Case #05 - Running into The Great Firewall: The Story of Online Censorship and Surveillance

When the great techno-utopian dreams of the late 20th and early 21st centuries are reviewed in years to come, the theme of the Internet delivering unrestricted access to information for all might well be remembered as something of an idealistic fantasy (Barlow, 1996). While we may just be experiencing a blip on the way to this tremendous outcome for all, Internet-enabled utopia has yet to materialise for the majority of the world's citizens with most of those online finding their movements scrutinized and logged by governments and businesses in a way that wasn't even possible, or thought about in the late 1990s.

Back then, the major growth in Internet users was happening in the world's developed regions: the U.S. and Europe. China, for example, only had 22 million users in 2000 (Internet World Stats, 2011a), and Internet penetration across the Middle-East was less than 2% (Internet World Stats, 2011b). The surge in Internet access in the U.S. and Europe fuelled a corresponding surge in innovation and Internet start-ups, many of which (Hotmail, AltaVista, Yahoo) focused on facilitating communications and access to information. Governments less inclined to letting citizens drive such things were able to take advantage of slower Internet development in their regions to build a network they were comfortable with, only encouraging people to go online when they were ready. By that time, an architecture of filtering and surveillance was installed in the infrastructure that continues to exist today.

The most famous of these network architectures is often referred to as the Great Firewall of China (Walton, 2001). Started in 1999, this gigantic surveillance edifice tracks communications and blocks Chinese citizens' access to websites, chatrooms, mailing lists or other online resources that could be harmful to morals or incite subversion (August, 2007). It does this through a sophisticated filtering system that builds on over a decade of advances in the area of blacklists and whitelists, keyword filtering and DNS blocking. It also helps that it allegedly employs around 30,000 people to engage in real-time surveillance of chatrooms and messaging services (Waters, 2008).

The scale of China's surveillance apparatus is difficult to replicate, but the technology behind it isn't. Since the beginning of the World Wide Web IT companies, particularly western ones, have been willing to sell equipment and expertise to governments like China's, and filtering/monitoring systems have been installed at national levels in Saudi Arabia and other Gulf States (OWNI/Wikileaks, 2011). Elsewhere, countries like Cuba, North Korea or Myanmar have built their own intranets for selected citizens to access, forbidding connection to the Internet that westerners take for granted. Pakistan even put an ad in the newspaper for help with their surveillance system (Sutton, 2012).

While the resulting censorship and curtailment of online freedom has drawn the well-meaning attention of human rights groups and, more recently, the U.S. Department of State, western governments have over time become more used to the idea of what is going on in the non-democratic countries of the world. While not endorsing Internet censorship per se, there seems to have been an acceptance on the part of western governments that some degree of filtering is acceptable. This acceptance starts with idea that there is undoubtedly some heinous illegal activity taking place online — child pornography for example. Internet blacklists that seek to prevent access to this material exist in Scandinavia, and several pieces of legislation have been passed in the U.S. (Hamilton, 2004; OpenNet Initiative, 2010). The UK has considered

requiring users to 'opt-in' to pornographic material when taking out a contract with an ISP (BBC, 2012).

It is possible to be against child pornography and the blacklisting of websites — such a crude technique has caused numerous cases of blocking access to legitimate websites (EDRI, 2012; Hamilton, 2004). Yet despite protests by Internet freedom groups, it still seems to be popular with policymakers as a solution to the problem. This is important, because the idea that some online activity is so awful that governments have a moral obligation to filter or monitor it is key to the success of other, apparently unrelated legislation such as the raft of anti-terror laws that were rolled out around the world in the wake of the 9/11 terrorist attacks in the U.S.. Any side effects that result from this moral obligation aren't important and mentioning them is unpatriotic — what is important is that something is being done.

In the U.S., for example, the USA PATRIOT Act[1] has normalised state surveillance of the Internet in the name of national security. The 9/11 hijackers supposedly used public library computers in Florida, which led U.S. lawmakers to believe that records of who uses what machines, where and when, needed to be kept (Manjoo, 2001).The national security excuse has always been present in China's explanation for its Internet censorship, but following 9/11 it became possible for western governments to raise the spectre of terrorism to institute wide-ranging surveillance and data retention policies that have a net effect of casting every Internet user as a potential criminal (Hamilton, 2004). Rapid developments in technology make the possibility of monitoring all citizens' electronic communications far more feasible than in the pre-Internet age.

Of course, with new technologies come new ways of avoiding them, and an arms race between the watched and the watchers began in earnest after 2001. The TOR network, anonymising proxy servers and virtual private networks (VPNs) all have become more popular with individuals in recent years. User privacy is becoming a mainstream issue, particularly since it is not just governments that wish to know what users are doing online. The rise of Internet giants such as Amazon, Google, or Facebook is based entirely on understanding the behaviour of their users, and then tailoring advertising directly to them to sell more products. Furthermore, the willingness of people to embrace social media has led to a tremendous increase in the amount of personal information available online, the consequences of which only really began to go mainstream in 2012, when the policies and practices of Internet companies began to be revealed as playing fast and loose with the concept of individual privacy (Mills, 2012).

Importance

This last development is crucial, because it shows that people are finally coming to realise the extent to which their every move is tracked online. If there is a certain inevitability to governments seeking to monitor the activities of their populations in a hopefully good-faith effort to provide only the best-tailored services and security in the Internet age, the idea that we are being pursued ever more intensely by commercial companies who wish to turn our every click into profit seems to rankle more (Honan, 2012).

[1] AKA the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' Act of 2001

Looking at the broader picture and regarding access to new markets on the Internet, it should be clear that we cannot depend on corporates to save us from government surveillance. While it would be nice to think that Google closed its Chinese mainland operations because of a humanitarian or ethical objection to requests from the Chinese government to censor its search results, in reality Google withdrew because, as Sergey Brin has admitted in rather clinical fashion, "On a business level, that decision to censor... was a net negative." (Martinson, 2007).

It's not in the interest of giant Internet companies to give up their users' information to security agencies but nor is it easy for them to avoid being in the position to be asked. Faced with enemies who are increasingly sophisticated in their use of online communications, Governments' desire for backdoor access to the huge banks of personal information held by companies such as Google or Facebook is increasing. In the U.S. a proposed extension of the Communications Assistance to Law Enforcement Act (CALEA) could authorise FBI access to information from 'all services that enable communications' — expanding in one go wiretapping possibilities from telecommunications carriers to email providers, instant messaging services, social media platforms and peer-to-peer technologies like Skype (Savage, 2010). In Europe, the UK government has proposed to resurrect previously abandoned plans for a real-time surveillance network that could access individuals' social media accounts (Katz, 2012). For both of these proposals to get off of the ground countless social media platforms will have to co-operate with governments and provide access to their customers' information to an unprecedented degree. They can most certainly be expected to fight it — it's a risk they would rather not take for fear that it would lead to a huge loss of users, popularity, and ultimately profit.

The rising profile of privacy issues is one of the most important developments in the recent history of the Internet. However, despite the ostensible efforts being put into resolving the issues on the commercial side through things such as do-not-track legislation in the U.S., or the Right to be Forgotten in the EU there is no guarantee that the world's governments are going to stop interfering with information flow online anytime soon (IP-Watch, 2011; Bright, 2012). There is a very real market for surveillance technologies that can help governments, and an appetite among them to explore the possibilities this technology offers (York and Timm, 2012). While the issue of popular revolution is dealt with in more detail in another case study in this paper, it is unquestionable that western governments, for all their public support of the Arab Spring, don't want anything like this happening on their doorstep. Witness the UK government's reaction to rioting in the summer of 2011, when the idea of turning off social media and instant messaging services was briefly mooted (BBC, 2011).

Many in the UK found the government's suggestion laughable, considering the freedom of the Internet in the country, but it is unlikely to be funny to those who used social media in the failed Green Revolution in Iran. The important thing about the development of censorship and surveillance on the Internet is that it *is* possible and it is happening, and that techno-utopianism is powerless in the face of the police turning up at one's door after a throwaway tweet expressing frustration at an airport delay (BBC, 2010). The very reality of governments' ability to restrict entire populations' access to information is key to understanding any future development of the Internet. Those who need to access or communicate information, no matter what it is, will want to do so. If this information is of a sensitive kind, access and dissemination of it may be restricted. Who comes out on top is down to the technologies either side has access to — and this leads to a type of arms race. Behaviour considered unacceptable, whether that is illegal pornography, or the co-ordinates of an anti-government protest, is driven further underground, where better

tools are needed to access/neutralise it. With non-democratic governments unlikely to open up their Internets in the near future, and with democratic ones happy to use the real — and occasionally not so real — threats to national security to ensure that their data retention and surveillance options are kept open, this one will run and run.

Seen from the perspective of most Internet users, it could be said that censorship and intrusion of privacy is only really a problem when it happens to you. In the first ten years of the World Wide Web, it is a fair bet that the vast majority of users on the Internet held little fears that their movements were being scrutinized, or that information was being denied to them. Users had to play with what was in front of them and in the west that meant an unrestricted web, while in Cuba it meant a restricted intranet, if you were lucky.

As time has gone on, however, a combination of factors, all of them underpinned by increasing Internet penetration across the planet, has raised people's awareness of both censorship and surveillance. In fact, many of the issues examined in this paper's case studies — the rise of e-commerce; the increasing use of social media; the risks inherent in illegal file-sharing; and the role of the Internet in popular revolution — have drawn attention to the fact that not everyone's Internet experience is equal. Some people on the planet are more likely to receive poorer quality information than others. Some groups purporting to represent the masses, such as WikiLeaks, Anonymous or LulzSec, have made it a raison d'etre to draw attention to the lack of transparency in society in general, and in doing so they have drawn attention to a lot of the parties involved in trying to stifle information flow, or pressure others to do so.

WikiLeaks may be most famous for its expose of U.S. government cables, but neither it nor groups of hackers like Telecomix have spared the business sector from the hard glare of publicity when it comes to their role in facilitating censorship and surveillance (Greenberg, 2011). Even on the ground in Iran, government opponents found the time to call out Nokia/Siemens for the technology they sold to the Iranian government that let them monitor calls and track activists (Dehghan, 2009). Cisco, Nortel, Blue Coat — all of these companies have been involved at some point in the sale of network technologies to repressive regimes (OWNI/Wikileaks, 2011). The role that surveillance plays in keeping Google or Facebook at the top of the Internet tree has already been pointed out. In terms of the future development of the Internet, the role of the market means that there will always be room for unscrupulous companies, which almost certainly means that the business sector is not going to be the actor that ushers in the age that techno-utopians dream of.

One advantage the business sector has is that governments are either complicit in, or clueless about, the situation. The desire to control populations existed long before the Internet, particularly in non-democratic societies, and Internet technology is merely the latest in a number of methods that have been previously employed. However, the Internet offers governments like China the opportunity to put down central hub points through which all communications traffic passes, at the same time as also offering it a gigantic propaganda opportunity that can fill the gaps in peoples' lives where information is missing. An online orthodoxy can be created and, in terms of future Internet development, it will be difficult to turn back the clock. Developments in Myanmar will be watched with interest.

The establishment of orthodoxy is backed up by the ability to target individuals, whether they are criminal or just subversive. When governments deem the retention of power so important as to reject democracy, the opportunities offered by Internet frameworks set up to control information and root out subversives is too tempting to

ignore. Speeches made by the U.S. State Department in 2011, or by representatives of the European Union, verge on hypocrisy in this regard, for in one breath the need for a free Internet is extolled, while in the next calls are made to combat online copyright infringement through increased traffic monitoring on networks (US Department Of State, 2011). As activists in Scandinavia understand, a system that starts out trying to combat access to one thing — child pornography — can, in only a handful of years, experience mission creep and be commandeered to block other types of information altogether. And not in a transparent manner.

We are now at the point where control mechanisms are embedded in the Internet's architecture. These mechanisms are exploited in government policy, and in business policy too. Users almost certainly expect to be monitored in some way, perhaps by companies in the west, or by the government in non-democratic regimes. This is key, because it means that there will be pushback and attempts, no matter how small, to live the techno-utopian dream. The question of censorship still can be considered in the context of the famous John Gilmour quote: that the Internet "interprets censorship as damage and routes around it" (Elmer-Dewitt, 1993). The control mechanisms can be avoided, but the stakes will continue to rise in the race for the mouse to stay ahead of the cat.