

# **Are We Forfeiting Privacy to Pay For Security?**

An Examination of Online  
Communication Issues

**Craig Dennis**

Design for Interaction

# Contents

Illustrations

Acknowledgements

Introduction

Chapter One - Privacy Law and Security Concerns

Chapter Two – Encryption and Code Breaking

Chapter Three – What Data is Out There?

Chapter Four – Rights and Violations

Conclusion

Appendices

Bibliography

# Illustrations

Privacy Cartoons

<http://www.sangrea.net/free-cartoons/privacy-cartoons.html>, Sangrea

# Acknowledgements

I would like to thank Jeremy Barr for guidance in the preparation of this dissertation and David Edwards for allowing me the time for an interview.

# Introduction

There is an inherent paradox with security and privacy issues surrounding the Internet. They seem to be unable to work in harmony even though their definitions are exclusive of each other. This could be due to pressures from the music and film industries with regard to file sharing but also the paranoia of various government agencies that feel their responsibility for protecting their nation stretches to knowing what everyone does with every piece of information and communication. Is this accurate or is it the nation's own paranoia generated through media both 'factual' and fictional? Could it be newspapers reporting on supposed clandestine operations with a certain poetic license or Saturday night television such as Spooks taking real threats and situations into our living rooms and making everything seem very plausible that is responsible for the feeling that big brother is always watching?

*Sacrificing anonymity may be the next generations price for keeping precious liberty, as prior generations paid in blood'*

*(Brin)*

Historically there has been a problem with security and privacy, none more so than during times of war. The privacy of other nations was being invaded but it was needed to ensure the security of the home nation. Is the problem now an international one and should it be dealt with on an international scale with all countries agreeing to a series of universal terms and conditions rather than each having their own?

The question is whether or not that would resolve the issue as the point of intelligence gathering is to be covert so the people who are the target of such operations do not change their procedures and render the gathered information useless.

There is a link between the current online climate and the climate of code breaking during World War II with regard to the Enigma machine and code breaking. Has anything really changed since then and is it just the technology that has advanced on both sides of the current 'cyber war'?

The aim is to look at the nature of security and privacy issues that have arisen providing context from historical data, looking at how or if they have been resolved and the various legal and social implications of such issues with specific emphasis on the current nature of the Internet and online communications. Who decides what should be monitored and what justification do they need?

The key difference is need versus want. Security is paramount as without it we are vulnerable yet we want privacy which seems to be infringed upon by security. Can there be a way to be protected without compromising the individual's right to privacy?

*'Quis custodiet ipsos custodes? - Who will guard the guards?'*

*(Plato, 350BC)*

# Chapter One

## Privacy Law and Security Concerns

In the current political climate there are many concerns about terrorism from Middle Eastern countries and fundamentalists who believe the only way to be heard is through random acts of violence and destruction. The resulting effect of this is an increased level of security readiness in the West to try and prevent such atrocities from occurring. This has much farther reaching implications for the average citizen who is the subject or target of surveillance operations, specific or generic.

*'Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extend information about them is communicated'*

*(Brin)*

While there may be some justification for a bespoke security operation on an individual, there are general operations designed to find connections that have no justification other than to find someone to conduct further surveillance on. This could be seen as everyone being initially suspected of potential terrorist activities and becoming an enemy of the state and a threat to national security.

*'National security is the entire scope of measures undertaken by the governments of nation-states in providing assurance of national sovereignty to the collective population of the state'*

*(Wikipedia, 2008)*

The data protection act is the main way in which our information is protected and our privacy maintained on a national scale. However in the case of national security there are areas of the data protection act that can be disregarded and so no longer apply.

*'(1) Personal data are exempt from any of the provisions of -*

*(a) the data protection principles,*

*(b) Parts II, III...*

*if the exemption from that provision is required for the purpose of safeguarding national security.'*

Where Part II is:

*'(a) the racial or ethnic origin of the data subject,*

*(b) his political opinions,*

*(c) his religious beliefs or other beliefs of a similar nature,*

*(d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),*

*(e) his physical or mental health or condition,*

*(f) his sexual life,*

*(g) the commission or alleged commission by him of any offence,*

*(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.'*

Where Part III is:

*'(a) the purposes of journalism,*

*(b) artistic purposes, and*

*(c) literary purposes.'*

*(The Data Protection Act 1998)*

This raises the question about the ultimate goal of government, whether they truly are 'for the people' which has been a constant source for conspiracy theories and paranoia.

This can be related to the issue of privacy and whether or not the government has legitimate cause to conduct their surveillance operations. More importantly if they do have cause then who is responsible for setting out what is needed to indentify such cause. If the people in control are setting less and less stringent conditions to put citizens under observation, how can we be sure that the cause is just?

While there are many levels of government and procedures in place to prevent such actions, the governmental agencies are so compartmentalised that it would be unsurprising to find that there are surveillance operations running that have no relevance, no purpose and have been forgotten about by higher authorities.

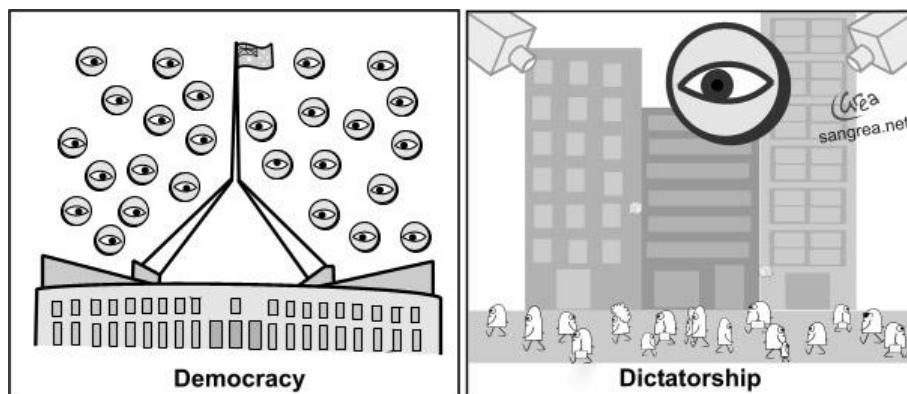


Fig 1 - Democracy and Dictatorship, Sangrea.net

*'The concern is that where the exercise of national security laws and powers is not subject to good governance, the rule of law, and strict checks and balances, there is a risk that national security may simply serve as a pretext for suppressing unfavourable political and social views.'*

(Wikipedia, 2008)

Under the umbrella of 'threat to national security' the government has access to any or all information stored anywhere, by anyone and at any time. To understand the concerns of the online community the concerns of citizens in general need to be considered, looking at security concerns and privacy issues in the broadest sense.

*'Between 150 and 300 million pounds per year is now spent on a surveillance industry involving an estimated 200,000 cameras.'*

*(Privacy International, 2008)*

CCTV penetration parallels the online security deployment in a way that could lead people to accept the changes being made or perhaps not even notice them as it would be something they just accept in the name of protection.

*'The justification for CCTV is seductive, but the evidence is not convincing. In a report to the Scottish Office on the impact of CCTV, Jason Ditton, Director of the Scottish Centre for Criminology, argued that the claims of crime reduction are little more than fantasy. 'All (evaluations and statistics) we have seen so far are wholly unreliable', The British Journal of Criminology described the statistics as "...post hoc shoestring efforts by the untrained and self interested practitioner.'"*

*(Privacy International)*

There are television shows that actively seek to promote the importance of the monitored society by producing shows using nothing more than CCTV footage from shops, city centres, and police vehicles.

This leads to the belief that it is acceptable for so many cameras monitoring our every move, to the point where we do not take any notice of them as they have become common place and seen by many as a good thing.

There is a high probability the same thing could happen to the online community.

There could be an attitude of *'I don't like it but I'll just have to live with it'* thus allowing ever more stringent security and surveillance measures to be placed on a so called public domain. Should the benefit of possibly catching a terrorist out way the definite invasion of privacy that this would entail?

*'Civil liberties are freedoms that protect the individual from the government'*

*(Wikipedia, 2008)*

Corporations would be the first to feel the impending crackdown with online security measures as they have to make sure they trade fairly and abide by all laws to allow them to continue trading.

*'Obviously you have to be compliant with certain laws and what have you because I think people get a bit paranoid about sort of data protection as a whole and there are a lot of companies out there I think making a lot of money out of scare stories and alarming people about you know.'*

*(Edwards, 2008)*

It is interesting that there are organisations set up to battle for our rights on a daily basis against schemes designed and advertised as *'for the greater good'*.

Surprisingly 23% of people surveyed agree with the statement *'We should have all our communications monitored so people who are doing wrong can be caught'* compared to 44% who disagreed.

*'...if you have nothing to hide you shouldn't be worried about things'*

*(Questionnaire Submission 67, 2008)*

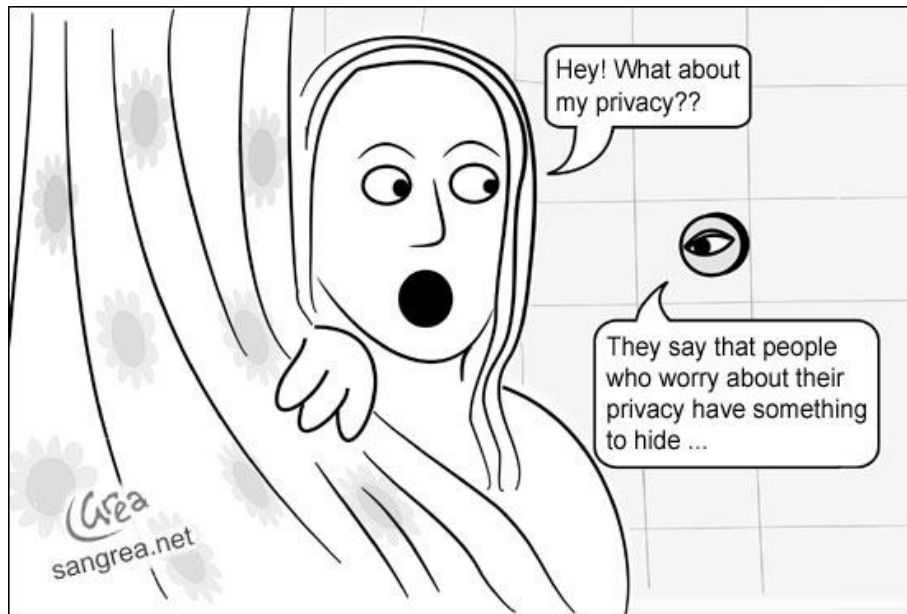


Fig 3 - Privacy Shower Scene, Sangrea.net

It is possible that they all agree with the statement in the strongest sense but it is more likely that it is a graduated agreement. Not fully understanding what would be given up in order to achieve such a goal.

Nothing would ever be secret again, all phone calls would be recorded, all data everywhere would be catalogued and stored and all transactions would also be recorded. Is it right for any individual to have such power over information and would that power corrupt. Recently the membership list for the British National Party was uploaded to the Internet by a disgruntled former member. Consequentially a police officer has been suspended for being on the list. While it is illegal for a member of an enforcement agency to be a member of a political party, should actions be taken as the information was supposed to be private and nobody had any reason to suspect him of membership?

*'In order for cyberspace to be policed, Internet activity will have to be closely monitored. Ed Giorgio, who is working with McConnell on the plan, said that would mean giving the government the authority to examine the content of any e-mail, file transfer or Web search. "Google has records that could help in a cyber-investigation," he said. Giorgio warned me, "We have a saying in this business: 'Privacy and security are a zero-sum game.'"*

*(Schneier, 2008)*

The government has a hard enough time ensuring the security of personal and private data they already hold on us such as tax information, with many reports of lost and found files and USB keys with thousands if not millions of records on. Would we trust this government to keep a quantity of information several orders of magnitude larger? While technically possible to keep track of all information, we need to look at whether it is worth it. If it will cost £10 to catch a criminal but £500 to install a system by which they might catch him for free, is it worth it? Do the ends justify the means?

# Chapter Two

## Encryption and Code Breaking

Historically the issue of security has been high on the agenda of every government with the threat of war, a threat that still exists today.

During World War II the Germans had a strategic advantage over the allies due their code cipher that was thought to be unbreakable. That cipher was called Enigma and the allies enlisted the help of the top minds at the time to try and crack it.

*'In the summer of 1939, a small team of codebreakers arrived at the Government Code and Cipher School's (GC&CS) new home at Bletchley Park, Buckinghamshire. Their mission was to crack the backbone of German military and intelligence communications, the Enigma cipher.'*

*(Government Communication Headquarters, 2008)*

At a time of heightened national security in 1939, the people involved in the decryption of the Enigma cipher worked in huts at Bletchley Park, each hut working on a separate objective but never knowing what their ultimate goal was. No individual directly working on the project was allowed to know anything other than what they had to do, a technique called compartmentalisation.

*'Alan Turing realised that 'cribs' offered a way of cracking Enigma. A 'crib' is a piece of encrypted text whose true meaning is known or can be guessed.'*

*(GCHQ – Government Communication Headquarters)*

While the scale of the operation was impressive at Bletchley Park, 'Some 9,000 people were working at Bletchley Park at the height of the code breaking efforts in January 1945', it was also called 'Station X'. Not because of secrecy and security but simply that it was the 10<sup>th</sup> station to be opened to tackle such problems during the war. Bletchley Park and others like it were sent messages by courier and then by teleprinter which were picked up by listening stations called 'Y-Stations' that would constantly monitor the airwaves for transmissions. Any citizen with a HAM radio at the time could apply to become a 'Voluntary Interceptor' and monitor a specific frequency.

*'Listening stations – the Y-stations (such as the ones at Chicksands in Bedfordshire and Beaumanor Hall in Leicestershire, the War Office "Y" Group HQ) – gathered raw signals for processing at Bletchley'*

*(Government Communication Headquarters)*

Many government operations involve 'need to know' information in order to maintain security but does this mean the problem at the moment is not one of too many people knowing individuals' information but one of too few people will? If there is no context for the information which is held then there is surely a further danger that it could be mistreated with the thinking 'it can't be that important'?

The fact is that people want to know what is going on, not only because it's human nature but also to determine if there is a threat to them. During times of war this sense is heightened and more and more effort is put into monitoring and decrypting opposition communications. Not only that but more effort is put into the encryption of their own communications with the knowledge that the enemy will be actively doing the same.

The Enigma Machine was the answer for the Germans during World War II but the methodology and technology have evolved and the same principles are still being used today. The threat of detection and the fear that people who are not intended to be receiving the information may be reading it has driven the legitimate and the illegitimate development of encryption technologies.

*'Encryption...gives criminals and terrorists a powerful tool for concealing their activities'*

*(Denning and Baugh)*

Understandably then, governments want to have access to all information flowing through the internet. If global access to all internet traffic were available with the justification that September the 11<sup>th</sup> would have been prevented as a result, then a large percentage of people would agree. However even if all traffic was monitored and decrypted, there is no guarantee the atrocity would actually have been prevented but there is a guarantee that people's privacy would have been irreversibly compromised.

*'It would not be feasible to decrypt everything even if it were technically possible'*

*(Denning and Baugh)*

*'Encryption is critical to building a secure and trusted global information infrastructure for communications and electronic commerce'*

*(Denning and Baugh)*

There are many websites available that give details about how to prevent being 'detected' on the internet. From setting up internet access through fake names to having all your internet traffic run through a proxy in another country. In the case of file-sharing the most popular method is a 'seedbox'.

This involves setting up a server with a company that offers 'bullet proof hosting' and access it remotely from anywhere in the world. They use 'military grade encryption', operate in numerous overseas locations and don't keep any of their logs. They are predominantly used for spam email and illegal content distribution.

*'Usually, your web hosting provider will shut down your web site within days...'*

*'We will not shut you down due to complaints'*

*(BP Hosting, 2008)*

While this is an expensive option for most, they are widely used

*'bulletproof hosting, and it's historically been used to insulate online criminal gangs against take-down efforts by law enforcers or private parties'*

*(theregister.com, 2008)*

The problem is that government does not know enough about the way the new online protections systems work, so even if they catch people and sentence them there are a myriad of different ways to overcome them.

*'the only practical effect his ruling had was to force a registrar by the name of Dynadot to suspend the Wikileaks.org domain name. The site remains reachable by accessing its IP address or alternate domain names such as Wikileaks.be and wikileaks.in. That's akin to removing a person's name from the phone book but not disconnecting his phone.'*

*(theregister.com)*

The progression from times of world war, the Y-Stations and Bletchley Park is clear when the principles of today's surveillance are looked at.

Exchange analogue radio signals for digital internet communications and there is the same task and the same problems but now not just focussed on an external enemy but instead focussed internally on the very part that makes a country what it is – its people.

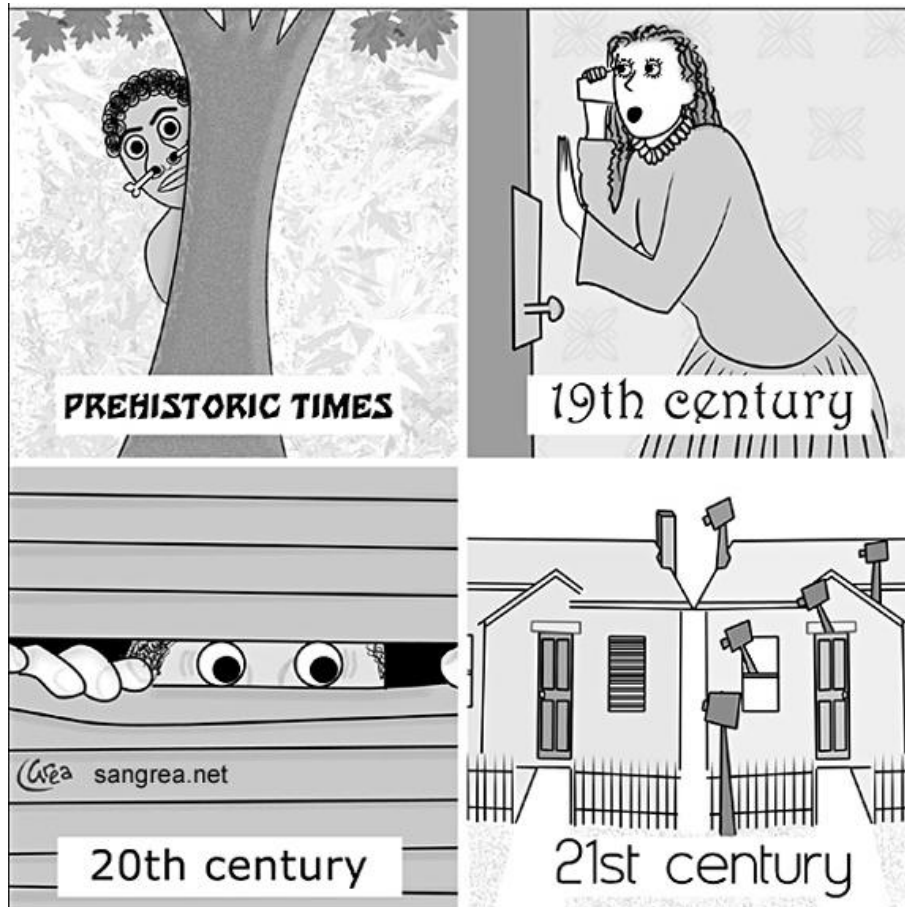


Fig 2 - Busybodies down the Ages, Sangrea.net

# Chapter Three

## What Data is Out There?

The Internet is growing. People are using it more and more for activities that would have seemed impossible not so long ago.

Peer-To-Peer is an Internet distribution network allowing users to share content without using dedicated servers or utilizing bandwidth. The users share information directly with each other using a centralised 'tracker' which directs the relevant information to the correct location.

*'Such networks [contain] audio, video, data or anything in digital format, real-time data such as telephony traffic is also passed using P2P technology.'*

*(Wikipedia)*

Many small businesses use peer-to-peer to keep distribution costs low as constant downloading from web servers results in high server costs for the client and slow download speeds for the customer.

*'10Mbps connection on a 3GHz Xeon server is priced at \$324 per month.'*

*(The Whir)*

VoIP telephone services such as Skype also use peer-to-peer networks to enable phone calls over the Internet for free for this very reason. So why then is there so much controversy over the use of such technologies?

There are clearly many benefits but the government is so adamant about stricter regulations, more stringent monitoring and new legislation which means Internet service providers have to track the content.

In order to understand the process of monitoring, content needs to be clarified. Content in this case could be regarded as something that a person has written in an email or a picture that has been uploaded but actually it is anything sent or received by anyone over the internet.

Content is often classified into different data types which are split into small packets of information which is rebuilt at the destination. More and more commonly though the destination is not an individual's system, rather it is in the 'cloud'. Cloud computing has been known by many names and is not a new phenomenon but only recently has it become so ubiquitous.

*'Although cloud computing is an emerging field of computer science, the idea has been around for a few years. It's called cloud computing because the data and applications exist on a "cloud" of Web servers.'*

*(Strickland)*

The sound of cloud computing seems to lend itself to corporations and large organisations who need instant, global access to data and to run multiple applications on portable devices simultaneously. In fact this is partly true however the most consumer penetration by cloud computing is online email.

People who use Windows Live Mail (previously Hotmail) or Google Mail have had access to the cloud for many years and information is accessible to them wherever there is an internet connection and a web browser. The technology has come a long way since then and there are now versions of Microsoft Office and various other free programs available to use through a web browser, without the application being run on the local machine. One example is Google Docs that acts as a word processor allowing people to write, save, edit and format a document entirely in a web browser, taking the strain off the local machine. Applications like this are occurring more frequently and people are using them with little or no thought about the wider implications of such data being virtual and not physically tied to their machine.

Even mobile internet devices have had their own specific pages made so as to be able to access the same information with a much smaller screen than a standard computer and tailored information to reduce download times, which is becoming less and less of an issue with increasing mobile broadband speeds.

One aspect that people have not realised is that if all of their information is stored on a third party system such as Google Mail, the company could turn around and say “we’re now going to charge for this” or just deny access to it full stop.

*“We offer a number of services that do not require you to register for an account or provide any personal information to us, such as Google Search. In order to provide our full range of services, we may collect...information”*

*(Google, 2008)*

Google search and Windows Live search are very powerful, free internet tools and information about what people have searched for is recorded but if people want to use any other services with either company then they have to register and give some personal information.

Google are trying to be transparent about what information is stored and how they use it, also detailing that they do not allow access to the information stored to any third parties unless they are partnered with Google and even then the information is limited.

*“When you sign up for a Google Account or other Google service or promotion that requires registration, we ask you for personal information (such as your name, email address and an account password). For certain services, such as our advertising programs, we also request credit card or other payment account information which we maintain in encrypted form on secure servers. We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information.”*

*(Google, 2008)*

*“When you access Google services, our servers automatically record information that your browser sends whenever you visit a website. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.”*

*(Google, 2008)*

Importantly Google specifically say that they are using information to identify you but only while you are accessing Google services. Google recently launched their own web browser called Chrome, while initial focus on the application was how it performed there were people looking at what happened to the information.

Similarly to what happens when you access Google's services, all information sent from the browser went through Google's servers first. In other words they would be able to see what you were doing, where you were doing it and at what time, regardless of if users were trying to access a Google page.

The information they have can be accessed at any time by government on a case-by-case basis but this could change if the government has its way.

*"When you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services."*

*(Google, 2008)*

The problem is that if requested by law, neither the company involved (in this case Google) nor the US government have to inform you for three months.

*'the statute [US Code 2705. Delayed notice] allows a delay of up to 90 days if the government just asks for the data and the court finds that "there is reason to believe that notification of the existence of the court order may have an adverse result"'*

*(Rasch)*

There is little chance for appeal due the information already being transmitted and the person who is the subject of the investigation having no knowledge that it even happened.

*'Putting aside the security, data storage, data retention, data destruction and other pesky issues associated with doing business in the cloud, one fundamental issue remains: Your data is being hosted, stored and transmitted through a third party. As far as the law is concerned then, that third party has control of your data and may therefore be subject to a subpoena for your data, often without your knowledge or ability to object.'*

*(Rasch)*

In one particular case the US government simply forgot about the notification altogether.

*“July came and went, as did August, September, October, November, December, January, February, March, April and May of 2007 before the government finally got around to telling Warshak that it had been reading his mail.”*

*(Rasch)*

With more and more people using the internet for communications, the market for advertising is increasing. In order to make the advertising less invasive and more applicable to the user, personalisation techniques are employed to try and make the advertising more relevant which in turn would make advertising more effective.

Currently advertising is personalised by geographic location identified by the IP address from which people access the internet and by keywords that appear on the page. The advantage of using this within the cloud networking system is that the keywords can be linked to individual's information such as within emails and documents stored on Google Mail and Google Docs. Google employs their advertising system by using a subsidiary called AdWords.

*‘create ads and choose keywords, which are words or phrases related to your business. When people search on Google using one of your keywords, your ad may appear next to the search results. Now you are advertising to an audience that is already interested in you.*

*(Google, 2008)*

*‘you can advertise to people searching on Google. Even if you already appear in Google's search results, AdWords can help you target new audiences on Google and our advertising network.’*

*(Google, 2008)*

There is little wonder then that governments are eager to get on side with companies like Google as they would indeed be very useful in a criminal investigation. Not only would they have access to what was sent, when it was sent and to whom but also they would have the IP address from where it was sent too, speeding up the process of catching the suspected criminal.

*'I think it's right we have the facility to do it. The corporate philosophy I think here is that we treat people like adults.'*

*(Edwards, 2008)*

Microsoft employs a similar system to provide personalised content but does not go so far as to provide personalised advertising.

*'We use the information we collect to provide the services you request. Our services may include the display of personalised content and advertising.'*

*(Microsoft, 2008)*

*'When we display online advertisements to you, we will place a persistent cookie on your computer in order to recognise your computer each time we display an ad to you. Because we may serve advertisements on many different Web sites, we are able to compile information over time about where you, or others who are using your computer, saw and/or clicked on the advertisements we display.'*

*(Microsoft, 2008)*

The moral way forward for advertising online should be one of personalisation and privacy.

*'The Google Mail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Google Mail.'*

*(Google, 2008)*

Personalisation gives people relevant information in relation to what they are looking at but privacy gives them the knowledge that what they are looking at is not linked to them or being recorded. If the combination can be found that works and is effective, there is no reason why similar thinking could not be applied to online communication in general. It may be possible but will it ever be allowed to be deployed with such privacy detracting from the amount of control authorities have over peoples' communications?

Phorm have been developing the idea of personalised yet anonymous advertising and have released something called the Open Internet Exchange (OIX) and also Webwise, both targeted at ISPs and advertising agencies.

*'The OIX platform combines anonymised ISP data with patent-pending Phorm ad-serving technology to help advertisers and ad agencies reach their most valuable customer segments with unprecedented precision, whilst giving publishers and networks more potential value from every ad slot.'*

*(Phorm, 2008)*

These services combine to form a framework from which any ISP or advertising agency can work within. Due to the personalisation working at ISP level there is much more of a ubiquitous advertising system that should no longer put off internet users. The results will be relevant to the individual rather than the page they are viewing, while maintaining their privacy.

*'Phorm's unique technology - unlike major search engines - doesn't see, capture or store any personally identifiable user information whatsoever and does not store any browsing history or user search terms.'*

*(Phorm, 2008)*

The basic principle comprises of each user being assigned a randomly generated number, so no tracking of IP address and no entering of personal information. Each web page that the number visits is compared to 'channels' like categories containing sub-categories, the record of the web page is then instantly destroyed and never actually recorded so nobody can access the information because it doesn't exist on any system. This channel then displays ads that match it and relevant ads appear on the page. So when the user leaves the page, no record of it kept.

*'Privacy advisory firm 80/20 Thinking has completed the comprehensive Privacy Impact Assessment (PIA) of Phorm and concludes that the company has embedded consumer privacy into its policies, practices and philosophy'*

*(Phorm, 2008)*

Unfortunately Phorm themselves were maintaining their own privacy at the start of their testing phase by illegally trialling the framework without users' consent with BT. People were subjected to the test and had no knowledge of anything in progress.

If the system operates the way it should then there would be no problem but if the system was flawed in some way (which is why testing is done in the first place) then the amount of personal information collected about individual users would cause an outrage.

*'BT has admitted that it carried out secret trials of the Phorm technology in late 2006.'*

*(Harvey, 2008)*

In response to critics to the system arguing that it is too intrusive BT said,

*'No personally-identifiably user data is stored as part of Webwise. Only the links between a random unidentifiable numbers contained in a cookie and advertising categories are stored in the system.'*

*'This information is deleted after a maximum of six months. It is simply not possible to reverse engineer user identity using this information.'*

*(BT, 2008)*

The question of whether or not the service is too intrusive is a complex one that will undoubtedly go on for some time but the service does offer an 'opt-out' option, meaning people are free to refuse to participate and if the service operates the way it says then no data will be held about an individual – just a number. This method of thinking could be used in real world applications as well as the internet in the broadest sense, allowing the preservation of privacy and the benefit of personalisation and anonymity. The question that needs to be asked though is: Do we want to be just a number?

# Chapter Four

## Rights and Violations

Communication has evolved, as everything does, and as such will keep evolving. How we deal with the changes brought about by that evolution ultimately affect the way we ourselves evolve and how we communicate. The Internet brought about a revolution in communication allowing near instant contact with anybody connected. Even now communication is evolving, with social networks being the driving force in the most recent acceleration, creating a new way for people to interact in a new environment. The advent of MySpace and Facebook meant that not only was there an online space for people to detail their opinions and see who else shares them but a new position of responsibility for the individual to showcase themselves, especially with MySpace which has become the favoured online music platform for up and coming as well as existing musicians. Some people, in particular people in power such as governments or dictators, may view this as too much freedom as the Internet is globally accessible and therefore anyone can read anything anyone has posted.

Specifically if any citizen 'oversteps the mark' their site will be removed and no doubt they will receive at the very least a letter and at most a criminal record. This could very easily lead to censorship of all content on the Internet with the view that it could be a security concern or a threat to a nations security however this clearly impedes on the individual's right to the freedom of speech.

*'From two in 2002, the number of governments filtering the net has risen to two dozen.'*

*(Faris, 2008)*

So what happens when an individual voices an opinion that is detrimental to a third party?

*'South Korean president Lee Myung-Bek is seeking to crack down on the Internet community which has helped intensify and focus criticism of his unpopular government, by introducing a Cyber Defamation Law...Korean journalists have criticised the proposals as a threat to free speech. Six Korean portals and search engines have teamed up to oppose the proposed law.'*

*(Oates, 2008)*

Lee Myung-bek is an example of a government using their power to abuse the privileges of their people to suit their own needs. Lee Myung-bek has introduced a new law to essentially control the content on the Internet in South Korea. Similarly in Burma, political dissidents were sentenced for posting on a blog.

*'An internet blogger and a writer who disguised an attack on Burma's dictator in the form of a love poem were among dozens of activists sentenced to draconian jail terms as the junta ordered a fresh crackdown on dissidents.'*

*(Parry, 2008)*

*'Security is a need that we all have and privacy is seen as a "bonus". What people don't realize is that when they give up privacy then they will ultimately become less secure. The difference is that the "enemy" changes. It may not be terrorists any longer now it is the government or the rogue elements within government.'*

*(Willingham)*

The ultimate goal is the balance between privacy of information and the protection of the people. Thinking about them as opposites may not help matters, it is possible to protect the people without forcing them to surrender their freedom and anonymity.

*'Internet censorship and surveillance are growing global phenomena. ONI's mission is to identify and document Internet filtering and surveillance, and to promote and inform wider public dialogs about such practices.'*

*(Open Net Initiative, 2008)*

Organisations like ONI and Privacy International look in detail at how the general public's access to the Internet is encroached upon by government organisations seeking to know what everyone is doing all the time. Without them there is a very real danger that there would already be a very real 'Internet police' that would indeed have access to everything people have access to online.

*'Workplace electronic surveillance is also an expanding area of business'*

*(Thomas and Loader)*

The media plays out all kinds of worst case scenarios but these tend to relate to public domain information. There are thousands of organisations, companies and other places of work that communicate via the internet, so could they be seen as just a big 'threat'. How do companies like these exist with the possibility of such harsh views?

*'I think of Premier as a culture, certainly my philosophy is to take a fairly relaxed view about it all.'*

*(Edwards, 2008)*

This may sound similar to Google's approach to the Internet which is making all information available to everyone. It is logical that Google would not consider publishing people's credit card numbers and bank account details but they do collect and analyze an incredibly large amount of data. Could this technology not be used to retroactively investigate a person's information, with proper reasoning and a court-order?

Surprisingly Google may end up being this 'police force' as their aim is the freedom of information for everyone however when any company gets to be as large and influential, it's motives and practices need to be carefully monitored to ensure no breaches in antitrust or civil liberties. Influence leads to control, control equals power and Google influence a large amount of data on the internet by their search algorithm alone.

*'Google has records that could help in a cyber-investigation'*

*(Giorgio, 2008)*

*'A lot of the stuff in cyberspace is just a reflection of what happens in real space'*

*(Bartow)*

The government is under pressure from the film and music industries to prevent file-sharing and copyright infringement. The proposed solution for this is a three strike rule by which you will be warned and then cut off by your Internet service provider if it is determined that you are downloading and sharing copyrighted materials.

*'If the law were enacted it would turn Internet service providers, like BT, Tiscali and Virgin, into a pro-active net police force.'*

*(Waters, 2008)*

Is this all just media hype though? It is reasonable to assume that newspapers want to sell more newspapers and TV channels want to attract more viewers. By publishing stories about worst case scenarios when the actual threat is not as great would certainly a way of doing so.

*'popular manifestation through the media...has often focused upon speculation about the detrimental effects of ICTs upon various aspects of law enforcement.'*

*(Thomas and Loader)*

Surely the three strike rule would be breaking current data protection law by sharing Internet traffic data with other Internet service providers? More seriously however they would be recording what every person was doing on the Internet at any given time. This amounts to an online version of a phone tap, which requires reasonable justification and needs to be approved by a Justice Minister.

If we entertain the idea using the same principle as the phone tapping procedure as a base model for comparison, it soon becomes clear that even if the government did in fact enact this three strike plan, it wouldn't work.

Firstly, the government listens to around 2,200 phone conversations each year.

*'Justice Minister Michael McDowell... refused to reveal the number of phone taps he has authorised during his time in office.'*

*(digitalrights.ie)*

Secondly, not all of them were correct and the people having their conversations recorded would not be able to appeal due to the covert nature of a phone tap. In the context of the three strike plan, people would be notified by letter three times before their connection would be cut off.

*'There were 2,243 phone tap warrants issued there last year. This included 66 mistakes, in which security services were listening in to the wrong numbers.'*

*(digitalrights.ie)*

A phone tap, or possibly a web tap (?), must be approved by the justice minister personally and the only way you can apply for a phone tap is if you have reasonable cause to suspect wrong doing on the part of the individual or group accused.

So they must have other evidence to support their need for a phone tap, but in the case of a possible 'web tap' no other evidence will be available as the government is going to be forcing Internet service providers to instigate what amounts to the same as a phone tap but on all its customers all the time.

*'Information should be available to everyone (concerning things like politics) but dangerous information such as "how to.." or information that could be dangerous in the wrong hands should be monitored by (i.e. in Europe) the EU but not by the specific country's government.'*

*(Submission 37. Questionnaire, 2008)*

If the UK government's three strike plan is put into effect, the part of the Internet service providers to ban users who download illegal content will be soured with many wrongful accusations and subsequent applications for compensation.

*'ISPA is worried about the cost to its members if users targeted by rights holders for copyright infringement turn out to be innocent.'*

*(Internet Service Providers Association, 2008)*

So the Internet service providers would need permission for each individual they targeted and even then they would require reasonable cause for such an action to be undertaken along with subsidisation from the in case they accidentally target the wrong users. So why are the government still pushing it if even the ISPA say it can't be done with any degree of success?

*'We still need to establish the proof points'*

*(Internet Service Providers Association, 2008)*

This is in stark contrast to Comcast, a large US cable service provider who has been in legal battles recently after being sued for deliberately sacrificing peer-to-peer bandwidth under the pretext of 'traffic shaping' to reduce the strain of the network at peak times.

A Comcast customer filed the lawsuit after being fed up with slow speeds while using peer-to-peer software.

*'...a lawsuit against the nation's biggest cable operator, alleging the company "intentionally and severely" impedes the use of peer-to-peer file-sharing applications.'*

*(multichannel.com, 2008)*

A few months later, a few more Comcast customers had a similar qualm and responded in the same way by filing a similar lawsuit which prompted a review of the company's policies and practices on management of their network traffic for specific protocols.

*'...claims that service frequently stops or slows to a crawl when using file-sharing applications'*

*(multichannel.com, 2008)*

Whereas the lawsuit was expected to get thrown out, surprisingly eight months later an independent researcher discovered that Comcast had been throttling certain peer-to-peer protocols.

*'Comcast was secretly throttling BitTorrent and other P2P traffic'*

*(theregister.com, 2008)*

Peer-to-peer data distribution does not mean copyright infringement and so people need to stop fighting the technology and rather the misuse of the technology. They need to rethink their own distribution arrangement and start working with peer-to-peer which is an excellent way to distribute data while maintaining low costs to the provider.

A successful adaption of such technology is Napster and the transformation of its music service from illegal to legal. For a low monthly charge you can download and play as much music as you like, transfer it to an mp3 player for a small amount extra each month or burn to CD with a one-off payment.

The idea of filtering the internet is not a new one. Censorship has been around since the start of recorded history and probably before that but that is what filtering equates to. There are degrees of net filtering such as to control bandwidth and to control access which have somewhat understandable actions but filtering to control content is censorship and is pervasive in many eastern parts of the world. No surprise that the areas with political content filtering are the same areas that have unstable governments or dictatorships. This is something that should not be encouraged or even considered in supposedly stable countries and yet, if governments had their way this is how things would be. *(See Appendix A)*

# Conclusion

In researching the topic of this dissertation it became apparent that many people are interested in it and subsequently feedback from the questionnaire was more helpful than expected. The questionnaire was designed to get as much quantitative information as possible while still having the opportunity to give personal opinion without feeling like they had to write an essay. By limiting it to 10 questions the questionnaire appeared short and quick while only having one question with a text box made it easier for people to write something relevant without needing to put in a lot of effort.

The research sources are predominantly internet based, from blogs of people who have a view on the topic to newspapers' online presence and government websites. The point being to show how much information is on the internet and how much it has become an integral part of many people's lives. While globally only 22% of people have the internet in their homes and that statistic is only going to grow, just like the percentage that own cars and a telephone. The important thing here is that global communications are evolving thanks to the internet and there are governments that are threatened by the thought of cheap or even free communication with different cultures with the inevitability of learning about information not normally readily available to citizens.

There are a lot of political aspects to consider when understanding why things are the way they are. Often they are clouded in smoke and mirrors with the very nature of politics making clear and valid arguments difficult to get to.

This is the major problem with privacy and security not just in the online community but universally because politicians are ultimately in control and their goal seems to be the continuation of that control. Saying what people want to hear and doing them are two completely different issues within politics.

The interviews were of great insight, providing a look at how a corporate entity deals with the constantly shifting battleground that is global online communication. With so many countries online it is inevitable that there will be a focal point at which the world realises a standardised method of controlling the internet is needed. Not censorship or monitoring but more what justification is needed to obtain information, what can be recorded by Internet service providers and when. The emphasis needs to be on the behind-the-scenes of the internet rather than directly affecting users and their rights.

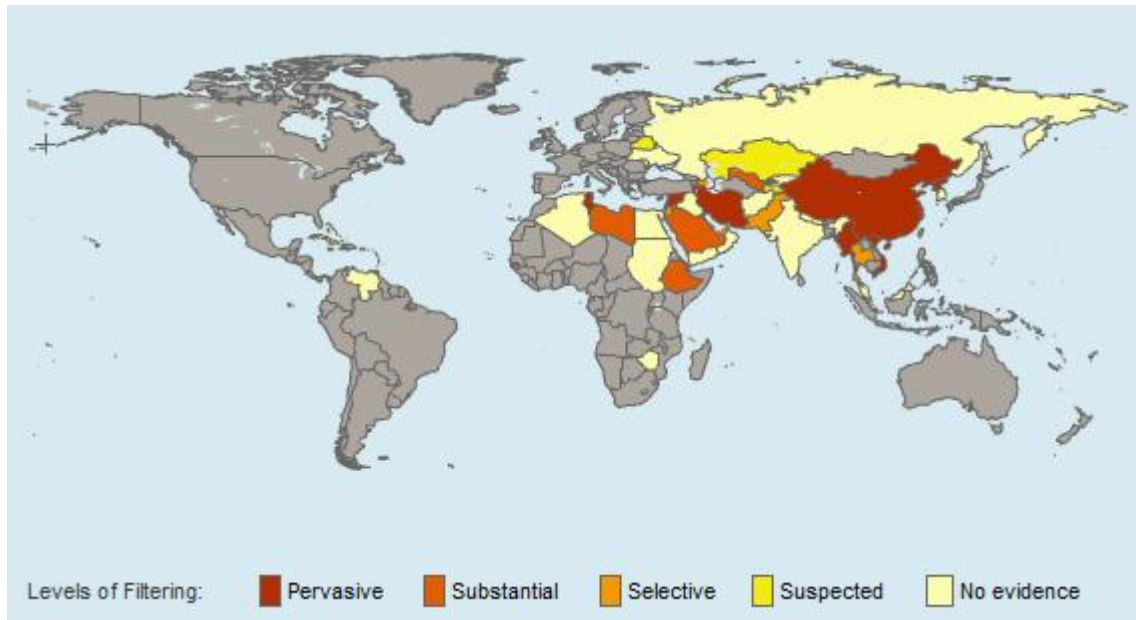
The title still does not accurately represent the focus of this dissertation as it is a global topic with millions of different opinions and seemingly just as many laws to go with them. The title underwent much iteration before an adequate one was found that was broad enough to outline the overall direction as well as some focus to maintain it within 9000 words. The topic is the cause of much debate and argument so is something that cannot be resolved over night. While not needing to be settled over night, there is sufficient cause for concern that the issues discussed are only going to increase over time. The main concern is that governments will step in without full knowledge of the systems and incorrect assumptions about their actions, only succeeding in exacerbating the situation and leading to the internet consuming itself. In response to the question set in the title, the way legislation is progressing there is a real danger of privacy being neglected with the hollow justification of protecting the nation from cyber crime.

# Appendices

## (Appendix A)

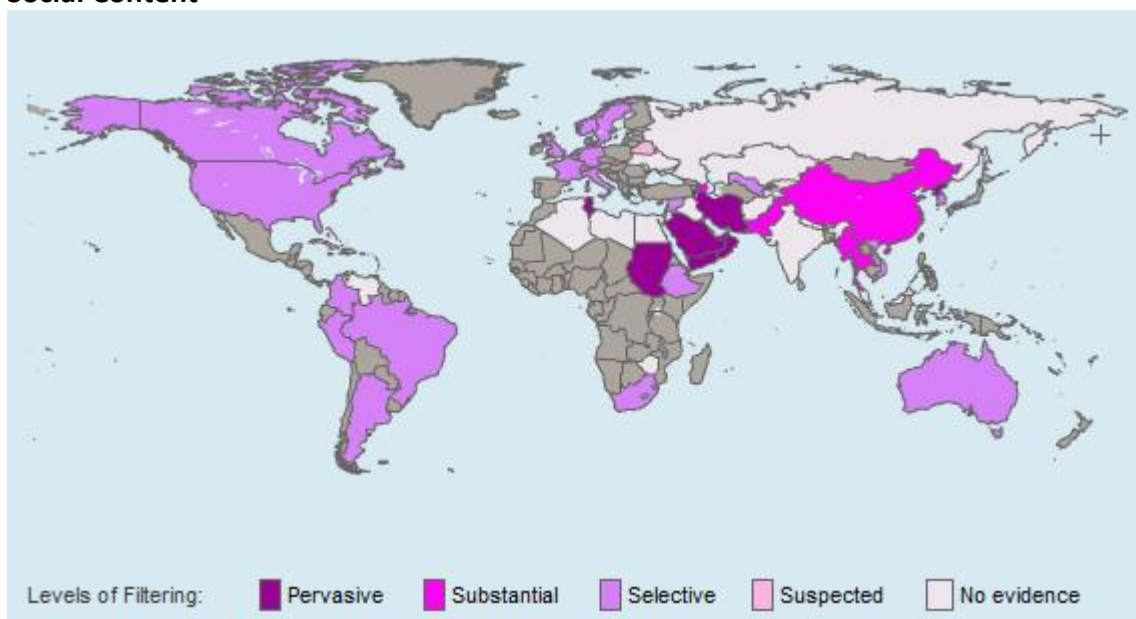
### Global Content Filtering by Type

#### Political Content



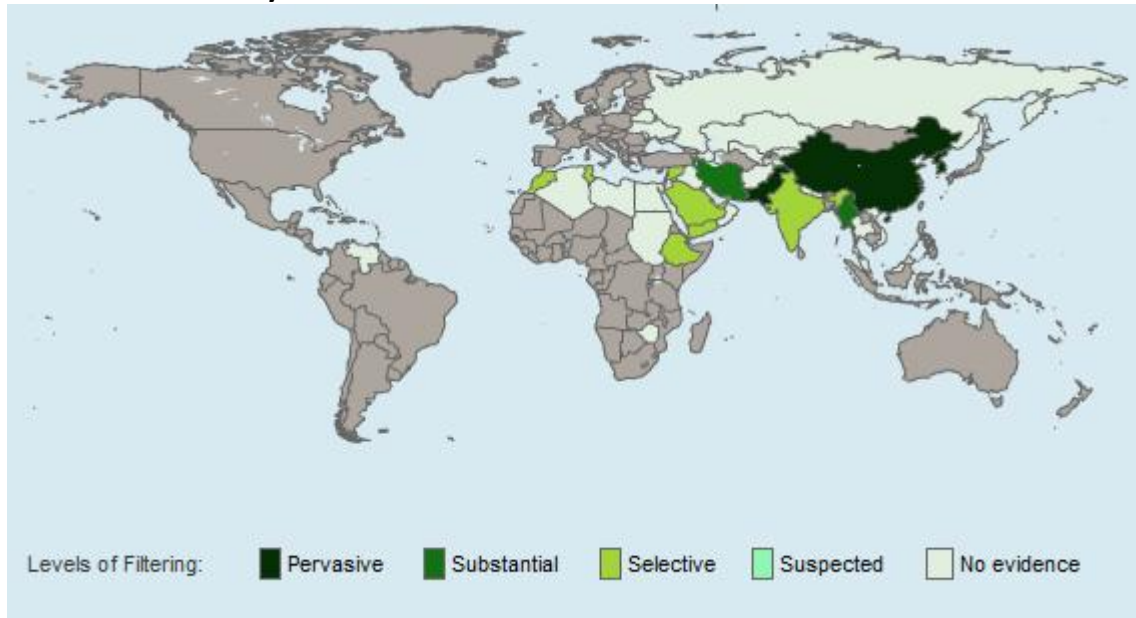
Content that expresses views in opposition to those of the current government, or is related to human rights, freedom of expression, minority rights, and religious movements.

#### Social Content



Content related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive.

## Conflict and Security



Content related to armed conflicts, border disputes, separatist movements, and militant groups.

'No data' sections display in grey. 'No data' does not necessarily indicate absence of filtering practices.

## (Appendix B)

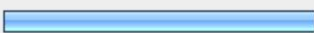

### Questionnaire Results

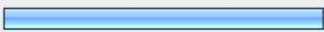

1. How often do you use the internet?			Response Percent	Response Count
Once a week			1.8%	3
Once a day			20.2%	34
More than once a day			78.0%	131
			<i>answered question</i>	<b>168</b>
			<i>skipped question</i>	<b>0</b>

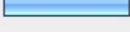
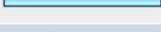
2. Do you use online email? Google Mail? Hotmail?			Response Percent	Response Count
Yes			91.1%	153
No			8.9%	15
			<i>answered question</i>	<b>168</b>
			<i>skipped question</i>	<b>0</b>

3. Do you worry that people may be able to read your emails?			Response Percent	Response Count
Yes			34.7%	58
No			65.3%	109
			<i>answered question</i>	<b>167</b>
			<i>skipped question</i>	<b>1</b>

4. Do you buy things online? Ebay? Amazon?			Response Percent	Response Count
Yes			91.1%	153
No			8.9%	15
			<i>answered question</i>	<b>168</b>
			<i>skipped question</i>	<b>0</b>

5. Do you fileshare? Torrents? Limewire? eMule?			Response Percent	Response Count
Yes			55.4%	93
No			44.6%	75
<i>answered question</i>				<b>168</b>
<i>skipped question</i>				<b>0</b>

6. Are you concerned that ISPs may know what you're downloading and what sites you're visiting?			Response Percent	Response Count
Yes			56.9%	95
No			43.1%	72
<i>answered question</i>				<b>167</b>
<i>skipped question</i>				<b>1</b>

7. How much do you agree with the following. "We should have all our communications monitored so people who are doing wrong can be caught"			Response Percent	Response Count
Strongly Agree			3.6%	6
Agree			22.0%	37
Disagree			46.4%	78
Strongly Disagree			28.0%	47
<i>answered question</i>				<b>168</b>
<i>skipped question</i>				<b>0</b>

8. Who should decide what information gets monitored? Could you?		Response Count
		123
<i>answered question</i>		<b>123</b>
<i>skipped question</i>		<b>45</b>

Responses to question eight are in Appendix C.

9. What security measures do you take when accessing the internet?			
		Response Percent	Response Count
Router with firewall		70.1%	117
<b>Username / Password</b>		<b>76.0%</b>	127
WPA		19.8%	33
WEP		18.6%	31
Mac Address Filtering		15.6%	26
None		1.8%	3
I don't know		13.8%	23
<b>answered question</b>			<b>167</b>
<b>skipped question</b>			<b>1</b>

10. If you use Facebook, what personal information is listed?			
		Response Percent	Response Count
None		12.7%	20
<b>Name</b>		<b>83.5%</b>	132
Address		4.4%	7
Phone number		12.7%	20
Email Address		58.2%	92
Date of birth		57.0%	90
<b>answered question</b>			<b>158</b>
<b>skipped question</b>			<b>10</b>

## **(Appendix C)**

**“Who should decide what information gets monitored? Could you?”**

**1.** Company Directors

**2.** this is a good question but i dont know and this is not a responsibility for 1

**3.** no

**4.** It is beyond the control of the proies

**5.** some sort of security system, but i also think that parents should have a vastly impact on kids up to 18's use of Internet. so parents

**6.** the police

**7.** The public should have some say. Some people should be monitored like convicted paedos, or those types of websites, ones declaring hatred and stuff should be monitored but the rest of us, not so much.

**8.** Yourself

**9.** On one hand some form of authority should monitor the usage, to prevent fraud or other illegal happenings, but then again saying that would mean the majority of the student population would be jailed for illegal downloads.....

**10.** Myself

**11.** Bob Sinclar and/or Judge Judy

**12.** search engines such as google should be monitored to check up on what people are looking up.

**13.** no

**14.** The government should enlist advisors to put forward a series of proposals which are then collected and worked thought to find a suitable level of monitoring. I couldn't

**15.** the police on a person to person basis

**16.** It should all be archived but only viewable via court order.

**17.** VERY GOOD QUESTION, I HAVE NO ANSWER

**18.** no

**19.** People - through a poll

**20.** parents

**21.** copyrighters? no

**22.** good point

**23.** It is not what should be collected, but from whom? I dont think data should be recorded about anyone in general without the authorisation of an independent institution. e.g. court or some sort of committee. - this box is rubbish to write loads of stuff in. maybe you could have a box at the end the next time, asking for more ideas on the subject, or just make a bigger textbox. by the way WPA2 is missing. question 9 could have 'other' textbox too - and sometimes you cannot decide which security to choose. e.g. public hotspot.

**24.** People who can also respect my personal data.

**25.** Mr Blobby

**26.** Perhaps the government, not myself - maybe a public survey to decide what the general public think should be monitored?

**27.** No - one should its a violation of privacy

**28.** yes

**29.** no one should, its supposed to be a free country

**30.** the way it is at present is ok, google, facebook, and government starting to pry to much i feel. i would not want to do it as i believe in freedom of information

**31.** police

**32.** no one, I don't believe in that

**33.** i should

**34.** Us

**35.** no one

**36.** dont know

**37.** i couldn't - I guess things like that need to be top down, not bottom up decisions.

**38.** nobody

**39.** I should decide and quite frankly nothing should be monitored on the Internet within reason.

**40.** No one we are not kids

**41.** Anyone who wants to, website, parents who want to monitor the usage of the Internet by their kids

**42.** No

**43.** I think the question should be "how do we decide who is monitored?" before we worry about what we're monitoring

**44.** A collaboration between government and civilians. Mainly informations that in some way are against human rights i.e. child pornographic content.

**45.** No

**46.** I believe I should be able to decide what info about me is kept, unless I have done wrong, then your rights to choose diminish

**47.** nobody should be monitored; you cannot control the state, look in the past at east germany!

**48.** i dont think anymore has the right but certain things should be policed

**49.** I think there should be a more specialised section in the government who should. People that we trust. But after all that has happened recently, i'm not sure how that would

**50.** no

**51.** no one

**52.** Don't know.

**53.** yes

**54.** no not me

**55.** There needs to be some new laws passed that are fair, and that everyone has a say in.

**56.** The police and consumer associations

**57.** Judges on a case by case basis

**58.** no one

**59.** the authorities with people they suspect may be doing wrong.. dont just monitor everyone

**60.** i guess the government, but i'm really not sure.. the police maybe?

**61.** no

**62.** There should be a central system so it is all secured by the government/defence services, not the service provider.

**63.** magistrates

**64.** yes, you could set it up in like your personal settings

**65.** I don't think information should be monitored

**66.** no one

**67.** Not sure.

**68.** Information should be available to everyone (concerning things like politics) but dangerous information such as 'how to..' or information that could be dangerous in the

wrong hands should be monitored by (ie in Europe) the EU but not by the specific country's government

**69.** yep

**70.** -

**71.** Police

**72.** Government

**73.** Don't know

**74.** parents of pc's or owners of computers

**75.** The Government? Police? Depends what they are monitoring, eg criminal activity

**76.** We should decide, and yes, yes I could.

**77.** i couldn't. if there was fund available, i think hacker groups would be interested. would be a win win

**78.** independent organisation that follows the laws of the nation of the user is situated

**79.** no

**80.** No-one and/or the individual in a free society that believes in the freedom of speech.

**81.** I don't know, if I chose what was monitored there would still be lots of problems.

**82.** ...Not sure. Too much of a job for one person to do so I guess a committee of some kind.

Most people probably say Government but surely it would have to be some independent organisation.

**83.** If info gets monitored, then it should be set in stone rather than ISP's catching people out...therefore laws should be put in place to make it legal for all ISP's to monitor anyone.

**84.** Internet providers should be responsible for what they host

**85.** no one

**86.** Yes, I could

**87.** Government through legislation

**88.** no one

**89.** Democratic vote

**90.** aol

**91.** not sure

**92.** Maybe Yes, but that really depends.

**93.** no-one can, as soon as someone has control everyone else will lose their freedom.

**94.** A designated governing body?

**95.** Nobody

**96.** Parliament (not government)

**97.** I guess people in charge, ie the government, police chiefs. I think they must do it anyway, so if you have nothing to hide you shouldn't be worried about things. It may not be right, but we can't stop it. I think I could decide what information gets monitored.

More of an issue I think is people finding information who shouldn't have it, and are not helping protect people; fraud for example.

**98.** No

**99.** Don't Know

**100.** I have o idea who should do it. Anyway, whoever does it will have some sort of connection with the government and i think there is no runaway from it. And, no I couldn't do it.

**101.** Monitored Information should be things that is illegal or potentially threatening... child porn, terrorism, etc.

**102.** No

**103.** not sure

**104.** I couldn't, I don't have the knowledge to know what i'm looking for. It should be trained staff

**105.** Can't decide

**106.** for protection purposes its good to have certain sites monitored, but not everything should be watched

**107.** I think its fair enough the way it is at the moment, but i dont agree our every movement should be watched, but children should be protected.

**108.** Criminal Justice System????

**109.** no one

**110.** I have no idea, monitoring too much information seems to breach a person's privacy.

**111.** no one

**112.** General Public

**113.** me

**114.** Who decides what constitutes 'wrong' behaviour?

**115.** Case by case scenario.

**116.** UN

**117.** No?

**118.** Nobody has the right to invade privacy, invade the lives of thousands so prosecute few is too large a sacrifice.

**119.** Home Office, following a public consultation. I couldn't

**120.** Those in the public security profession - not politicians or middle managers

**121.** terrorist threats

**122.** It shouldn't be monitored unless you are a convicted criminal

**123.** Dunno

## **(Appendix D)**

### **Interview Transcript**

David Edwards  
Group Information Services Manager  
Premier Oil plc.

All questions asked are highlighted in bold.

#### **Tell me a little about yourself.**

My real skill is not in the technical arena, I've got people I trust to do that. I see my job as being a bridge between the business and IT so the IT guys know what can be done and what's achievable but I've got a better idea of what's needed.

#### **How does Premier Oil operate with regard to IT?**

I think of Premier as a culture, certainly my philosophy is to take a fairly relaxed view about it all. Obviously you have to be compliant with certain laws and what have you because I think people get a bit paranoid about sort of data protection as a whole and there are a lot of companies out there I think making a lot of money out of scare stories and alarming people about you know.

Sarbanes Oxley is an American act that was passed after the collapse of N-RON Sarbanes and Oxley are the two senators who saw it through the House of Representatives and it's a real pain in the arse. We don't operate in the states so we don't have to comply with and long may that continue because it's a real heavy bureaucratic overhead to actually keep track of all information, who did what and audit trails everywhere.

John Brown said before he retired for BP said that that act increased BP's cost of doing business in the states by \$60 million a year. In terms of our philosophy we actually reserve the right to monitor information.

**Do people have to sign a document?**

No, by signing their contract of employment they tacit their agreement to the HR policy and part of that includes extracts from IT policies which state that "we reserve the right to monitor your emails and all data on Premier's network is Premier's data'. In practice we don't bother, it's too much hassle unless there's a specific reason to do it IE.

**What kind of reason?**

Without getting into specifics, one of the directors has asked us to do an email count which happened a few months ago. There was a complaint from one employee against another, a consultant, so we asked to look back at the emails to find out what was sent and said.

**So is it retrospective?**

Yes, we don't actively monitor.

**If there is a threat from an external source, how are you notified about it?**

It would go to an individual mailbox, but if someone was on holiday...

**So it has to be raise by an individual? There are no automated systems?**

Well we run Exchange here, I don't know if you've heard of the Journaling feature.

Journaling basically takes a copy of every email that comes in and out, whatever it is, and just shoves it in a database which is then backed up. We keep that switched off.

Now some companies if they want to do some real cast iron email monitoring and management will switch journaling on and using an application (there are many applications on the market) one of which is Storage Vault which takes the journaling copy shoves it into that server and the database on there is constructed as such that actually only the vendors of the software have access to it. So that in a court of law you can prove that "this is what was sent or received, we have no way of accessing that, here's a third-party company to certify that there was no way we could have tampered with that". Now we haven't got that level of legal ability so we're taking risks there but I've mulled it over with our lawyers and we came to the conclusion that, actually, for the effort of administering all that and the cost of putting the system in place we're prepared to take the risk. So in other words if we had a commercial dispute with another company and they tampered with an email exchange and said "no well you said 50 million not 40 million. Look here's the email." We couldn't actually prove that that it was otherwise. So we would claim "no well you've tampered with the email and they'd say "no you have'.

The thinking there is that large sums of money like that, you wouldn't be doing that by email anyway. There would be written contracts and things like that. So there is a slight risk there, we're prepared to take it.

**If you wanted to trace an email from an external source, how would you go about doing it?**

We would initiate it but then pass it on to Daemon, our ISP and they would then follow the trail. In actual fact I think you'd probably go to the Police now and the Police would then instruct Daemon to do it. I think threats are generally still being done by telephone.

**Could you handle something like that if it wasn't by telephone?**

It would be difficult to set something up to manage that content, there are so many variables that you would have to save. Are you just going to look out for the word "bomb"?

About 18 months ago we looked and found about 150,000 emails hitting our firewall each week. Now actually 70 percent of that is spam. We reckon that about 30,000 are actually valid. But if you wanted to setup some kind of monitoring for a person to look at each email for every time the word "bomb" occurs out of 150,000 I bet you there would be about 1000 a week that would have related.

The only thing would be if someone was sending someone porn that is something we'd want to block.

**Do you think it's right that the ISP monitors internet traffic?**

I think it's right we have the facility to do it. The corporate philosophy I think here is that we treat people like adults.

So say what is acceptable and what's not accepted use, limited personal use is acceptable but don't start downloading anything sexist, racist or violent or pornographic. But we don't actually put any blocks on that kind of thing we just say that you'll be in trouble if you're caught.

And we reserve the right to monitor the systems if we fancy it, 'cos it's our information. We haven't done spot checks, not just for the sake of it but occasionally when we do email checks, things crop up from time to time. I think it's a small enough user community, I mean you wouldn't get away with this if you had 5000 employees. We're all in an open plan office and that kind of polices itself in my view.

**Do you have access to any data whenever you like?**

Yes, without telling them you mean? I am told by my lawyers that by saying upfront "all data belongs to Premier" then we have a right to have a look at it and that cover us on that front. The exception to that is our office in Norway. If you leave then we won't forward you email externally but we will forward it to a nominated Premier employee here. But because we allow the email for personal use, in Norway that policy is not acceptable, we can't just nominate someone else to forward the email so we have to write a separate leaving policy.

**Are there any other countries with similar restrictions?**

Well we've had to set different email disclaimers but that's sort of more copyright issues. I think that Britain after Norway is one of the most liberal countries that we [Premier] operate in. So if something passes here then it tends to be fine in Pakistan and Vietnam.

**Do you agree with the statement "Who should decide what information gets monitored?"?**

Well I think there needs to be due course for investigating someone.

**What kinds of things do you monitor then?**

We recently purchased some asset management software called "Sentential Discovery" that plugs into every device on our network and brings back a list of all applications running. This is just to cover us in terms of software compliance to ensure that everything on our network, we have a licence for.

An example is that a lot of people run Google Earth here and Google Earth is freeware for domestic users and it does clearly state on the freeware licence that it is not for commercial users. We are an exploration and production company and it wouldn't wash in a court of law that everybody was using it for personal use because we've got geologists, geophysicists who use maps as their main tools. So we will have to buy some professional licences which are about \$400 a pop.

**Can anyone install anything on your systems?**

No, executable files get blocked at the firewall. We do have admin access should anything need to be installed.

**The government wants ISPs to monitor anything and everything. Do you have any thoughts on this?**

It's the cost to the country to do that, the amount of information that's passed around networks each day.

It's like the pan-national NHS project, if you talk to technical people they just say "it's too big a project, it was too ambitious and it's just never going to work" and I think this again... if you had enough money then you could probably do it but you'd have to slash the defence budget.

They already have the right to access anyone's email account and force ISPs to give up information on an Ad Hoc basis, a case by case basis so why not just enforce that law properly. The law enforcement agencies have those tools at their disposal so what is this nonsense?

I think it's insane the way the current government has this uncontrollable urge to actually control everything, every aspect of the individual's life. I see it as a balance between civil rights and security and there is a balance needs to be struck.

## **(Appendix E)**

### Progress Map

#### April 2008

- Discuss interests and formulate possible dissertation questions.

#### May 2008

- Finalise dissertation question based on feedback from tutor.
- Write synopsis for dissertation.
- Begin research.

#### June 2008

- Search for first-hand research sources.
- Search for case-studies relating to question or conduct own.

#### July

- Discussion of possible interview candidates
- Continue research into relating issues.
- Draft chapter titles.

#### August

- Try to arrange interviews.
- Increase the depth of chapter outlines.
- Research sources leaning heavily on online influence, possible need to balance for credibility.

## September

- Collating research and picking out passages or quotes that might be useful.
- Post questionnaire details.
- Del.icio.us account has many articles broken into sections.
  - Privacy
  - Piracy
  - Legislation
  - File Sharing
  - Copyright
  - Anonymity
  - General

## October

- Draft chapters take shape.
- Draft of introduction, chapter two and most of chapter four completed.
- Historical context moved and combined with encryption.
- Bulk added to chapters.
- Questionnaire results reach 150

## November

- Based on feedback, complete each chapter and arrange for proof reading.
- Complete final interview.
- Correct any mistakes and ensure the dissertation is balanced and not biased.

# Bibliography

## Books

BRIN, David. **The Transparent Society**, Perseus Books. 1999

Oxford Internet Surveys (OXIS). **The Internet in Britain**, 2007

SIYASINGHE, Udara Rusiri. **Anonymous Communication on the Internet**

THOMAS, Douglas and LOADER, Brian D. **Cybercrime**, Routledge. 2002

## Interviews

EDWARDS, David. Premier Oil Headquarters, London. 21 Nov 08  
(Mr Edwards is Group Information Services Manager for Premier Oil plc.)

FRANKLIN, Kevin and MACFARLANE, Garth. Premier Oil Headquarters, London. 21 Nov 08  
(Dr Kevin Franklin & Garth MacFarlane work for Maple Craft who deal with Corporate and Social Responsibility)

## Websites

'Burma activists sentenced to 65 years each'  
<http://www.timesonline.co.uk/tol/news/world/asia/article5129509.ece>, 01 Dec 08

'Microsoft's Online Privacy Statement' - Microsoft  
<http://privacy.microsoft.com/en-gb/fullnotice.mspx#EYB>, 28 Nov 08

'Safe Harbour' – Export.gov  
<http://www.export.gov/safeharbor/>, 26 Nov 08

'Privacy Policy' – Google  
<http://www.google.com/privacypolicy.html>, 26 Nov 08

'Privacy Notice' – Google Mail  
<http://mail.google.com/mail/help/intl/en-GB/privacy.html>, 26 Nov 08

**'The Internet Services Providers' Association'**

<http://www.ispa.org.uk/>, 25 Nov 08

**'Sorting 1PB with MapReduce'**, Official Google Blog

<http://googleblog.blogspot.com/2008/11/sorting-1pb-with-mapreduce.html>, 25 Nov 08

**'Privacy vs Security'** – SCHNEIER, Bruce

[http://www.schneier.com/blog/archives/2008/01/security\\_vs\\_pri.html](http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html), 24 Nov 08

**'Internet Censorship and Mission Creep'** – GROSSMAN, Wendy M

[http://www.theregister.co.uk/2008/05/27/Internet\\_censorship/](http://www.theregister.co.uk/2008/05/27/Internet_censorship/), 30 May 08

**'Average Bandwidth Price'** - Web Hosting Talk

<http://www.webhostingtalk.com/showthread.php?t=673780>

**'Peer-to-peer'** - Wikipedia

[http://en.wikipedia.org/wiki/Peer\\_2\\_peer](http://en.wikipedia.org/wiki/Peer_2_peer)

**'RackForce Drops Bandwidth Prices'** - WHIR News

[http://www.thewhir.com/marketwatch/053006\\_RackForce\\_Drops\\_Bandwidth\\_Prices.cfm](http://www.thewhir.com/marketwatch/053006_RackForce_Drops_Bandwidth_Prices.cfm)

**'UK Considers Internet Ban On Illegal Downloaders'** – Trusted Reviews

<http://www.trustedreviews.com/networking/news/2008/02/13/UK-Considers-Internet-Ban-On-Illegal-Downloaders/p1>

**'The Privacy and Electronic Communications (EC Directive) Regulations 2003'** - Office of Public Sector Information

<http://www.opsi.gov.uk/si/si2003/20032426.htm>

**'Rectification, blocking, erasure and destruction'** – Office of Public Sector Information

[http://www.uk-legislation.hmso.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_3#pt2-l1g14](http://www.uk-legislation.hmso.gov.uk/acts/acts1998/ukpga_19980029_en_3#pt2-l1g14)

**'Fine Gael Concerns about Phone Tapping'** - Digital Rights Ireland

<http://www.digitalrights.ie/2007/03/23/fine-gael-concerns-about-phone-tapping/>

**'Illegal downloaders 'face UK ban''** – BBC News  
<http://news.bbc.co.uk/1/hi/business/7240234.stm>

**'Spain bans file-sharing'** – READE, Quentin  
<http://www.webuser.co.uk/news/87703.html>

**'Comcast Sued Over Peer-to-Peer Delays'** – SPANGLER, Todd  
<http://www.multichannel.com/article/CA6501572.html?industryid=47201&q=Comcast+AND+class+action>

**'Comcast cops to BitTorrent busting'** – METZ, Cade  
[http://www.theregister.co.uk/2008/02/13/comcast\\_fcc\\_network\\_management\\_filing/](http://www.theregister.co.uk/2008/02/13/comcast_fcc_network_management_filing/)

**'Microsoft swoops into schools to teach P2P morality'** – The Register  
[http://www.theregister.co.uk/2008/02/14/microsoft\\_ip\\_education/](http://www.theregister.co.uk/2008/02/14/microsoft_ip_education/)

**'ISPs demand record biz pays up if cut-off P2P users sue'** - WILLIAMS, Chris. The Register  
[http://www.theregister.co.uk/2008/02/12/anti\\_filesharing\\_paper\\_leak/](http://www.theregister.co.uk/2008/02/12/anti_filesharing_paper_leak/)

**'Everyone's a winner'** – The Guardian  
<http://media.guardian.co.uk/tvtoday/story/0,,2261631,00.html>

**'Creativity policy pits internet providers against pirates'** – The Guardian  
<http://www.guardian.co.uk/technology/2008/feb/23/piracy.Internet>

**'Turkey's Capricious Filtering - Just Too Easy'** – Open Net Initiative  
<http://opennet.net/blog/2008/11/turkeys-capricious-filtering-just-too-easy/>, 07 Nov 08

**'Internet Legislation'** – Hands Off The Internet  
<http://handsoff.org/blog/category/Internet-legislation/>, 06 Nov 08

**'DontRegulate.org'**

<http://www.dontregulate.org/>, 06 Nov 08

**'Firefox Add-On Allows Users to Experience Chinese Internet Censorship'** – Open Net Initiative

<http://opennet.net/blog/2008/11/firefox-add-on-allows-users-experience-chinese-Internet-censorship>, 05 Nov 08

**'China Channel Firefox Add-on - Experience the censored Chinese Internet at home!'** – China Channel

<http://chinachannel.hk/>, 05 Nov 08

**'French pirates face net cut-off'** – BBC News

<http://news.bbc.co.uk/1/hi/technology/7706014.stm>, 04 Nov 08

**'Google, Microsoft help found anti-censorship group'** – Electronista

<http://news.bbc.co.uk/1/hi/technology/7706014.stm>, 29 Oct 08

**'Global Network Initiative Principles'** – Global Network Initiative

<http://www.globalnetworkinitiative.org/principles/index.php>, 29 Oct 08

**'Antitrust Division Manual, Chapter II. Statutory Provisions and Guidelines of the Antitrust Division'** – Department of Justice, Antitrust Division

<http://www.usdoj.gov/atr/public/divisionmanual/chapter2.htm>, 29 Oct 08

**'New steps to protect free expression and privacy around the world'** – Official Google Blog

<http://googleblog.blogspot.com/2008/10/new-steps-to-protect-free-expression.html>,

28 Oct 08

**'Civil Liberties'** - Wikipedia

[http://en.wikipedia.org/wiki/Civil\\_liberties](http://en.wikipedia.org/wiki/Civil_liberties), 28 Oct 08

**'European Convention on Human Rights'** - Wikipedia

[http://en.wikipedia.org/wiki/European\\_Convention\\_on\\_Human\\_Rights](http://en.wikipedia.org/wiki/European_Convention_on_Human_Rights), 28 Oct 08

**'Delta to censor WiFi: content inappropriate' for an aircraft blocked** – SlashGear  
<http://www.slashgear.com/delta-to-censor-wifi-content-inappropriate-for-an-aircraft-blocked-0318188/>, 27 Oct 08

**'Assessing the impact of CCTV'** – The Home Office  
<http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>, 27 Oct 08

**'ONI Home Page'** - OpenNet Initiative  
<http://opennet.net/>, 27 Oct 08

**'UK Home Office Releases Research on CCTV Effectiveness'** - Privacy International,  
[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-167206](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-167206), 26 Oct 08

**'Statement on CCTV Surveillance'** - Privacy International,  
[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-61926](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61926), 26 Oct 08

**'How "free" can our data be?'** – BBC Technology Blog  
[http://www.bbc.co.uk/blogs/technology/2008/09/how\\_free\\_can\\_our\\_data\\_be.html](http://www.bbc.co.uk/blogs/technology/2008/09/how_free_can_our_data_be.html),  
24 Oct 08

**'Dell, Universal Music offer DRM-free music bundles'** - Electronista  
<http://www.electronista.com/articles/08/10/23/dell.offers.music.bundles/>, 24 Oct 08

**'Dutch court orders Google to reveal Gmail user'** – The Register  
[http://www.theregister.co.uk/2008/10/20/dutch\\_court\\_orders\\_google\\_to\\_reveal\\_gmail\\_user/](http://www.theregister.co.uk/2008/10/20/dutch_court_orders_google_to_reveal_gmail_user/), 21 Oct 08

**'TOP TEN WAYS TO PROTECT YOUR PRIVACY ONLINE'** – Centre For  
DemocracyandTechnology  
<http://www.cdt.org/privacy/guide/>, 16 Oct 08

**'Is music winning the digital war?'** – BBC Technology Blog  
[http://www.bbc.co.uk/blogs/technology/2008/10/is\\_music\\_winning\\_the\\_digital\\_war.html](http://www.bbc.co.uk/blogs/technology/2008/10/is_music_winning_the_digital_war.html),  
14 Oct 08

**'BT rolls out Phorm web tracking - Times Online'** - Times Online

[http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article4847212.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article4847212.ece),  
02 Oct 08

**'Digital music - who can beat iTunes?'** – BBC Technology Blog

[http://www.bbc.co.uk/blogs/technology/2008/09/digital\\_music\\_who\\_can\\_beat\\_itu.html](http://www.bbc.co.uk/blogs/technology/2008/09/digital_music_who_can_beat_itu.html),  
17 Sept 08

**'The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State'** – Open Rights Group

[http://www.openrightsgroup.org/orgwiki/index.php/The\\_Impact\\_of\\_Surveillance\\_and\\_Data\\_Collection\\_upon\\_the\\_Privacy\\_of\\_Citizens\\_and\\_their\\_Relationship\\_with\\_the\\_State](http://www.openrightsgroup.org/orgwiki/index.php/The_Impact_of_Surveillance_and_Data_Collection_upon_the_Privacy_of_Citizens_and_their_Relationship_with_the_State),  
16 Sept 08

**'Data Protection Act 1998 (c. 29)'** – Office of Public Sector Information

[http://www.opsi.gov.uk/Acts/Acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1), 16 Sept 08

**'The Data protection Act'**

<http://www.dataprotectionact.org/>, 16 Sept 08

**'Internet anonymity endangered by UN agency project'** – Electronista

<http://www.electronista.com/articles/08/09/12/Internet.anonymity.threat/>, 16 Sept 08

**'Ad perfect'** - Google Official Blog

<http://googleblog.blogspot.com/2008/09/ad-perfect.html>, 15 Sept 08

**'El Reg drops in on Bletchley Park'** – The Register

[http://www.theregister.co.uk/2008/09/10/bletchley\\_park\\_campaign/](http://www.theregister.co.uk/2008/09/10/bletchley_park_campaign/), 12 Sept 08

**Scientology critics fight YouTube takedown notices** – The Register

[http://www.theregister.co.uk/2008/09/09/scientology\\_youtube\\_dmca\\_takedown\\_fight/](http://www.theregister.co.uk/2008/09/09/scientology_youtube_dmca_takedown_fight/),  
10 Sept 08

**'Sony Ericsson Launching Unlimited Music Downloads'** – Dial-a-Phone

<http://www.dialaphone.co.uk/blog/?p=2184>, 10 Sept 08

**'iTunes Beater Out for Christmas!'** – Dial-a-Phone  
<http://www.dialaphone.co.uk/blog/?p=2103>, 10 Sept 08

**'Official Google Blog: Another step to protect user privacy'** – Official Google Blog  
<http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html>,  
09 Sept 08

**'Phorm\_PIA\_interim.pdf'** – Phorm  
[http://privacy.phorm.com/Phorm\\_PIA\\_interim.pdf](http://privacy.phorm.com/Phorm_PIA_interim.pdf), 01 Sept 08

**'South Korean prez turns on the Internet'** - John Oates,  
[http://www.theregister.co.uk/2008/08/05/korea\\_Internet\\_law/](http://www.theregister.co.uk/2008/08/05/korea_Internet_law/), 01 Sept 08

**'Google: 'Even in the desert, privacy does not exist''** – The Register  
[http://www.theregister.co.uk/2008/07/31/google\\_desert\\_privacy/](http://www.theregister.co.uk/2008/07/31/google_desert_privacy/), 29 Aug 08

**'MPs report back from Internet's dark side'** – The Register  
[http://www.theregister.co.uk/2008/07/31/cms\\_report\\_Internet/](http://www.theregister.co.uk/2008/07/31/cms_report_Internet/), 29 Aug 08

**'AT&T to bar P2P activity from 3G networks'** – Electronista  
<http://www.electronista.com/articles/08/07/30/att.to.bar.p2p.activity/>, 29 Aug 08

**'No snapping: Photographers get collars felt'** - The Register  
[http://www.theregister.co.uk/2008/08/23/camera\\_analysis/](http://www.theregister.co.uk/2008/08/23/camera_analysis/), 23 Aug 08

**'Copyright lawyers accuse 25,000 UK videogame filesharers'** – The Register  
[http://www.theregister.co.uk/2008/08/20/davenport\\_lyons\\_25000/](http://www.theregister.co.uk/2008/08/20/davenport_lyons_25000/), 21 Aug 08

**'Cloud computing lets Feds read your email'** – The Register  
[http://www.theregister.co.uk/2008/08/20/cloud\\_computing\\_privacy/](http://www.theregister.co.uk/2008/08/20/cloud_computing_privacy/), 21 Aug 08

**'UK.gov to spend hundreds of millions on snooping silo'** – The Register  
[http://www.theregister.co.uk/2008/08/19/ukgov\\_uber\\_database/](http://www.theregister.co.uk/2008/08/19/ukgov_uber_database/), 19 Aug 08

**'Road Pricing 2.0 is two years away'** – The Register

[http://www.theregister.co.uk/2008/08/18/road\\_pricing\\_2\\_dot\\_beta/](http://www.theregister.co.uk/2008/08/18/road_pricing_2_dot_beta/), 18 Aug 08

**'Judgment against RIAA precedent for more defences'** – Electronista

<http://www.electronista.com/articles/08/08/14/riaa.ruling.sets.precedent/>, 14 Aug 08

**'Facebook sued for Beacon blunder'** – The Register

[http://www.theregister.co.uk/2008/08/15/faceboo\\_beacon\\_sued/](http://www.theregister.co.uk/2008/08/15/faceboo_beacon_sued/), 15 Aug 08

**'Warning letters to 'file-sharers''** – BBC News

<http://news.bbc.co.uk/1/hi/technology/7486743.stm>, 25 Jul 08

**'Music versus TalkTalk - it's war...'**

<http://www.bbc.co.uk/blogs/technology/2008/04/03/index.html>, 25 July 08

**'Music industry to tax downloaders'** – The Independent

<http://www.independent.co.uk/arts-entertainment/music/news/music-industry-to-tax-downloaders-875757.html>, 25 July 08

**'Warning letters to 'file-sharers''** – BBC News

<http://news.bbc.co.uk/1/hi/technology/7486743.stm>, 25 Jul 08

**'A blog about technology from BBC News'** – BBC Technology Blog

<http://www.bbc.co.uk/blogs/technology/2008/04/03/index.html>, 25 July 08

**'Music industry to tax downloaders - News, Music'** - The Independent

<http://www.independent.co.uk/arts-entertainment/music/news/music-industry-to-tax-downloaders-875757.html>, 25 Jul 08

**'Congress accuses American Phorm of 'beating consumers''** - The Register

[http://www.theregister.co.uk/2008/07/17/house\\_nebuad\\_hearing/](http://www.theregister.co.uk/2008/07/17/house_nebuad_hearing/), 18 Jul 08

**'Swedes call on Human Rights Court to review snoop law'** - The Register  
[http://www.theregister.co.uk/2008/07/17/echr\\_swedish\\_wiretap\\_law\\_review/](http://www.theregister.co.uk/2008/07/17/echr_swedish_wiretap_law_review/), 17 Jul 08

**'EU tells UK to deal with Phorm - or else'** - The Register  
[http://www.theregister.co.uk/2008/07/16/eu\\_warns\\_uk\\_over\\_phorm/](http://www.theregister.co.uk/2008/07/16/eu_warns_uk_over_phorm/), 16 Jul 08

**'Call for reform as UK data protection rules turn 10'** - The Register  
[http://www.theregister.co.uk/2008/07/16/dpa\\_10/](http://www.theregister.co.uk/2008/07/16/dpa_10/), 16 Jul 08

**'Phorm protestors picket BT AGM'** - The Register  
[http://www.theregister.co.uk/2008/07/16/bt\\_phorm\\_protest/](http://www.theregister.co.uk/2008/07/16/bt_phorm_protest/), 15 Jul 08

**'ebay UK pimps users' privacy for targeted ads'** - The Register  
[http://www.theregister.co.uk/2008/07/16/ebay\\_targeted\\_advertising/](http://www.theregister.co.uk/2008/07/16/ebay_targeted_advertising/), 15 Jul 08

**EU accidentally orders isps to become copyright police - The Register**  
[http://www.theregister.co.uk/2008/07/09/eu\\_telecommunications\\_legislation/](http://www.theregister.co.uk/2008/07/09/eu_telecommunications_legislation/),  
15 July 08

**'Isps laud their data pinging services but refuse to use them'** - The Register  
[http://www.theregister.co.uk/2008/07/07/massillon\\_and\\_newwave\\_use\\_frontporch/](http://www.theregister.co.uk/2008/07/07/massillon_and_newwave_use_frontporch/),  
13 Jul 08

**'Google's spycar revs up UK privacy fears'** - The Register  
[http://www.theregister.co.uk/2008/07/07/google\\_spycar\\_slammed/](http://www.theregister.co.uk/2008/07/07/google_spycar_slammed/), 12 Jul 08

**'Europe drafts law to disconnect suspected filesharers'** - The Register  
[http://www.theregister.co.uk/2008/07/06/europe\\_drafts\\_law\\_to\\_disconnect\\_filesharers/](http://www.theregister.co.uk/2008/07/06/europe_drafts_law_to_disconnect_filesharers/),  
11 Jul 08

**'Google, privacy and Street View'** – BBC Technology Blog  
[http://www.bbc.co.uk/blogs/technology/2008/07/google\\_privacy\\_and\\_street\\_view.html](http://www.bbc.co.uk/blogs/technology/2008/07/google_privacy_and_street_view.html)  
11 Jul 08

**'Would a data notification law improve UK data security?'** - The Register  
[http://www.theregister.co.uk/2008/07/04/data\\_protection\\_changes/](http://www.theregister.co.uk/2008/07/04/data_protection_changes/), 11 Jul 08

**'Transatlantic data sharing talks stumble over access to justice'** - The Register  
[http://www.theregister.co.uk/2008/07/03/eu\\_us\\_data\\_sharing/](http://www.theregister.co.uk/2008/07/03/eu_us_data_sharing/), 10 Jul 08

**'No defence for 'stealing' music'** – BBC Technology Blog  
[http://www.bbc.co.uk/blogs/technology/2008/07/no\\_defence\\_for\\_stealing\\_music.html](http://www.bbc.co.uk/blogs/technology/2008/07/no_defence_for_stealing_music.html),  
10 Jul 08

**'Virgin warns 800 punters for file-sharing'** - The Register  
[http://www.theregister.co.uk/2008/07/03/virgin\\_letters\\_numbers/](http://www.theregister.co.uk/2008/07/03/virgin_letters_numbers/), 10 Jul 08

**'Court slaps UK bittorrenters with landmark damages award'** - The Register  
[http://www.theregister.co.uk/2008/07/02/davenport\\_lyons\\_dream\\_pinball\\_win/](http://www.theregister.co.uk/2008/07/02/davenport_lyons_dream_pinball_win/), 10 Jul 08

**'Virgin Media rubbishes P2P throttling rumours'** - The Register  
[http://www.theregister.co.uk/2008/06/23/virgin\\_media\\_application\\_throttling\\_denial/](http://www.theregister.co.uk/2008/06/23/virgin_media_application_throttling_denial/),  
27 Jun 08

**'Pirate Bay bitchslaps Swedish law with SSL'** - The Register  
[http://www.theregister.co.uk/2008/06/23/the\\_pirate\\_bay\\_ssl/](http://www.theregister.co.uk/2008/06/23/the_pirate_bay_ssl/), 27 Jun 08

**'Compressed voip leaves eavesdropping clues'** - The Register  
[http://www.theregister.co.uk/2008/06/23/compressed\\_voip\\_traffic\\_analysis/](http://www.theregister.co.uk/2008/06/23/compressed_voip_traffic_analysis/), 24 Jun 08

**'Sweden ushers in bugging for all'** - The Register  
[http://www.theregister.co.uk/2008/06/18/eavedropping\\_sweden\\_now\\_legal/](http://www.theregister.co.uk/2008/06/18/eavedropping_sweden_now_legal/), 18 Jun 08

**'Swedish parliament rejects snoop everyone law'** - The Register  
[http://www.theregister.co.uk/2008/06/18/sweden\\_fails\\_on\\_snoop\\_john\\_b/](http://www.theregister.co.uk/2008/06/18/sweden_fails_on_snoop_john_b/), 18 Jun 08

**'Phorm failed to mention 'illegal' trials at Home Office meeting in 2007'** - The Register  
[http://www.theregister.co.uk/2008/06/18/home\\_office\\_phorm\\_meetings/](http://www.theregister.co.uk/2008/06/18/home_office_phorm_meetings/), 18 Jun 08

**'80% want legal P2P – survey'** - The Register  
[http://www.theregister.co.uk/2008/06/16/bmr\\_music\\_survey/](http://www.theregister.co.uk/2008/06/16/bmr_music_survey/), 17 Jun 08

**'Google preps net neut dowser'** - The Register  
[http://www.theregister.co.uk/2008/06/13/google\\_network\\_management\\_tools/](http://www.theregister.co.uk/2008/06/13/google_network_management_tools/), 17 Jun 08

**'EU security agency gets three more years'** - The Register  
[http://www.theregister.co.uk/2008/06/13/enisa\\_overtime/](http://www.theregister.co.uk/2008/06/13/enisa_overtime/), 17 Jun 08

**'Canada moots tough sanctions for DRM flouters'** - The Register  
[http://www.theregister.co.uk/2008/06/12/canada\\_copyright\\_reform\\_june\\_2008/](http://www.theregister.co.uk/2008/06/12/canada_copyright_reform_june_2008/),  
17 Jun 08

**'Google supports US privacy law'** - The Register  
[http://www.theregister.co.uk/2008/06/11/google\\_privacy\\_pledge/](http://www.theregister.co.uk/2008/06/11/google_privacy_pledge/), 16 Jun 08

**'Call to prosecute BT for ad trial'** – BBC News  
<http://news.bbc.co.uk/1/hi/technology/7438578.stm>, 14 Jun 08

**'Virgin Media and BPI join forces to attack illegal filesharing'** - The Register  
[http://www.theregister.co.uk/2008/06/06/virgin\\_media\\_bpi\\_deal/](http://www.theregister.co.uk/2008/06/06/virgin_media_bpi_deal/), 08 Jun 08

**'Bletchley Park activates online donations'** - The Register  
[http://www.theregister.co.uk/2008/06/05/bletchley\\_online\\_donations/](http://www.theregister.co.uk/2008/06/05/bletchley_online_donations/), 07 Jun 08

**'World+dog ignores Sweden's Draconian wiretap bill'** - The Register  
[http://www.theregister.co.uk/2008/06/04/sweden\\_wiretap\\_bill/](http://www.theregister.co.uk/2008/06/04/sweden_wiretap_bill/), 07 Jun 08

**'Internet censorship and mission creep'** - The Register  
[http://www.theregister.co.uk/2008/05/27/internet\\_censorship/](http://www.theregister.co.uk/2008/05/27/internet_censorship/), 30 May 08

**'Piracy growing as fewer fans buy downloads'** - The Guardian  
<http://www.guardian.co.uk/technology/2008/may/15/piracy.digitalmusic?Gusrc=rss&feed=technologyfull>, 28 May 08

**'The Pirate Bay plans to buy island'** - The Local  
<http://www.thelocal.se/6076/20070112/>, 28 May 08

**'What Do You Do When Someone Steals Your Content'** - Lorelle on wordpress  
<http://lorelle.wordpress.com/2006/04/10/what-do-you-do-when-someone-steals-your-content/>, 28 May 08

**'Openid'**  
<http://openid.net/>, 28 May 08

**'Deeplinks Blogs related to Anonymity'** - Electronic Frontier Foundation  
<http://www.eff.org/related/3005/blog>, 28 May 08

**'Pirate Bay Admins Charged with Assisting Copyright Infringement'** - torrentfreak  
<http://torrentfreak.com/pirate-bay-team-charged-080131/>, 28 May 08

**'bittorrent Anonymously'** - Btguard  
<http://btguard.com/>, 28 May 08

**'Feature: Protect Your Privacy When Downloading'** – Life Hacker  
<http://lifelifehacker.com/372633/protect-your-privacy-when-downloading>, 28 May 08

**'ANONYMITY & PRIVACY'** - JAP  
[http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html), 28 May 08

**'anonymity online'** - Tor  
<http://www.torproject.org/>, 28 May 08

**'International copyright talks seek bittorrent-killer laws'** - The Register  
[http://www.theregister.co.uk/2008/05/27/acta\\_leak/](http://www.theregister.co.uk/2008/05/27/acta_leak/), 28 May 08

**'UK.gov plans central database for all your communications'** - The Register  
[http://www.theregister.co.uk/2008/05/20/central\\_government\\_database\\_proposed/](http://www.theregister.co.uk/2008/05/20/central_government_database_proposed/), 23  
May 08

**'Massive Seedbox Links List'** - Torrent-Source  
<http://torrent-source.net/?P=64>, 08 Apr 08

**'PHP bittorrent Client'** - Torrentflux  
<http://torrentflux.com/>, 07 Apr 08

**'Isps demand record biz pays up if cut-off P2P users sue'** - The Register  
[http://www.theregister.co.uk/2008/02/12/anti\\_filesharing\\_paper\\_leak/](http://www.theregister.co.uk/2008/02/12/anti_filesharing_paper_leak/), 03 Mar 08