

A lighthouse at night with a bright beam of light shining out. The lighthouse is illuminated from within, and the beam of light is very bright and focused. The background is dark, and the lighthouse is the central focus of the image.

Internet lockdown or the end of freedom

by Vincent Maher

Some time in the near future we may well find ourselves looking back and realising that the combination of the dot-com crash, the legal action against Napster and the Bush administration marked the end of a period of cultural freedom on the Internet. The signs of this change are among us right now, but it might already be too late to reverse this trend.

There are three key areas where the rights and freedoms that seemed to be intrinsic to the Internet – built into its very fabric – are being bludgeoned with a very blunt instrument, an amalgam of the law, fear, ignorance and silence. The first has been termed “net neutrality”, the second revolves around intellectual property rights and the third around privacy and surveillance. The current incarnation of each of these aspects of the Internet is precisely what makes it a radically different type of mass medium that is, at least theoretically, more democratic and so, as the theory goes, better for our global culture than the endless looping of MTV and the Cartoon Network.

Even the most hardened geeks tend to switch off when someone invokes the register of Internet governance or net neutrality, not because it seems irrelevant but because it seems to be in the same league as fighting for environmental rights, a battle in an arena where the real players are too big for one individual to take on.

Network neutrality

In short, network neutrality means that all websites and services have equal access to the available bandwidth on the various telecommunications networks that make up the Internet. This is how it has been since the beginning, if you ignore China and other countries that censor the web for political and economic reasons. The issue of neutrality came into the spotlight recently when an amendment to the US Telecommunications Act that would have specifically protected net neutrality, was defeated in a lobbying burnfight (read more details about this on savetheinternet.com).

The outcome is not conclusive, but what has become apparent is that many of the large telecommunications companies in the US would like to see a scenario where they can legally throttle or slow down websites that do not pay, while simultaneously speeding up the services that they either own or have partnered with. This type of scenario hearkens back to the idea of privately-owned and restricted networks that use the Internet as their backbone, much like the Microsoft Network (MSN) in the early days.

If we imagine the Internet organised around these principles, there doesn't seem to be much difference between it and the current mass media like cable or satellite TV: you'd have to buy a package that includes the websites you want high-speed access to.

This is probably an unnecessarily pessimistic vision and, no doubt, the actual outcome would be something more palatable. As usual, it comes down to money. Each web user pays to access the Internet, each website pays its Internet service provider (ISP) for the bandwidth it uses, and each ISP pays for the bandwidth it uses to the large infrastructure providers. If I were an optimist I'd think that changing large websites for high-speed channels across the Internet might bring about a further decrease in ISP charges but the fact remains that the possibility would legally exist for a curtailment of our freedom to surf.

Intellectual property rights

Much like the egalitarian allocation of bandwidth, the protection of intellectual property rights involves a balancing act between market forces and the freedoms of individuals or corporations.

In the beginning, the World Wide Web was designed to

be a space for sharing and collaborative work. The original architecture of the web was intended to allow anyone to read and write a page, the way a Wiki works today, but this was never implemented to its full extent. There was a definitive period between the days when peer-to-peer (P2P) file-sharing networks like Napster and Audiogalaxy started up and exploded the traditional notions of copyright ownership in the music and movie industry, and the time when the big corporations woke up and started their legal reign of terror on the web. Since then we have seen the collapse of many P2P networks, children and 80-year-old grannies sued, and a propaganda machine that spins a suffocating yarn of anti-piracy talk.

The moral and ethical issues of digital piracy are more complex than a simple equation with stealing a handbag or shop-lifting: copying is a theft of potential business with no conclusive evidence that it prevents those sales from taking place anyway. In many ways, the sharp response from the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) is an attempt to use the legality of copyright to bide some time while they figure out how to deal with a fundamental flaw in their business model in the age of the Internet. The recording industry is based substantially on distribution and, like estate and travel agents, are increasingly finding themselves out of the distribution loop.

The extent of the corporate response to this is various. On the one hand, online shopping solutions like the Apple iTunes Store have been successful and have demonstrated that people will buy music online if the price and configuration is right and convenient. On the other hand, the enforcement of ownership and the rights to copy are being built into the hardware and the software of the future – the term Digital Rights Management (DRM) refers precisely to the structural incorporation of the logic of ownership into the very machines we run at a fundamental level.

The newest generation of DVD standards (Blu-ray and HD-DVD) both use Advanced Access Content System (AACS), a DRM implementation that will effectively prevent the playback of high-definition video unless your monitor or video card do not also use a specific standard for copy-protection developed by Intel. What this means, in plain English, is that the fair-use that copyright law currently affords you, will be extremely difficult if all your hardware is not compliant and, even then, you will be at the mercy of the hardware manufacturers and standards developers. Your computer will have a legal framework built into it.

The other side of the coin is the advocacy groups emerging to protect certain freedoms, like the freedom to give away your work on a license less restrictive than copyright. Organisations like Creative Commons have been particularly visible in this area, offering a public license that enables the creator to specify what others can do with their work. While it is often difficult to fully grasp the significance of Creative Commons, it is easier to understand if you strip away all the rhetoric and consider it practically: whenever you create something, copyright is automatic; you don't even have to put a © on it; so people tend to avoid building on the creative work of others for fear of retrospective legal action; the Creative Commons license allows you to build on the work of others in a way that protects you legally if you become a superstar one day. It's that simple. The spin-off is explicit cultural freedom from the legal framework.

Surveillance and the illusion of anonymity

So far I have discussed threats to the freedom within the mechanism of the Internet itself and threats to the freedom to use and build on the culture that is forming within the medium. More often than not, freedom is an illusion of anonymity. We can track an increase in surveillance everywhere, from cameras in cities to the massive mobile phone or ATM networks that can pinpoint our location, movement patterns and habits quite accurately.

One of the consequences of the American war of terror is the polarisation of society and the unlikely willingness of individuals to give up their rights in exchange for reassurances of national security. This conservatism and ethnic protectionism has created a psychological groundswell that somehow paints those campaigning for civil liberties as irrelevant agitators or hippies, out of touch with the ‘real’ problems faced by the West.

Ironically, the Internet may seem like a haven for those who crave anonymity from the airport scans, the cameras and the forms. I say ironic because the Internet, if one conceives of it as a virtual space, is the most monitored environment you could go to, it's simply not visible, hence the illusion of freedom. This, too, is changing.

In South Africa it is now illegal to give someone anonymous access to a computer network, and access providers must store that information for a set duration and be available to hand it over if the government wants it.

In the US, the government issued a subpoena for search records recently, and Google was the only search provider to resist the pressure in a public battle that took place simultaneously with their decision to allow their search results to be censored by the Chinese government for the sake of increased market share.

The simple fact is that most, if not all, websites keep a record of your IP address (the unique number that distinguishes the computer you are using from all the others), the time and date, the previous site you were visiting and other information. This would allow someone with reasonable technical expertise to figure out your entire online life.

It makes you wonder, then, why people think the Internet is the Wild West, where anything goes. Perhaps it is because many still consider it not to have the same weight as the traditional media. Last year, for instance, some visitors to the Guardian Online were up-in-arms because the *Guardian* printed comments they submitted to the website, even though the Guardian was within its rights to do so.

In another conversation, a blogger told me she was considering deleting five years of her personal life history because she was about to apply for a new job. Suddenly the weight of her public history was too much to bear, and I can understand why.

Like the recording industry, governments and police are waking up and realising that these records exist, that they can be extracted and used as evidence in a prosecution. With this knowledge comes a culture of internalised surveillance in which we constantly have to remind ourselves that everything we do can resurface later, that ambiguity and experimentation with ideas and actions on the web can emerge as damning evidence later, in a different context.

There are other aspects to this too, that revolve less around privacy and more around the level of visibility of one's public activities. Erasing a record online is becoming increasingly difficult as search engines like Google cache pages of the web so they remain available even if you delete the original. Bloggers might copy and paste something you said, others may save it to their hard drives. In fact, I have seen several instances of private conversation via email erupting onto the Blogosphere. It has reached the point where you need to specify a license agreement for the reuse of the content of your email, to protect confidentiality.

Let's put this all into a dark premonition: in 2016 the speed at which websites get to you will be determined by commercial agreements beyond your control or the capacity of your network, your computer will not let you do much except what is strictly and bluntly legal and you will be nagged by paranoia every time you go online. The startling thing is that this version of reality will not seem any different to the way things are now because, in many ways, it vibrates with the timbre of inevitability. ■