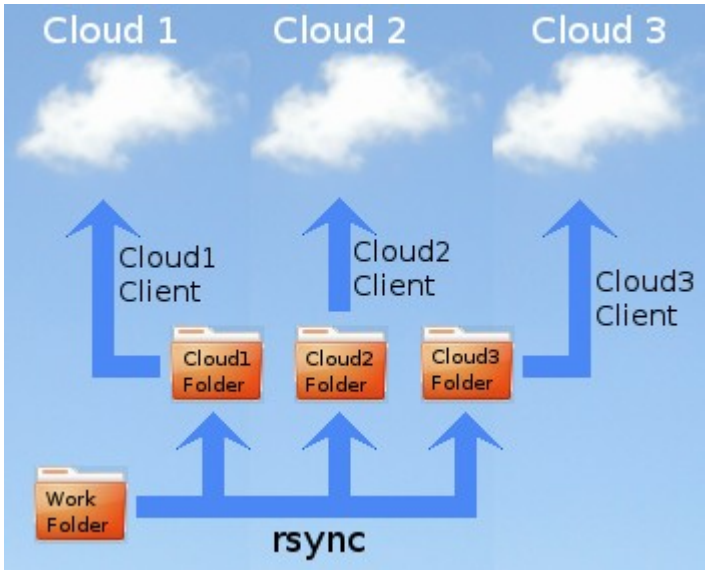
Furthermore, there is nothing to stop the service provider opting for the methodology whereby it is his server, rather than the client software, that issues the session encryption key for each call. In this case, any agency with access to the service provider's server can eves-drop on any conversation between any users worldwide. Hereby, the identities of the parties to a conversation, and the content of what they say, can now be intercepted, monitored, recorded, interrupted or blocked by any third party interest such as the service provider concerned or - by the appropriate legal instrument - any US government agency. And are we realistically to believe that if they can, they won't?

Cloud Storage Sites

A *cloud*, in this context, is a large mainframe computer - or even an array of such computers - which has a very large amount of data storage resources (such as disk drives) attached to it. This computer has very high bandwidth access to the Internet. Anyone may open an account on this computer via the cloud service provider's web site. This gives him an initial amount of free storage space. He may request more than this, but he will then have to pay so much a month for the extra space. To be able to use the cloud service to backup his data, he must download and install the cloud service provider's client software to run on his personal computer.



I think it was around 2008 that certain corporations started to offer limited amounts of *cloud storage* to people in general free of charge. Currently (early 2014) I subscribe to three cloud storage services on which I'm allowed between 2 and 5 gigabytes of storage for free. I use each to make an off-site safety backup of my work, which comprises my writing, software and research library. This all amounts to no more than 1·5 GB.



I have a separate folder in my **home** directory for each cloud service. I synchronize my work folder to each of my cloud service folders weekly, using the Linux **rsync** utility. Each cloud service provider's client software, running within my computer, then synchronizes its respective folder to my storage space in its cloud. I consider this two-stage approach essential to avoid any synchronization mishaps where the cloud service could possibly corrupt items in my work folder. This indeed did happen before I adopted the two-stage approach.

Cloud computers are equipped with high redundancy recoverable data storage resources. They are therefore super-reliable and dependable. Consequently, if ever my personal computer were destroyed or stolen, along with all my on-site backups, I could download all my work from one of my cloud accounts into a new computer. That is the great and primary value of cloud storage.

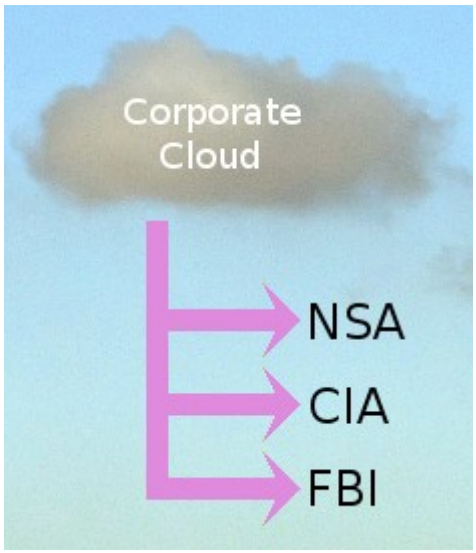
What motive do the cloud service providers have for offering people free storage? The amount of free storage they offer is small compared to the normal contemporary amount of storage available within a personal computer. Even my mobile device is currently equipped with a 35GB memory card. The average person tends to use up the space he has available, mainly by not bothering to purge outdated documents and photographs that did not turn out as well as he would have wished. Thus files tend to accumulate on his device and fill up its available storage space. As he uses up more and more of the storage on his personal device, so too he will want to back it up. And cloud storage is the ideal place. Consequently, he will quickly run out of his free allocation and have to buy more space from his cloud service provider. If the cloud service user is a company, then almost certainly the free space allocation will be insufficient right from the start. So the free space is, in effect, a pre-purchase free trial. Of course, there are some like me who keep their storage use well trimmed, even on their personal computers. But we are a relatively small minority.

Is this all there is to it? How is it that all these successful cloud service providers are American? Is the rest of the world full of inepts? What catapults these two-geek start-ups to world domination so quickly? There are lots of equally clever people in other countries. They obviously get copious starting capital. They obviously get administrative assistance and seem to find uncannily obstruction-free routes to rapid growth, which their would-be counterparts in other countries don't seem to get. Could it be, therefore, that what they are doing is extremely useful to certain powerful organs, institutions and agencies?

Is my data safe when stored on a cloud? As far as storage integrity is concerned, it's as safe as houses! It is extremely unlikely ever to get lost or corrupted. But is it safe from the point of view of privacy? If I store personal confidential information on a cloud, is it possible for anybody else to access it? "No," say the cloud service providers. Why? Because all my data is password protected. It is also encrypted by an encryption key that has been generated from my password. And I am the one who originates my own password. One cloud service says that even its own staff do not know my password. Consequently, nobody can have access to my information stored on its cloud, unless I deliberately make all or part of my data shareable.

Notwithstanding, all passwords are stored somewhere on the cloud service provider's computer. They may themselves be encrypted. But the decryption mechanism must exist somewhere on the cloud service provider's computer. It can thus be found by anybody with root (administrator) privileges. One way or another, the cloud service provider's system administrator, operators and programmers between them have the capability of accessing my data and decrypting it. Government institutions and agencies know this.

The cloud service provider and its computers are based in the US at the confluence of the global internet backbone. They are thus under the jurisdiction of US law. If, therefore, the US government or one of its agencies has reason to want to see my data, it can issue a legal instrument compelling the cloud service provider to provide it with a decrypted copy of my stored data. The US government or one of its agencies could even request that the cloud service provider provide it with a back door entrance to the cloud storage so that it could decrypt and inspect at will any or all data stored on the cloud. In my case, I think they would be extremely bored by what they found.



I remember a blog comment by a coordinator at one of the major (yes they do exist) non-American cloud services. He strongly advised that no file should be placed in cloud storage that had not been strongly encrypted separately by the user himself beforehand. This is an additional stage in my weekly backup routine that I did not mention above. I create strongly encrypted **.pgp** files from all my modified work files before placing them into their respective cloud upload folders on my computer. Provided my **.pgp** encryption keys do not become compromised, this gives me my best shot at maintaining my privacy.

The only further measure I could possibly take would be to copy all my modified work files onto a memory stick and encrypt them using an off-line computer that is never connected to the Internet. But that's a bit too much work.

For most of the inhabitants of Planet Earth, the cloud storage service is probably the one area of cyberspace in which they are most vulnerable to clandestine surveillance. This is because, within their cloud space, unlike in emails or on social media, they store practically *all* their personal information in a complete and organised form.

Portent From The Past

The best protection the individual can acquire for the privacy of information he transmits across the Internet is encryption. Current encryption methods are so strong that it is estimated that it would take all the computing power in the world a length of time equivalent to 5 times the age of the universe to crack the encoding and reveal the naked contents of an encrypted file.

The individual may thus encrypt his emails, including attached files, before he sends them so that they can be decrypted only by the legitimate recipient. He can encrypt files he stores on a cloud so that they can only be decrypted by himself in the event that he needs to retrieve the information stored within them. Provided his keys and files are not compromised within his own computer itself, encryption is nowadays invincible.

This does not suit the powers-that-be. It renders them blind. It strikes fear into their hearts. There is only one way they can fight this. That is to make encryption illegal. Remember Section 2, Clause 11(2)b of the "Terms, conditions and limitations" of the UK's Amateur Radio Licence I mentioned earlier. Even now, I hear murmurings of the desire in high places to put forward a Bill to enact a Law to ban the encryption of data sent by private individuals across the Internet.

Of course, it may be permissible to encrypt Internet chats, whether typed or voiced, so long as they are conducted via a centralized server where the powers-that-be can have access to the encryption keys via a back door. But direct end-to-end encryption between peers, including the off-line encryption of email attachments: no way. Such a ban may not succeed the first time. But it's coming. Mark my words.

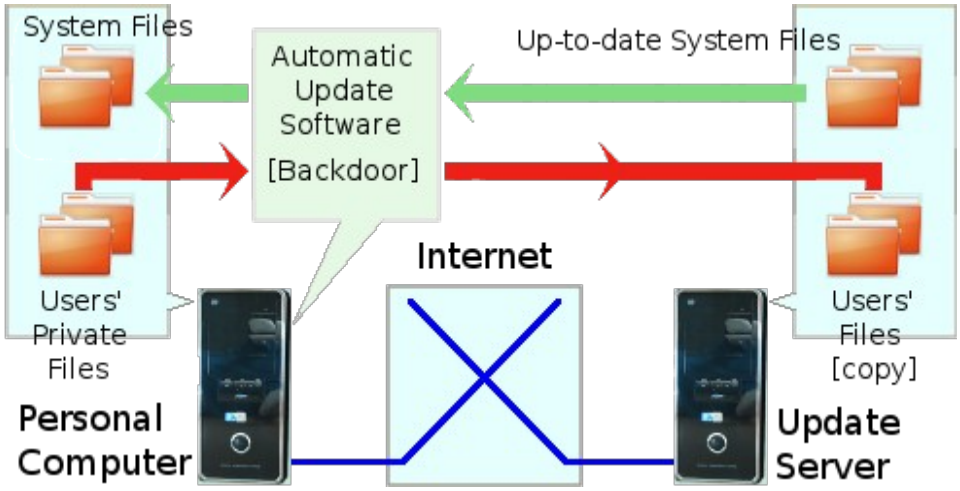
Infiltrating Your Computer

I think of the data storage space on the hard drive of my personal computer as my private territory. I feel sure that most people also think the same about their personal computers. Before personal computers were connected to the Internet, this was largely true. It was possible to infect a personal computer with a so-called *virus* via removable media such as a floppy disk. With a little care and a few precautions, however, this was preventable. But the Internet changed everything with regard to the security of one's own personal data within one's own personal computer. Nowadays, who knows who may be snooping around your hard drive poking their noses inside your personal files? It is as well to beware what you store within your personal computer.

Although it was possible, personal computers prior to about 2004 did not really have the speed and capacity needed to run Unix-derived operating systems. Most therefore did not have the enforced privacy and protection of Unix's user account system with its individual, group and general file permissions.

From their beginning, personal computers operated mostly with MS-DOS and then MS Windows. I don't know about after 2008, but up until then certainly, these had little or no effective security built into them. Security, if it existed, comprised third-party programs whose job it was to frantically scan the computer's storage for known viruses and "firewall" software that monitored incoming Internet packets for "suspicious activity", whatever that meant. The anti-virus scanners had to be regularly updated as the war between virus producers and the anti-virus software raged on. This, of course, resulted in an unwelcome on-going cost for owners of the personal computer.

Operating systems have now long included a built-in facility for automatically updating themselves via the Internet. This is well protected from malicious use by means of strong encryption and the exchanging of digital certificates. Notwithstanding, it does give the operating system manufacturer a secure back door into your personal computer.



The operating system manufacturer could, if he so wished, include additional functionality within his automatic update software. This could easily be a program to scan your hard drive for whatever he may wish to look for. The operating system manufacturer is an American corporation, which operates within US jurisdiction. If the US government, or any of its agencies, were to issue a legal instrument requiring the operating system manufacturer to provide access to any or all personal computers, then the operating system manufacturer would have no choice but to comply.

With a closed-source operating system running on your computer, you can have no idea of what's really going on "under the hood" - behind the glossy graphics user interface on your screen. It could be passing your personal data, through a back door, to goodness knows where on the grounds of US national security.

The operating system itself is not the only possible source of insecurity to the private information on your computer's hard drive. Application programs can also snoop on your private data. Perhaps the greatest culprit here is the web browser. There are at least four means whereby a web browser can cause information about you to be gathered and sent to an unknown destination. These are: cookies, browser plug-ins, JavaScript programs embedded in web pages and Active-X controls.

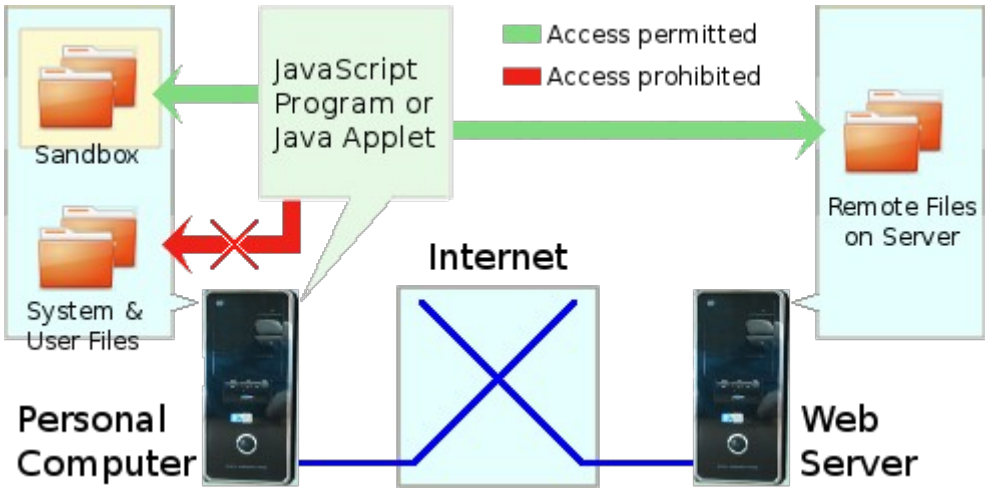
Cookies really only gather statistics about your browsing habits, i.e. what web sites you have visited. They probably don't even identify you as an individual. They could pass on your IP address. However, the average user's IP address changes at least every time he starts his computer. A cookie is useful in that it can enable a particular web site to "remember" your preference settings and log-in details for that site. However, the fact that it preserves such data leaves your details vulnerable to being picked up by any malicious agent lurking within the browser environment.

A web browser can also have, installed within it, little "helper" programs called plug-ins. These enable the browser to do things like play movies or sound streams through embedded objects within the browser window. However, the producers of these plug-ins could easily include additional functionality that is nothing to do with the task in hand.

JavaScript programs and Java Applets are computer programs that are embedded within a web page and are executable while the page is being displayed. They are useful in that they can automate forms that you need to fill in on a web page. I use them to automate the illustration of certain things in other parts of this web site.

JavaScript programs and Java Applets, according to their original functional concept, are perfectly safe. This is because they are confined to run inside what is termed a *sandbox*. This means that a JavaScript program or Java Applet fundamentally cannot access or store anything on your computer outside the browser's own dedicated temporary folder. It can read data from, and write data to, the

server from which the displayed web page was served. But there is absolutely no way that it can look at, add to or modify anything anywhere else on your computer, including your private files or folders.

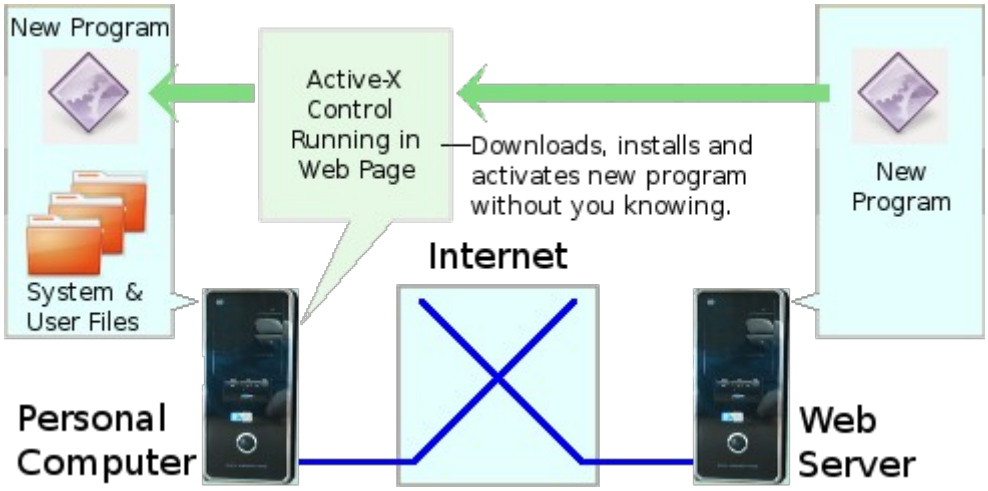


I became very frustrated two or three years ago when I noticed, on somebody's Windows machine, that when Microsoft Internet Explorer loaded some of my web pages, it displayed a terse warning message to the user saying that my page could possibly harm his computer. This, of course, was an utter lie. There is no functionality within my code that can possibly harm anybody's computer. In fact, the code concerned simply displayed, in the browser's status bar, the date that the page was last modified. It did not do, nor could it do, anything more. My JavaScript code was clearly there to be seen in the web page's source. Anybody with only a rudimentary knowledge of JavaScript could see that it could cause no harm.

So, why the warning? I can only speculate that it be because of the following:

1. Microsoft extended the capability of the version of JavaScript, which it has implemented in its Internet Explorer web browser, to be able to be used in such a way as to harm the operation of, or access the data stored within, somebody's computer, and
2. Microsoft's facility for detecting the presence of JavaScript code in a web page is not sufficiently intelligent to be able to determine what that JavaScript actually does, and
3. Microsoft's JavaScript detector played safe by, in the circumstances, presuming the worst and condemning my JavaScript code as potentially malicious. This I perceive as a tort of defamation against me, as the author of the site, in that it effectively labels me as being under expert suspicion of having the malicious intent to harm the user's computer.

Microsoft's version of JavaScript can be used, by a web page, to download and run ActiveX controls. These are, in effect, native programs that run on your computer as if they were applications invoked and run by you. They are thus not confined to the browser's *sandbox* folder as were Java and JavaScript programs that conformed to the original concept.



Consequently, an ActiveX control can, be it designed to do so, access your entire filesystem, including your personal private data. Why introduce this glaring vulnerability? Because it facilitates something that many people find useful. It enables teams of people to use application programs, like word processors and spreadsheets, seamlessly across many computers connected via the Internet, as if they were a single computer. But was it worth it? In my opinion: definitely not.

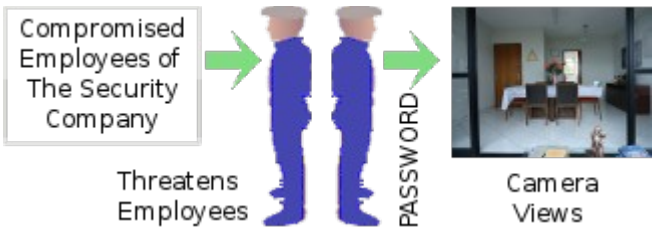
The upshot of ActiveX is that danger can come simply by your accessing a rogue web site. The content of the web site itself may be quite benign. Notwithstanding, a web page could contain a program, embedded within it, which is capable of downloading a native program into your personal computer, and hooking it into the operating system so that it will, forever after, be running whenever your computer is on. Not all downloaded programs do this. But they could. The capability is there.

Exacerbated by Naïvety

The predatory surveillance, by foreign powers and common thieves alike, which takes place over the Internet, is willingly assisted by the incredible naïvety and gullibility of the general public, who flippantly label all dissenters as paranoid. One particular example is as follows.

Recently, the residents of the condominium of apartments where I live decided, at great cost, to install "security" cameras all over the building and its approaches. The camera images are supposedly viewable by all the residents on their home computers via the Internet. I have 3 computers, plus a laptop and a tablet. However, the camera viewing software, as supplied by the vendor of the camera system, is incompatible with all of them.

Fortunately, I discovered an installation of Microsoft Windows XP in an old disused partition on my laptop's hard drive, which contained no personal data. I downloaded the camera viewing software and was able to view the camera images. The definition was so poor that it would be impossible to identify anybody from the images. So they couldn't be used to catch a thief.

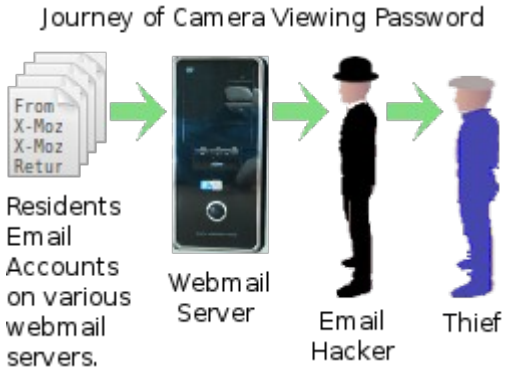


Any employee of the security company, who administers client passwords, can access the camera views. Such an employee is vulnerable to being bribed or threatened into revealing our building's password to a potential thief. For instance, a thief could research a particular employee of the private security company. He could find out where the employee lives. He could find out where the employee's children go to school and photograph them. Then he could threaten the employee

concerning the "safety" of his family if he did not reveal the password. The thief could then access our cameras over the Internet just as we can. He could then take as long as he likes to "case the joint", seeing who comes and goes and when. And if for our building, why not for many or even all buildings who subscribe to the security company's camera plan?

The password for the camera views was included with the instruction document on how to install and use the viewing software. This document was in a PDF file kept on a public dropbox server. The condominium administrator distributed the open web link to this PDF file in an open email sent to each of the residents. I know of residents whose email accounts are on Yahoo, Hotmail and Gmail. Other residents probably have email accounts on many other email service providers. Some residents may download their email into an email client. Others may access their emails directly on the host servers.

It is well known that the email service providers scan our emails for the declared purpose of targeted marketing. And who knows what else for who else? So any employee, of an email service provider, with access to email scanning facilities, can access or pass on the link to the camera instructions and hence our building's password.



Furthermore, each resident doubtless has a contacts list, within his email account, listing the email addresses of his friends, acquaintances, colleagues and various others. These all, in turn, have contacts lists. By using any of a whole range of fairly simple hacking techniques, such as writing an appropriate macro for an email client, any one of an open pyramid of contacts could become the route whereby any one of our resident's email accounts could be unknowingly compromised. A resident could also inadvertently include the link-bearing email in a "reply to all" on his contacts list.

I recently watched a friend buying something on-line from a vendor's website. The buyer was asked to enter his email address so that the vendor could send an email confirming the details of the purchase. The buyer was then required to enter and confirm a password. We assumed, at first, that this was to be a new password for the buyer to register as a customer at the site. So my friend entered and confirmed a newly made-up password. A message box then opened saying that the password was incorrect. Then I noticed that, underneath the password entry field, a short explanation had appeared. It explained that the vendor needed the password to my friend's actual email account, which was necessary in order for the vendor to verify that the email address given was, in fact, the genuine email address of the buyer. My friend decided not to make the purchase.

Of course, my friend could have given the vendor the password to her email account and then changed the password of her email account as soon as the account had been verified by the vendor. Notwithstanding, once the vendor's automated system had logged into her email account, she would be unable to access it until the vendor's automated verifying system logged out. During that time, such a system could scoop up an awful lot – if not all – the content of all her emails. It could, in fact, should it have been programmed to do so, change the password to her email account and thereby lock my friend out of her own email account. I am not saying it would, but it could.

I wonder if any residents of my condominium building have bought anything from this very large and popular on-line vendor. If so, that company, some of its employees, its software provider and some of its software provider's employees potentially have full access to their email accounts. And hence to the building's camera system and to the hard drives of the residents' computers.

Once the link has been acquired and the password discovered, anybody can get the viewing software, as it is a generally available package with minimal configuration required to suit the individual installation.

The viewing software was written as an Active-X control, so I am thankful that I had absolutely no private data in that Windows XP partition. Who knows what back doors the security company or its software provider built into their closed-source Active-X control? Its compressed installer alone is over 104 MB. All this just to select and display video streams through a browser's video plugin?

What could the rest of this rather over-sized program be up to? Technically, it could contain code to enable the security company, its software provider or any of their relevant employees to access whatever information may be stored on the computer of any resident of our condominium who has the proprietary viewing software installed.

A Precipitous Event

A so-called security issue occurred at our condominium building on the 2nd of March 2015. The inter-phone in my apartment rang. My companion answered. It was the young man who brings our hot lunch on Mondays, Wednesdays and Fridays. My companion recognised his unmistakable voice as he said "Marmitex", the name of his employers. She took the lift to the entrance and went out into the street to take the lunch pack. While my companion was on her way down, the inter-phone rang again. A voice simply repeated "Marmitex". But it wasn't the voice of the young man. Apparently, at the instant the young man pressed the button for our inter-phone, a very large muscular man arrived. He was the one who had pressed the button a second time and repeated the word. The young man gave the lunch pack to my companion and went on his way.

The large muscular man told my companion that he had an appointment with a foreigner to repair some furniture units. He gave our apartment number. I am the only foreign resident in the building. My companion said she did not know about any such arrangement and that I certainly would not make such an arrangement without her knowledge. She told him to wait. She re-entered the building to return to our apartment to ask me. She opened the gate and went in. Before she could close the gate again, the man had slipped in behind her like a slithery snake. There he was, inside the building. My companion had no way of expelling him. He was three times her size and very strong. She had no option but to continue taking the lift up to our floor. The man followed tightly behind her. I heard them talking as they emerged from the lift.

I opened the kitchen door and my companion slipped through. The man tried to snake in behind her. I closed the door to a narrow slit and placed my foot to stop him opening it, trying to look as menacing as I could. The man was quite theatrical. He created a strong expression of having recognized me, by which he tried to induce a complementary reaction from me. I was puzzled at first but affirmed that I had not made any appointment with him and that I had never laid eyes on him before. He then tried to convince me that we had met before and that I should let him in to see about the furniture repairs or modifications that we had arranged. All the time he was dancing around, like an over-sized monkey, with his head almost in the door, desperately trying to get as much a vision of the inside of our apartment as he could. I remained adamant.

Eventually, he gave up and pulled away. He apologized, saying that he was sorry but he had so many people to remember that he sometimes got confused. He said that it wasn't the 4th floor he remembered, it was the 8th floor. My companion then made the mistake of mentioning the name of the person on the 8th floor. The man then in a triumphant voice affirmed that the name my companion gave was indeed the person with whom he had made the appointment. The person on the 8th floor later related to us that the man had gone through the same routine with him, except that the arrangement he claimed to have made was to paint a bannister rail. I wonder why the change of story. The resident on the 8th floor sent him away.

The man then seemed to spend some time wandering the building, with which he seemed uncannily familiar. My impression was that he was neither a carpenter nor a painter. He had a very small light canvas tool bag in his right hand. I was worried at first that it could contain a gun. However, after scrutinizing it, I saw that it could only contain very small light tools such as those used by an electronics, computer or telecommunications technician. He eventually let himself out of the building and slinked away.

Paranoid Reaction

I have related the story of this man to provide context for explaining the inverted perception most ordinary people seem to have regarding cyber-security, as illustrated by the paranoid reaction to this event by the Clique of Four who make it their self-appointed business to decide how our condominium is administrated. One of the things they decided was that there should be a list of do's and dont's regarding how people enter and leave the building or allow non-residents to enter. This was an excellent and sensible suggestion.

Notwithstanding, this was followed by the proposal that the security company (who supplied the original cameras) should be consulted for advice on how to improve the security of the building. Of course, surprise, surprise, they recommended that the condominium spend more money on more cameras. The innocent motive of commerce. This, of course, provides any band of thieves, with a computer-savvy member, an even better facility for casing the joint.

Then, after castigating my companion for mentioning his name to the man, the inhabitant of the 8th floor (one of the Clique) came up with the brilliant suggestion that all residents should form a group with the name of the condominium on Whatsapp (a social media facility popular at the time of writing)! Don't mention anybody's name and apartment number to any stranger in the building but publish an identifiable organized list of the names and phone numbers of all the residents to the whole world.

As far as I know, Whatsapp does not have a group search facility at this time. Nonetheless, there are several bolt-on third-party apps, which facilitate group name search with geographic constraints. Besides, there is nothing to stop Whatsapp itself adding such a facility at any time. Use an inverted database view of the phone directory to link phone number to address and Bob's your uncle, or rather, Ali Baba's dream. The potential thief thus has the name of the building, a list of residents with phone numbers and hence apartment numbers, plus the facility to watch who enters and leaves each floor of the building and the main door by way of time-stamped video streams.

A Personal Experiment

By the time of this incident, I had long since erased the old Microsoft Windows XP partition from my laptop's hard drive. I desperately needed the extra space for the Linux installation. Consequently, I could no longer run the security camera supplier's proprietary camera-viewing software. Since I was being charged for the security service anyway, I decided that I had right of access to the camera

video streams for our condominium building. I spent 4 hours researching for relevant technical information on the worldwide web, constructed the necessary Real-Time Stream Protocol (RTSP) requests, put them into the standard VLC video player and up popped the 12 camera views. All without any of the vendor's proprietary client software. The first thing, of course, that shocked me was that these video streams are unencrypted. They are completely open.

Reading further, I discover that the Digital Video Recorder (DVR), installed in our condominium building, runs Linux and has only weakly protected telnet access. With this, I can effectively get command of the system as the root user. I thus have access the full command set not only for accessing the camera video streams, but also for playing back *and/or erasing* video from specified past time periods, or even changing the content.

I discover other information about how to use ping-like utilities to sniff out the IP addresses of RTSP servers. With these I can build lists of the IP addresses of local video stream servers, many of which will be the DVRs of other local condominium buildings. I can then probe Port 554 in these servers to latch into the video streams from these other condominiums. I can also log into these servers via telnet and assume the same command options. The DVRs of other condominiums are, naturally, protected by different 6-digit passwords. However, these can be rapidly cracked by looping the RTS sniffer command and piping it via a utility such as .

And I am certainly not a hacker. Not by any stretch of the imagination. It seems to me that these camera systems are negligently unprotected. The worldwide web is replete with articles about just how vulnerable they are. The only way to make a camera system secure is to make it truly CCTV, that is CLOSED circuit. It should be connected in no way, by either cable or wireless, to anything outside the building. Specifically it should not be connected to the Internet.

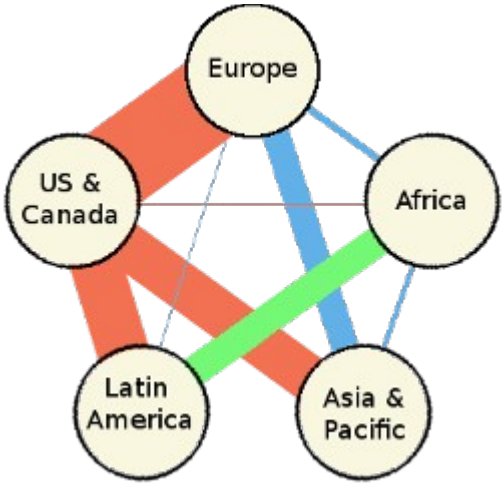
The camera system is not the only way that personal data of residents may fall into the hands of criminals. The condominium administrator sends a bank payment slip for the monthly condominium fee each month to each resident. The bank payment slip is sent as a PDF file attached to an email. The resident has no choice but to receive it this way. The PDF file is not encrypted. It can therefore be read by any hacker who may manage to gain access to the resident's email account. The bank payment slip contains not only the resident's name and address, but also various other identifying codes and numbers pertaining to that person. It is therefore a prime source from which a criminal can build a full profile of the resident. So even if, as I, one would naturally take all sensible precautions regarding Internet security, one can still be forced, by petty officialdom, to leave oneself vulnerable.

Perhaps nothing bad will ever happen. Perhaps, by luck, no thief will think of stealing items from the residents apartments or personal or financial data stored on their PC hard drives. Nevertheless, I think it is very stupid to spend other people's money on a system which undoubtedly reduces the security of all concerned, leaving their comings and goings open to view by who knows whom.

Thus, foreign government agencies are not the only entities who can nose around inside the files stored on your personal computer's hard drive. So too can private companies, their employees and whosoever might compromise their employees, including common thieves. And if they can, they will. As regards the Internet, there is no such thing as paranoia, only naivety. In modern cyberspace, your computer is a house of glass in a savage land owned and ruled by marauding forces you cannot see, as the vast expanse of Asia was once owned and ruled by the fear of Genghis Khan.

A Cyberspace Policy

The highly asymmetric imbalance in the current architecture of the Internet's global backbone facilitates and encourages the totalitarian control of cyberspace by the government of the United States of America and its agencies. In my opinion, this is not healthy for anybody - including the Americans. The distribution of the total data bandwidth among the links of the global backbone should follow much more closely the distribution of global population.



The first and most pressing need in the essential quest to rectify this imbalance is for a South Atlantic Link. This should be a secure data super-highway between Brazil and South Africa, as shown in green on the left. To ensure its robustness, it should use fibre-optic and microwave technologies with fall-back all the way to a slow HF spread spectrum link as an ultimate recourse. It should also be built from native technology and manufacture: not imported. This is to ensure that no outside political interest can implant covert back doors within the technology whereby the link could be monitored, controlled or even shut down at will by a foreign power.

The South Atlantic Link could then become the first phase of what could become a BRICS backbone for the Internet, linking Brazil, South Africa, India, Russia and China. I think this would go a long way towards rectifying the current imbalance. Nodes within the BRICS backbone would then become natural choices for locating non-American search engines and other Internet service resources. If other economic blocs of the world then further the homogenization of the global backbone, cyberspace should gradually become the common heritage of mankind rather than the private property of those who rule the United States of America.

The presence and growth of the Internet demonstrates a desire - which has turned into a need - for individuals all over the world to be able to communicate with each other. This includes not only intellectual communication between peer and peer, but also collective communication between broadcaster and audience. The Internet has answered this desire well. It does, however, have a disturbing draw-back. It requires for its operation a large, complicated and expensive high-technology infrastructure. And this infrastructure is currently, for the most part, owned by large private interests, all too many of whom have exhibited rather poor behaviour towards the individual user. For example, have you ever vainly attempted to cancel an account with a telecommunications giant?

It would be far more comfortable and far less stressful, for the individual inhabitant of Planet Earth, if he were able to communicate with any of his human peers by natural means - independently of any intervening artificial infrastructure. A possible solution could be to replace the Internet with a global patchwork quilt of *ad hoc* wireless networks. The necessary long-reach bandwidth would be attained through the massively parallel nature of the quilt.

An *ad hoc* wireless scheme provides the individual with independence from corporate domination. Notwithstanding, it does place on each individual the public obligation to contribute to, and participate in, the scheme. And it still depends on very complex - if not proprietary - technology.

Another option - which could in any case be used as fall-back - could be a scheme based along the lines of amateur radio's 2-metre relay service. With this, a radio amateur, entirely at his own expense, provides a relay transceiver operating on the 2-metre amateur band. It is left switched on all the time and automatically relays calls from other radio amateurs on to the next relay. Thus one radio amateur, in one part of the world, can hold a conversation with another radio amateur, in another part of the world, using the relatively short-range 2-metre band. This scheme could use relatively low technology. Equipment could even be self-built by the enthusiastic user. Of course, the bandwidth available is vastly lower than the Internet or WiFi provides. On the other hand, the truck-loads of superfluous graphical decoration, which uselessly flow daily around the Internet, impose an enormous bandwidth overhead, which the naked information content doesn't really need. The bandwidth offered by 2-metre relay is certainly sufficient to carry a Short Message Service or even email.

All modes of HF transmission, including a suitable adaptation of spread-spectrum, offer yet another even lower bandwidth option for inter-personal communication worldwide. This too would make an excellent fall-back option in the event that the faster more complex options should fail. Privacy for all these communication options - Internet, *ad hoc* wireless, VHF (2-metre) and HF - should be effected by end-to-end encryption established and maintained by the individual end-users.

To protect the interests of the individual user within his personal computer, we need to revert to secure open-source operating systems. Then, at least any competent programmer in the world - whatever his allegiances - is able to see clearly all that is going on "under the hood". What is happening or can happen within one's computer will thereby be in the public domain, and hence will be open to public scrutiny.

To furnish the individual with his self-evident right of unencumbered access to the entire rich content of the whole of the worldwide web, some kind of global non-censoring search facility is needed. I think that this could best be done in a distributed way by open-source software running within a new generation of domestic servers, which are left running continuously.

For the time being, the web search engine is no longer an effective means of disseminating intellectual discussion between people of like minds. Other means must be sought. Perhaps the best is to convert web articles to PDF files with file names that comprise a list of relevant keywords. Then place them on various file sharing networks like gnutella, eDonkey and Freenet. Interestingly, since I started serving my PDF files on these networks, the hits to my web site increased several fold. This is probably because my PDF files contain hyperlinks which refer to other pages on my actual web site.

Conclusion

All the foregoing having been said, why should I be perturbed by the fact that the all-seeing eye of the US government and its agencies is able to read my emails and spy inside my private files on the hard drive of my personal computer? After all, as many are quick to retort, "if you have nothing to hide, you have nothing to fear". Whether or not I have anything to fear - and hence to hide from them - depends more on the dubious nature of their motives and ambitions than on the quality of my moral integrity.

I could therefore, unknowingly, have much to fear and consequently, much to hide. I am simply one of those strange individuals who would feel uncomfortable and embarrassed at having to live in a house with glass walls.

Of course, the US government is not the only villain of the piece. Many other countries have clandestine agencies like the Israeli MOSSAD and Britain's infamously secretive and invasive GCHQ. Their motives and ambitions must be, at least to some extent, different from those of the US. However, none of these, at present, sits at the confluence of the global Internet backbone. Perhaps, if and when the backbone becomes more homogeneous, the threat to individual privacy will become more distributed, balanced and hopefully more diluted. I think that would make me feel safer.

Cyberspace thus does not have the nature or character of a sovereign state, nor even of a confederation or a political alliance. It has more the nature of the high seas, where dominant maritime powers vie to consummate their respective ambitions. But there is a difference. The high seas lie outside all sovereign territories. Cyberspace does not. Cyberspace is everywhere. The upshot is that a dominant sovereign state may rule that part of cyberspace that lies within its sovereign territory according to its own sovereign law. However, this does not bind it so to do in that part of cyberspace which lies outside its sovereign territory. There it may, should it choose to do so, behave like a marauding buccaneer on the high seas, free of the constraints of its own internal laws - or indeed, of any laws at all. Its behaviour will therefore be most likely determined by the covert strategies of its secret agencies.

What is the purpose behind these covert strategies? It is to gather, by all means fair and foul, intelligence that will facilitate the ambitions of these agencies' masters. But who are these agencies' masters? Are they the taxpaying citizens of the sovereign state these agencies serve? Supposedly, but no. Their real masters are an international faceless elite, who strike dubious deals with warlords and dictators, to take for themselves, from the poor of all nations, all the wealth of the Earth for the price of a banana. This super-regenerative process of escalating disparity is inherently unstable. It cannot be sustained. The time must therefore come when unfettered knowledge will blast away the scales, which currently blind the eyes of mankind from the reality under which they live. Then humanity will rise and take back its lost inheritance.

This article is also available in Portuguese.