Date: Sunday, 17 May 2009
Name: Dephormation.org.uk
Contact: Pete
Address:

'Can we keep our hands off the net?'

Question 1 - Can we distinguish circumstances when ISPs should be forced to act to deal with some type of bad traffic? When should we insist that ISPs should not be forced into dealing with a problem, and that the solution must be found elsewhere?

The essence of the dilemma is freedom and liberty, versus control and safety. To paraphrase Franklin, we deserve neither liberty nor safety if we sacrifice essential liberty for temporary safety.

Censorship

In the most simplistic form, 'bad traffic' originating from a given source can be blocked by an IP address. A more sophisticated method of filtering can be applied to the *content* of communications, using 'Deep Packet Inspection' (DPI) to examine the detail of the messages.

The cultural view of 'bad' content varies between countries, and age groups, and for some audiences may include controversial topics such as war, drugs, sex, health, politics, and other material legal in the UK.

One highly contentious issue arises around the use of the internet to transfer media over peer to peer networks. Yet peer to peer technology can be used both *legally* and illegally.

Capping and Traffic Shaping

Several larger ISPs also impede 'heavy users' by capping and traffic shaping. This has the effect of stifling competition for online media services such as IPTV (Internet Protocol Television).

Yet users affected by capping and traffic shaping have often paid for a service that is advertised as 'unlimited'.

What is Bad Traffic?

Thus the difficulty lies in strictly and accurately defining 'bad traffic', particularly if that traffic is encrypted.

Allowing ISPs to implement unregulated 'protective' measures risks communication censorship, anti-competitive behaviour, and denies citizens the freedom to use services fairly.

Using DPI to trawl for and detect offences transforms the UK into an Orwellian nation of suspects.

Recommendations

1. **The solutions must be found elsewhere; such as in education, encouraging adequate parental supervision, and warranted surveillance. Legislating for 'bad content' is a matter for politicians. Policing crime is a matter for the police to fund and address (perhaps through the Central E-Crime Unit). ISPs must be prevented from creating and enforcing arbitrary restrictions on legal communications.**
2. **For the sake of personal liberty, and fair commercial competition, ISPs must remain as far as possible mere conduits, and nothing more.**
3. **UK ISPs must be prevented from censoring telecommunications without the explicit consent of their customers, or legal authority. (For example, it is understood that UK mobile broadband connections are subject to 'child friendly' content filters by default – the details of the filter have not been published)**

Question 2 - Should the Government be intervening over behavioural advertising services, either to encourage or discourage their deployment; or is this entirely a matter for individual users, ISPs and websites?

Behavioural targeting is a technique used by businesses to anticipate the interests of their customers.

The use of private and confidential communication data for behavioural advertising is, and should always remain illegal. It allows businesses to anticipate the interests of *other companies'* customers.

The Nature of World Wide Web Communications

It is important to recognise and understand the **conversational** nature of interactions between web sites and visitors. Web pages are not broadcast like television pictures. The internet is a communications infrastructure. **A web page is the content of a private message to the user who is viewing a web site.**

Thus the intelligence that can be obtained by monitoring those private and confidential interactions is often highly sensitive and highly valuable.

Monitoring such communications amounts to

- Mass personal surveillance
- Mass industrial espionage
- Mass copyright infringement

Mass Personal Surveillance

In the UK, citizens are entitled to expect that their private, confidential and often sensitive communications will not be monitored or interfered with, without consent or suspicion of criminal misconduct. This is assured by the Regulation of Investigatory Powers Act. The right to private and confidential communication is vital to democracy (particularly so e-voting), freedom of speech, freedom of association, freedom of expression. It is guaranteed by Article 8 of the European Convention on Human Rights.

Mass Industrial Espionage

UK businesses also require and are entitled to expect that their private and confidential communications with customers and suppliers will not be intercepted and abused by telecommunications companies. This should also be assured by RIPA.

By monitoring the conversational exchange between a website and their visitors, it is possible to target those visitors with advertising for competitor products and services.

The use of DPI advertising therefore conflicts with the communication companies' role as a trustworthy 'mere conduit', and destroys any trust or confidence in an Internet Service Provider that instead uses private and confidential communication traffic for economic intelligence gathering.

This is the digital equivalent of opening business letters, and selling the commercial intelligence obtained to competitors. By installing such systems in the largest UK ISPs, it would be possible to monitor 75% or more of the private and confidential communications between any online business and any of its customers.

Mass Copyright Infringement

The creator of a web site receives no consideration for the duplication, processing, and commercial exploitation of their creative work. The model of operation is completely parasitic.

Worse still the creator is damaged, by the promotion of competitors using the intelligence obtained. This copyright violation will harm the businesses that invest most effort, time, and money accurately presenting their products and services on the World Wide Web. It is simply digital media piracy.

Impact on UK Telecommunications

Failing to uphold the privacy, security, and data integrity of UK telecommunications will collapse confidence in all methods of communication. The same techniques presently proposed for web traffic can also be applied to voice, email, sms and all other methods of personal and commercial communications.

At that point - without resorting to encryption - all communication privacy in the UK is at risk.

Encryption creates additional economic cost, imposes issues of technical interoperability, and creates an obstacle to legitimate use of surveillance for law enforcement.

Restricting such technology does not deny users liberty or choice.

Desktop 'spyware' can be freely installed by people who so wish. Evidence to date suggests that, given informed choice, people reject such intrusive surveillance.

Recommendations

1. **Existing interception laws must be enforced. Future deployment of interception-based advertising should be stopped – as it has been in the US – and a prosecution brought against those responsible for BT's trial of Phorm on hundreds of thousands of people and the web sites that served them in 2006-07. Statements by the Home Office and the Information Commissioner claiming that interception based advertising systems can operate lawfully must be withdrawn.**

Question 3 - Is there a need for new initiatives to deal with online privacy, and if so, what should be done?

Measures in the Telegraph Act 1868 (c.110) made it a criminal offence to "disclose or in any way make known or intercept the contents or any part of the contents of any telegraphic messages or any message". (This act was repealed by Statutory Instrument 2001/1149 in 2001).

Similar measures must be reinstated to clearly and unambiguously outlaw the disclosure to a third party of the content, the sender, or the recipient of any electronic message.

With the widespread use of mobile communication devices, such as mobile broadband and mobile telephony, legislation would need to be updated to outlaw disclosure of location data too.

Recommendations

The following measures are required.

1. **There must be effective penalties for malicious commercial violation of the Data Protection Act and the Privacy and Electronic Communications Regulations. At present the Information Commissioner's Office claim no action can be taken if the malicious misconduct has already ceased.**
2. **The Government should review whether Ofcom can combine the roles of regulating communications, regulating the media, and encouraging investment in infrastructure without unacceptable conflicts of interest arising. The Government should consider whether Ofcom should be split into a telecommunication regulator and a media regulator.**
3. **Telecommunication companies should be encouraged to develop a voluntary code of conduct, including the commitment to refrain from certain conflicting business pursuits, particularly those involving media and advertising interests.**
4. **The Information Commissioner's Office must employ qualified IT expertise, and demonstrate a capability to conduct independent critical regulation of the Communications and IT industry.**
5. **Recognising the advent of mobile communications, the privacy of data concerning the location of the parties to a communication should be protected.**
6. **The Government should prohibit trading in personal data without explicit consent of the data subject.**

"The Internet in general has and deserves the same protection as paper mail and telephone."
– Sir Tim Berners Lee

Question 4 - Is the current global approach to dealing with child sexual abuse images working effectively? If not, then how should it be improved?

The current approach to dealing with child sexual abuse images is not effective. Defining illegal content is a matter for politicians. Policing internet content & communication should a matter for law enforcement agencies (such as Police Central E-Crime Unit), with full public accountability for any decision to implement censorship.

Question 5 - Who should be paying for the transmission of Internet traffic? Would it be appropriate to enshrine any of the various notions of Network Neutrality in statute?

There is not, and never has been a funding gap in the transmission of internet traffic.

Internet subscribers (personal users and corporate customers) as sender or recipient of data traffic pay for their services according to the volume of traffic transferred and/or the speed of connectivity and/or standard of service provided.

Internet Service Providers charge one another interconnect fees, in a similar fashion to interbank settlements. These interconnect agreements[1] may take the form of

- **Bilateral Agreements -** Two operators interconnect. Each accepts traffic destined for its own customers and originating within the other's network. Neither network delivers traffic to third parties on behalf of the other. *Each charges for the volume of traffic it accepts from the other.*
- **Sender Keep All -** As with bilateral settlements, two operators each accept traffic from the other, for delivery to the accepting network's customers. *But no charge is made.*
- **Transit -** One operator, the provider, accepts traffic originating within the other's network, destined not only for its own customers but for third party networks with whom the provider in turn connects. *The provider charges a fee for carrying the other network's traffic.*
- **Multilateral exchanges -** An operator connects to an exchange, a (usually commercial) facility carrying connections from multiple operators. There, traffic is routed to other operators' networks via equipment provided by the exchange and according to rules administered by the exchange; *the operator settles through the exchange for traffic that others carry on its behalf and that it carries on behalf of others.*

Well managed Internet Service Providers in the UK are profitable. Charles Dunstone of CarPhone Warehouse described his business as one of scale. He recently stated that operational efficiencies allowed the company to generate £150M.

In the UK, funding issues occur because UK domestic Internet Service Providers are overselling the availability of 'unlimited' flat rate internet access to high consumers (leading to capping/throttling for cost control).

As internet access speeds grow ever faster, the difference between the promised 'unlimited' service and the capability to sustain unlimited consumption will become ever more acute. ISPs, like other utility companies, will eventually have to accept pricing based on resource consumption.

Recommendations

1. **The transmission of internet traffic is paid for by originators and recipients, it is a profitable business, there is no funding gap and no need for intervention**
2. **Regulators need to force the overselling of 'unlimited' internet access to end**
3. **Internet Service Providers must be prevented from arbitrarily capping or throttling services, abusing private/confidential communication traffic, and censoring legal communications without explicit consent.**

[1] source: Interisle Consulting Group