Internet and Mobility: Youth Technology Trends

This paper examines internet and mobility trends and how these will impact the youth market. Smartphones and tablets will be the next big thing – how will this impact on the user experience? Ever more personal data is digitised and online; when this is combined with the emergence of geolocation, powerful new features and services are offered, but what are the risks? There are numerous standards, technologies and protocols on the horizon, but how will they affect and influence young people?

The UK Council for Child Internet Safety (UKCCIS) brings together 180 organisations and individuals from government, industry, law enforcement, academia and charities, including parenting groups. Their aim is to work in partnership to keep children and young people safe online. Working together in partnership - across industry and government - is essential to delivering practical and effective solutions to help keep children safe online.

Research and evidence is vital to inform the promotion of a safer online environment for children. The UKCCIS Evidence group is made up of academics and representatives from industry. It aims to provide UKCCIS with a research strategy and a timely, critical and rigorous account of available research relevant to the ongoing work of UKCCIS. The evidence group commissioned this report as part of its remit to inform UKCCIS's work.

Independent research funded by BT

This is independent research funded by BT. The views expressed in the document are the views or the researcher, Chi Durbin, and do not necessarily reflect the views of BT.

Disclaimer

Every effort has been made to ensure this document accurately describes technology trends. Nonetheless, the analysis is that of the author and may not necessarily reflect those of other individuals and institutions, including those cited within.

Scope

This paper overviews emerging trends in internet and mobility and how these affect the child and youth market. It is *not* an in-depth analysis but rather aims to give the non-technical reader an insight into changes in the technological landscape and user experience. The focus, as befits the UKCCIS remit, is on the risks rather than the opportunities afforded by new technologies to children, in so far as these exist and may be identified. Furthermore, the focus is on how technologies may pose certain risks, and it does not present detailed evidence regarding whether or not such risks do, in practice, result in harm to children.

Executive Summary

This paper aims to provide the reader with a base understanding of the issues and trends in internet and mobility, and how this might impact young people. This is not limited to technological development and new capabilities, but how it will affect the user experience and how traditional risks have evolved in these paradigms.

Mobile phones and the internet have reached virtual ubiquity in the UK, but many parents and children are still unclear about the risks that these technologies pose. Smartphones and tablets, widely expected to be the 'next big thing', combine many of the features and capabilities of mobile phones and the internet, and bring with them many of the risks. Perhaps the biggest concern is the reduced capacity for parental oversight for these devices.

This document looks at the current state of play in the smartphone market, the key players and typical features; it also examines evolving and future capabilities. Tablets have been on the IT horizon for some time, but with the launch of the *iPad* they have achieved mainstream acceptance and success. Tablets are in essence smartphones with larger screens for a better user experience, offering all the features and capabilities and bringing with them all the risks inherent with smartphones.

There are two classes of risk with smartphones and tablets - technical and social. The big technical fear is the porting of PC based threats (viruses and malware), which may have a larger impact but are perhaps less likely (because of the lessons learned from PCs). The social risks – sexting, cyberbullying, identity theft and fraud, potentially harmful content and sexual predation – are not entirely new; they have merely evolved in step with technology and the internet.

Geolocation is a technology that allows a user to locate services and events near their geographic location; this is achieved using GPS, Cell ID, A-GPS or IP geolocation (the latter typically more relevant to fixed internet devices). Geolocation also brings with it the risk of tracking and privacy intrusion – the UK has a code of practice for location services providers, but there are instances of organisations failing to properly handle this data.

Personally identifiable Information is known to be the wares of identity thieves and fraudsters. This is often stolen wholesale from organisations (beyond the control of the individual) and with computer viruses. Social networks and Web2.0 [2] are seeing users post their own personal information on publicly visible profiles, and there is some evidence to suggest this is being mined by potential employers and college admissions tutors. Personal information may also be of value to child abusers - *there have been numerous investigations into the possibility [87] and much hyperbole [86] especially surrounding the 90,000 sexual offenders removed from MySpace [85]*, though grooming may not involve the use of personal information obtained through social networking sites. Social networks (the typical source of such personal information) are statistically safer than other internet activities [83] [87]. While the use of privacy controls in social networks, or setting profiles to private by default, might mitigate some risks, there will remain the problem of an offender infiltrating children's social networks and then befriending those who have private profiles.

Key Points

- The smartphone and tablet now provide a mature user experience for mobile internet access. Mobile computing takes the risks associated with the internet outside of the home and away from easy parental oversight. *While this is also the case with laptops/netbooks, these devices are portable rather than truly mobile.*

- Smartphones and tablets (or another device that provides a similar feature set) are set to become ubiquitous.

- Near Field Communications (NFC), High Definition (HD) media, multiple screens, folding screens, digital projectors, multiple processors and 3D screens are all likely to be seen in the next generation of smartphones.

- Geolocation provides a method to physically (geographically) locate users – this capability enables the user to find services in their area (e.g. locate a restaurant), but the technology also has privacy implications. *The risk of 'geo-stalking' is considered low.*

- The digitisation of personal data is ever present. Users often publish personal information on publicly available social network pages and other web 2.0 sites (e.g. blogs). This is probably not a key target for fraudsters, but users should consider the risks and practice better security hygiene by engaging privacy controls.

- With users storing more and more of their lives on phones and computers, they should think seriously about disaster recovery (backups) and security (encryption, firewalls, anti-virus software). Many such products and services are free.

- New technologies such as HTML5, 4G, IPv6, and principles such as net neutrality may not directly impact the user, but do provide new features and capabilities for developers and service providers. This will enable the creation of new products and services which may have the potential to change behaviour through the user experience.

- The risks posed by the internet and mobile devices are *not* new. They are the risks children have always faced (and will continue to face in the future), and are a product of society. These risks *have* evolved with new technology and the internet, they now manifest in new ways and bring new challenges but the underlying nature of the risks is unchanged.

Contents

Tables

1. INTRODUCTION

This paper examines trends in internet and mobility (based on cellular and Wi-Fi) and how these have affected young people in the UK. Its aim is to give the reader an insight into major developments in the ecosystem and what this will mean for the next generation of users. This paper focuses on smartphone and tablet devices (considered by some to be the next 'big thing' in mobile computing), and geolocation and personal data (two underappreciated commodities that are continuing to become more valuable). The paper also covers emerging protocols, standards and technology and how these will shape the landscape of internet and mobility.

This document is a meta-analysis that draws on a broad range of sources including surveys, sales figures and projection, industry press releases, products reviews, product roadmaps, and respected industry news sources.

Mapping the next generation of technology is a relatively accurate process - research activities, hardware developments, protocols drafts etc are generally public and well known throughout the industry. With the ever-falling cost of devices[1], offering cheaper and greater access it can be assumed that greater numbers of people will buy products and services from sales figures and projections. Predicting usage patterns and applications (e.g. why *Facebook* is a runaway success while *Bebo* struggles) is entirely different. It is a function of human preference, something which continues to evade product designers, engineers and marketers. It is possible to say people will be watching HD content on the next generation of smartphones; it is not possible to say what they will be watching nor the application or service providing the content.

Information security is the cornerstone of risk in the technological world. A computer or smartphone can store a complete history of a person's life - photos, videos, diary, school work and their 'electronic footprint', browsing history, passwords, purchase history, geographic location, calendar, messaging history (SMS, email, Instant Message or IM), call logs etc. Some of this information is destined to be shared with a wider audience; some of it is private and must be secure. Identity theft has long been a problem on computers and the internet, but this problem now exists on smartphones too. It is perhaps harder to tackle in this form (at least in the current generation of devices). In addition to identity theft is the issue of 'free' services and applications that have no explicit monetary value but require the user to hand over personal information. Previously the user could register with fake details, but as these applications and services hook into mobile devices and services such as *Facebook*, the information is passed directly from provider to provider, with the user largely out of the loop. How secure is a smartphone? What happens if it is lost or stolen? What about the risk of remote exploits – theft of data or services without the handset leaving the user's possession? How can users protect against this?

With more and more personal information on the internet and better indexing, new opportunities and risks are appearing. In particular, problems are occurring from potentially

[1] Moore's law: an informal law that says the number of transistors on a integrated circuit doubles every two years. This is linked to continually improving performance, and thus falling cost, of computers and digital electronics.

embarrassing information posted to social networks, wider indicators of identity fraud, and storage of location data.

These new and emerging risks come in addition to the more familiar risks of grooming, bullying, and exposure to unwanted material etc which now can present themselves in an ‘always on, always available’ connected form.

2. SMARTPHONES

Once the preserve of the enterprise providing web, email and calendar functions and smartphones have, in recent years, evolved and become a mainstream consumer technology. Whilst not 'new', the user interfaces have matured to a stage where mobile computing is no longer an awkward or niche experience – it is this (rather than the devices or principle) that is considered likely to be the next 'big thing' [81].

Though no standard definition exists, a modern smartphone would likely have most if not all of the following capabilities - high speed internet access, large storage capacity, email, calendar, Instant Messaging (IM), GPS, multimedia capability and cameras, Wi-Fi, Bluetooth, accelerometer (tilt sensor for image rotation and image stabilisation), digital compass and the ability to download and run additional applications. Smartphones offer the user much of the functionality and features of a laptop or computer.

2.1 Market Overview

The key players in the smartphone market are *Symbian, RIM, Microsoft, Apple,* and *Android*.

The *Symbian* operating system has been in smartphones for over a decade and although it has been available on other hardware *Symbian* is probably most synonymous with *Nokia*, featuring on many of their mid to high end handsets. *Nokia* are moving to *Windows Phone* as their main smartphone operating system [1], this will likely see a substantial decrease in *Symbian's* market share in coming years.

Microsoft has two incompatible smartphone operating systems, the legacy *Windows Phone 6.5* (formerly *Windows Mobile*) and the (new) *Windows Phone 7.* Though only available since late 2010, *Windows Phone 7* has shown strong sales [4].

Research In Motion (*RIM*) makers of the *Blackberry* range of smartphones were originally in two-way paging in North America. They have a long history in the corporate world due largely to the way email is handled and the tools which allow corporate IT departments to manage entire mobile estates. *Blackberry Enterprise Server* (*BES*) integrates with *Microsoft Exchange* and other email systems to provide unified business communications and a rich set of management and administration features. *Blackberry Internet Service* (*BIS*) is a managed service that provides a similar but stripped down feature set tailored to the consumer market.

Apple entered the smartphone market in 2007 with the *iPhone*. Now in its fourth revision, *Apple* maintains tight control over the value chain – only software approved by *Apple* can be installed. This is restrictive in terms of choice but does have security benefits[2]. Applications have been refused approval and even removed from the *App Store*[3] for a number of reasons [2]. This has spawned a cottage industry known as 'jailbreaking' – gaining full access to the *iPhone* and installing applications not approved by *Apple* [3].

[2] Viruses and malware are less likely when the value chain and delivery mechanism is managed.

[3] The repository of *iPhone* software.

The *iPhone* invigorated the smartphone market and broadened its appeal by making a portable computer that made phone calls rather than a feature rich phone. Failure to focus on the user interface (UI) and user experience (UX) have been cited as key reasons for the decline of *Symbian* [19]. Added strengths arose through their *Apps Store* (based originally on *iTunes*) and developer community.

Android is a mobile operating system from *Google* based on *Linux*. *Google* maintains the operating systems but does not manufacture handsets. *Android* phones are produced by a range of companies including *Samsung*, *HTC*, and *Motorola*, which choose and customise the features of the OS depending on the functionality desired and market for the phone.

Smartphone sales have seen substantial growth in recent years, outselling PCs in the fourth quarter of 2010 [5]. *Table 1 shows global smartphone sales and market segment for 2009 and 2010.*

	2010	Market segment	2009	Market segment
	Units 000s	%	Units 000s	%
Symbian	111,576.7	37.6	80,878.3	46.9
Android	67,224.5	22.7	6,798.4	3.9
RIM	47,451.6	16.0	34,346	19.9
Apple	46.598.3	15.7	24,889.7	14.4
Microsoft	12.378.2	4.2	15.031	8.7
Other	11417.4	3.8	10432.1	6.1

Table 1 - Global Smartphone Sales. Source Gartner [6].

2.2 Evolving Capabilities

The following capabilities are beginning to appear in smartphones, or are likely to appear in future generations.

2.2.1 Near Field Communications

Near Field Communication (NFC) is a very short range (only a few centimetres) wireless communication technology. This has numerous possible applications, including mobile payment (multiple trials are currently underway [79]), proximity card (e.g. *Oyster card*) replacement, RFID reader (e.g. reading RFID barcodes).

NFC consists of two key components - the antenna and the secure element (this can be built into the phone, the SIM, other accessories such as phone covers or an expandable module e.g. MicroSD card). The secure element is managed by a trusted provider that dictates what applications can be installed i.e. what the device can be used for [7]. Examples of potential trusted parties for managing the secure element include the network operators, banks, and credit card companies. The time to mainstream adoption is three years or less.

Some phones already have support for NFC, such as the antenna and the secure element, and more are in development [78].

2.2.2 High Definition

There are already phones on the market that are able to record and playback high definition video (scaled down because of small screen sizes), and this trend is expected to continue. This goes hand-in-hand with growing camera megapixel count. The time to mainstream adoption is two years or less.

2.2.3 Screens

Smartphones are becoming more powerful and more like PCs all the time. A major limiting factor has been the screen size, but potential ways to address this are emerging; multiple screens, folding/malleable screen and projection. Dual screen devices are not uncommon, and dual screen (clamshell with screens side-by-side) smartphones are available [10] and others seem probable [82]. An approach, or one similar, is likely to gain traction in future - smartphones providing more screen space without increasing the form factor. The time to market for dual screen devices is expected to be two years or less.

Future smartphones may incorporate a form of folding malleable screen the user can unfold to a size suitable to the task in hand [11] [12]. The time to mainstream adoption for folding screens is probably five years, and it is expected to take two years to finalise the manufacturing processes [76].

2.2.4 3D

With a 3D screen (special glasses won’t be necessary), and dual cameras, it will be possible to create and enjoy 3D content (photos and video) on a smartphone [9] [13]. This feature is expected to become common on high end media phones. The time to mainstream adoption is expected to be three years or less.

2.2.5 Projectors

Digital projectors are a common sight in meeting rooms and presentations, and the technology is now available on phones too. Micro projectors add to the physical size of the phone, and drain the battery quickly when in use. Initially they appeared as plug in accessories, but have since been integrated into handsets. They will probably not be a common feature across the smartphone landscape for some time but may appear in high end and media centric devices [8]. The time to mainstream market is expected to be three years or more.

2.2.6 Multiple Processors

As smartphones become more powerful and feature rich, they will likely contain multiple processors (in particular the high end models) as seen in [9]. The time to mainstream adoption is two years or less.

2.3 Platform Convergence

Platform convergence is the conflation of features and functionality from previously separate but similar systems, such as computer and phone features converging into smartphones, with emails, IM, *Facebook* messaging, SMS converging – all are available to a phone’s messaging function. Users choose to message each other from which service best meets their needs. As youth are able to access new messaging services from their phones, SMS, the dominant standard is in decline [62].

The key devices to watch would appear to be the smartphone and the tablet (essentially a smartphone with a bigger screen). These devices will supplant traditional phones, MP3 players, PMP, sat nav, portable gaming devices, cameras, netbooks, and to some extent laptops. Users will continue to own these individual devices (notably where the user has an additional need e.g. a keen photographer with a DSLR) but they will become less common – particularly in the mid to long term. Users will generally carry a 'digital device' that performs the following functions 'well enough' so that they will not need (and certainly will not carry) additional devices.

- Phone
- Messaging
- Internet (mostly web and web services)
- Media (MP3, video playback, photo album, streaming)
- Camera (photos and video)
- Navigation (primarily GPS/A-GPS)- **DN -** I think this list can be removed

2.4 Technical Risks

Botnets are networks of compromised computers known as zombies or bots under the control of hackers (bot herders). Computers can be compromised via infected emails, drive-by-downloads, Trojans, operating system or application vulnerabilities etc, giving the hackers full control of the computer. Botnets are typically used for spam distribution, distributed denial-of-service (DDoS), click fraud, search engine manipulation (spamdexing), and theft of personal information and login credentials (e.g. internet banking user name and password).

Mobile malware, viruses and botnets have long been an industry fear [14] [15], but unlike PCs (where they are an epidemic), they have largely appeared unnoticed [suggested rewording] on smartphones. Although botnets (and other malware) have [been noted – suggested rewording] on smartphones, [16] [17] they have yet to become an endemic problem. Smartphones are becoming more powerful, more numerous and contain more personal information.
Additionally, people may be less aware of the risks and less rigorous in their security hygiene. However, most smartphone applications are signed[4] and/or require specific privilege escalation[5] (necessary to access many functions and data). There are four, probably soon five (expected increase market share of *Windows Phone 7*) major smartphone platforms. This makes creating and delivering the code (virus/malware) harder and less effective, and perhaps less attractive. In contrast a single platform, *Windows* makes up 90% of traditional computers [18].

The next generation of smartphones will face new threats and contain new vulnerabilities. It is likely new mobile botnets will appear, but unlikely they will become the major security issue they are on the desktop, at least in the short term. However, users should of course practice good security hygiene.

[4] Digital signatures are a mathematical method for proving the authenticity and integrity of a file.
[5] The user has to permit explicitly the action or installation – it cannot happen in the background.

2.5 Social Risks

As well as the technical risks facing smartphone users, the social risks must also be considered. Sexting, cyberbullying, identity theft and fraud, exposure to potentially harmful material and grooming are very much in the public conscience. Egregious media coverage [51] and (perhaps) the perceived complexity of the internet have left many ill-informed and poorly equipped to face these threats.

None of the above threats are new: they have in some form or other always existed in society. The following table lists each of these modern threats and their pre-internet equivalent.

Internet era	Pre-internet
Sexting	'You show me yours, I'll show you mine'
Cyberbullying	Bullying
Identity theft and fraud	Identity theft and fraud via offline personal information
Harmful material (pornography, hate speech, violent content)	Pornographic magazines and video tapes, far right demonstrations, football violence, *The Anarchist Cookbook*
Grooming	Grooming, child abuse, molestation

Table 2 - Internet Vs Pre-internet risks

The 'game changing' aspect to each of these risks is how the following features of digital technology and the internet have affected them.

- Always-on / always there.
- Capture and recording of events.
- Permanence / persistence.
- Distribution / ease of access.
- Batch processing / copying.

The following examines how these features and functions have evolved these threats.

2.5.1 Sexting

Only the individuals present at 'you show me yours...' (probably no larger than a small group) see anything or know what happened. Sexting (sharing sexually explicit messages) provides a digital record (images or video) which can be replicated without loss of fidelity and distributed almost instantly among a peer group, or even published in a public forum. If a child told their peers they had seen another child naked, the other child could deny the event ever took place (boys are prone to exaggerating such matters). The quality of digital cameras, even on budget phones[6], is typically high enough to identify the individuals involved and makes repudiation much harder[7].

[6] Numerous phones in the under £50 price bracket have 2 megapixel cameras.

[7] Interestingly, the power and simplicity of modern photographic manipulation software mean photographs can be easily altered (often referred to as 'Photoshopping'), and thus also easily denied. Altering video is considerably harder, and thus difficult to repudiate, but is becoming easier.

Digital information is persistent and often virtually permanent. It can be stored (and accessed) in multiple locations (SNS, blogs, emails, photo and video sites e.g. *Flickr* and *YouTube*). Without direct control over the data (for example, someone else has uploaded a sexting video (underwear, no visible genitals), a user may have great difficulty having the photos (or video) removed. Once a service provider is notified of such material, it can be hours, maybe days, before the content is removed, during which time many individuals may see and even mirror[8] it.

2.5.2 Cyberbullying

Bullying has always been a part of society, particularly among children, but home can no longer be considered a sanctuary. The always-on/always-with-you nature of phones (smartphones especially) allows bullies to torment their victims at anytime.

Cyberbullying also brings with it anonymity through the use of sock puppets[9] and spoofing[10]. Acting from a distance may also empower bullies and further desensitise them to their actions [65]. Such considerations are beyond the scope of this paper and are mentioned here for completeness.

Although cyberbullying is a poorly researched and poorly understood phenomenon, sources suggest perhaps as much as 30% of children are involved as either bully, victim or both [52]. The effects of cyberbullying *may* be more severe than traditional face-to-face bullying [53] and have longer term effects [54].

2.5.3 Identity Theft and Fraud

Identity theft has always been a problem; the internet allows fraudsters to operate anonymously, from anywhere, targeting thousands (even millions) of individuals simultaneously. Many of processes of identity theft are automated allowing fraudsters to quickly and easily exploit stolen credentials.

2.5.4 Potentially Harmful Material

Potentially harmful material has been a problem for parents and governments throughout history, especially following the invention of the printing press (and increasing literacy rates).

Pornography and obscene literature, subversive literature, hate speech, far right marches, football violence, ‘video nasties’ – these have all existed for at least a generation. The internet publishing and distribution model[11] means the volume of harmful content is greater than before, and the bar to access is much lower. Previously harmful materials had to be produced (printed, recorded, organised) and a physical product (or people) needed to be transported to a destination (library/shop/market). This involves resources, costs, and logistics which were previously a bar to entry. Monitoring, restricting and policing such

[8] Copy and republish.

[9] User accounts (SNS, IM, email) registered with a false identity i.e. false flag.

[10] A technical term which means to shield a user’s identity.

[11] Anyone can post content on the internet for free, which can be easily found and consumed by a (potentially) huge number of people.

material was far easier. With the exception of child abuse images[12], every type of potentially harmful material can be accessed in seconds on the web, from anywhere at any time. To a large degree harmful content can be filtered using software - this is relatively straightforward on a computer but can be difficult on a smartphone.

UKCCIS readers wishing to learn more about filtering should consult the Parental Controls work stream outputs.

2.5.5 Sexual Predation

Paedophilia has always existed, but it has only received widespread public attention since the 1980s [56]. While paedophiles are traditionally perceived as the 'dirty old man' type, the overwhelming majority of child abuse takes place within the family, or at the hands of individuals well known to the family [57]. Internet grooming is rare, but some risk does exist. Numerous factors and behaviours influence a child's risk of sexual victimisation [36], such matter are beyond the scope of this document and mentioned only for completeness.

How has technology changed the dynamic of grooming? Ignoring individuals known to the family (such people are typically trusted), parents could, before the arrival of the internet monitor who their children met with relative ease. Now children can easily converse with 'faceless' strangers anywhere in the world. This distance[13] and anonymity may be empowering potential child abusers, and be more difficult for parents and children to identify.

The vast majority of internet grooming is of post pubescent children [57], and the majority of groomers are open and honest about their intentions [36]. Such blatant advances should be easy for both parents and older children to identify. The more devious approaches can be difficult to detect. They pose the challenge of a cooperative victim[14] – a child who believes they are in a loving relationship and wants to avail themselves to their abuser [36] – who is constantly online and available.

Technology does have a part to play keeping children safe. Approximately 80% of grooming is blatant solicitation, and this is trivial to detect (automated analysis and classification is not necessary). However, it is extremely difficult to determine whether a teenager (the high risk group) is flirting with someone their own age or someone *pretending* to be a teenager - the conversation is essentially the same (showing interest and affection, being attentive etc).

Many of the 'new' threats to children are the 'old' threats re-vamped, threats that have existed throughout human history, and will to continue to manifest in the future. The underlying nature of these risks has not changed, they have evolved with technology and been catalysed by the omniscient reach of the internet. This has the potential of considerably magnifying their impact – *suffering and victimisation.* Some threats, however, are new, for example the possibility of abusing a child via webcam in their bedroom.

[12] Websites hosting child abuse images are not indexed by search engines (the true volume of child abuse material on P2P networks cannot be independently verified, as this would be illegal).

[13] The dissociative effect of 'faceless' communication as well as physical distance.

[14] Their emotions having been manipulated by their abuser.

The first stage in mitigating these risks is recognising their origins and addressing their root social causes. Technology can help, particularly in the defence of younger (more naive) children, but it will remain a bit player. Education, vigilance, support and intervention are the most effective way to combat social risks.

2.6 Opt-out filtering

Readers wanting a fuller technical understanding of the issues surrounding classifier design and opt-out filtering should consult the UKCCIS Parental Controls workstrand.

At present internet access in the UK is provided as an 'unfiltered pipe' - the user receives (access to) everything and chooses what they want to enjoy. If the user wants to restrict certain material they 'opt-in' to content filtering. Opt-out filtering refers to a model where internet access is provided through a 'censored pipe' (with potentially harmful information removed). If users want access to censored material they have to 'opt-out' of filtered content. This is essentially a reversal of the current system.

Whilst opt-out might at first seem like a panacea against potentially harmful material, it is fraught with technical and social difficulties.

2.6.1 Failure Rate and Performance Degradation

In order for material to be filtered it first has to be classified. There are two key ways to achieve this: list (indexes), and analysis. Content can be automatically classified on-the-fly (analysed based filtering) as it traverses the network, or classification can be list based[15].

Classification is far from 100% reliable, trending towards a 20% failure rate - 20% of content that *should* be blocked is not (underblocking), and 20% of content that *should not* be blocked is (overblocking) [58]. More restrictive classification results in greater overblocking, less restrictive classification leads to greater underblocking. Classification of pornography is typically more accurate than classification of other potentially harmful content. Filtering static web content (and email) is relatively easy, filtering dynamic (changing) content, particularly Web2.0 (UGC) e.g. social networking sites and IM is considerably more difficult – and has a far higher failure rate.

Opt-out filtering can only be implemented where content delivery is controlled, effectively limiting its application to service provider networks. Theoretically this could be achieved using only major ISPs (all but the largest ISPs backhaul at least some traffic over major providers). This would be technically unviable and probably illegal under RIPA[16].

Real-time content analysis typically adds significant latency internet traffic [59], users experience this as lag (webpages take longer to load, applications become unresponsive). The majority of internet traffic is managed by Transmission Control Protocol (TCP) - when TCP detects latency (a drop in performance) it slows the data transfer rate to ensure data is

[15] In order to be added to a list, content must be classified in some way – human examination, statistical inference, content labelling etc. Though important from a cost /resource/quality perspective, how the list is compiled and managed is not important to its operation. It is treated as an external artefact.

[16] This is lay legal analysis: neither the author nor any associated organisation takes any responsibility for the accuracy of this opinion.

not lost. Latency in the network can cause additional delays to be introduced as traffic is slowed to ensure it is reliably delivered. Real-time analysis also has civil liberties and privacy implications - a proposed network level filter in Australia has drawn sharp criticism on these (and other grounds) [80].

2.6.2 Implementing Network Filters

List based filtering i.e. if a webpage appears on a list it is blocked - is typically implemented in one of two ways – a DNS black hole, or a HTTP[17] proxy.

A DNS black hole restricts access to any website that appears on a blacklist. It is cheap and technically simple to implement and has a negligible effect on performance. However it lacks granularity – it *cannot* block individual webpages, instead it can only block entire websites. For example, it could block every page of *sex.com,* but could not block a single objectionable *Facebook* profile or *YouTube* video (the whole site would be blocked). This is probably less of a problem with pornography (such content is banned from sites like Facebook and YouTube, but it may be a problem with other types of content e.g. hate speech.

A HTTP proxy fetches content from a website, strips out any objectionable content and serves the end user with a copy of the webpage but without the unwholesome content. Proxying provides fine grain control over which content is blocked – single webpages, even individual elements (text, graphics, and video) within a webpage can be blocked. Proxying requires significant computing and administrative resources.

It may therefore be considered that proxying is unsuitable for opt-out filtering on cost, complexity and performance grounds. DNS filtering, though offering less control is cheap, simple and would probably block the majority of potential harmful content. ***NB*** - both proxying and DNS blackholing require a blacklist (a list of content to be blocked) – creating and maintaining such a list is a non-trivial activity. Neither approach, and indeed no filtering method is entirely reliable – any technically proficient user would be able circumvent such controls.

2.6.3 Cultural and Social Implications

In addition to the technical challenges, cultural and social factors need to be considered, such as:

- when does 'glamour' (e.g. 'Page 3') become pornography?
- when does free speech become hate speech?
- content suitable for a 14 year old may not be suitable for an 8 year old – how should the filter be configured?

It is possible to create multiple levels of filtering but this increases the complexity for the end user, which will likely translate to increased calls to ISP helpdesks (these may be inadequately staffed for a large increase in call volume). *Who would pay for additional call centre staff, and administrative resources – end users, ISPs, tax payers?*

[17] HyperText Transfer Protocol – the protocol which powers webpages.

Companies developing content filters in the US adhere to US cultural standards which may be considered by UK standards homophobic and ‘soft’ on guns. This would probably result in increased implementation complexity, as any list would need at least some bespoke administration.

Libertarians and civil liberties groups may also object to *any* filtering of internet content, even where filtering is not mandatory i.e. users can take opt-out option.

Readers interested in DNS filtering should see OpenDNS[18], a free DNS service that provides category based list filtering.

[18] http://opendns.com

3. TABLET COMPUTING

The concept of tablet computing has been in the industry conscience for at least a decade since *Microsoft* presented prototypes at the *Comdex* computer expo in 2001 [23] (although the idea was not new). Tablets remained a largely a niche device [24] until the *Apple* launched the *iPad* in 2010.

3.1 Tablet Vs Tablet PC What is a tablet computer?

When the concept was first publicised, a tablet computer was a laptop type device which also accepted touch screen input from a stylus. The current breed of tablet devices more closely resembles an oversized smartphone – a low power, highly portable device, ideal for browsing the internet, and media consumption. For the sake of clarity this document shall refer to oversized smartphone type devices as tablets, and fully functional touch screen computers (with or without keyboard, mouse and other peripherals) as a tablet PC. Some authors feel [25] that the current success and interest in the tablet will not be shared with the tablet PC, at least in its current form.

The tablet sits between the smartphone and laptop. It typically has a feature set similar to a high-end smartphone, but with a larger screen for an improved internet and media experience. These devices generally provide a reduced feature set from that of a laptop or desktop computer in a highly portable footprint, with an almost instant-on feature. Tablet PCs (excluding specialised niche devices) have traditionally provided a laptop experience with the addition of a touch screen. Until Tablet PCs come to market featuring the latest Microsoft tablet OS, [30] it is impossible to say whether they will be used in the same way as tablets or whether they will rival (in terms of usage profile) the laptop.

The tablet market is very new, which makes it difficult to conduct any trend analysis. However, sales have been, and are projected to be strong, and there is speculation that tablet computing will be the next big thing [26].

3.2 Key Players

As with the smartphone, whilst *Apple* did not invent it, they did present it in a form that invigorated the mainstream market. *Apple* launched the *iPad* in April 2010, and recently (March 2011) the *iPad 2.* It has a very similar feature set to the *iPhone* (but with a bigger screen) and as with the *iPhone, Apple* maintains tight control over the device.

As with smartphones, *Google's Android* operating system is available for tablet devices too, and as with smartphones, *Google* provides only the OS, Original Equipment Manufacturers (OEM) build the devices. Two early devices generating a lot of interest among reviewers are *the Samsung Galaxy Tab*[19] and the *Motorola Xoom*[20].

RIM, makers of the *BlackBerry* range of smartphones, are soon to launch the *BlackBerry Playbook. RIM* is offering a native[21] development environment (for creating applications) for

[19] http://www.samsung.com/uk/galaxytab/

[20] http://www.motorola.com/staticfiles/Consumers/XOOM/index.html#/features

[21] Applications that run in a native environment are typically faster and have access to more of the devices features.

the *Playbook* that is not available for their phones [27]. This could lead to a wider range of applications with greater capabilities.

Microsoft has taken a different tack with their tablet PC approach, adapting their desktop operating system rather than their smartphone OS. This offers more power and functionality (though is heavier and will take longer to boot up), but commentators have suggested this may not fulfil customer requirements [25] [28]. As with their smartphone OS, *Microsoft* only provide the tablet PC OS and OEMs (such as *HP*) will build the devices.

Screen size is the primary differentiating feature between smartphones and tablets. Among the existing and coming tablets the form factor varies [29] between approximately 7 inches (*Galaxy Tab* and *Playbook*) and 10 inches (*iPad* and *Xoom*), whether one size comes to dominate or whether sizes continues to vary remains to be seen.

Analysis by *Forrester* [31] suggests tablet sales (in the US) will surpass netbook (NB a netbook is small low power device, similar to but not synonymous with a laptop) in 2012 and exceed desktop sales by 2015. *Gartner* [32] reported global 2010 sales of tablets at 19.5 million and project 54.8 million devices sold in 2011, rising to 208 million by 2014.

4. GEOLOCATION

Location Based Services (LBS) provide the user access to information and services based on their geographic location. For example, with LBS, a user could search for a restaurant and be shown a list of possibilities and the distances to each from their current location.

There are several ways to determine a user's location. The following are of interest to this document - GPS, Cell ID, A-GPS, and IP geolocation.

GPS and A-GPS require hardware (a GPS receiver in the device); Cell ID is a feature of mobiles networks and hence available to any mobile phone; IP geolocation is a function of the internet addressing scheme and is available to any internet based service e.g. a website.

4.1 GPS

The Global Positioning System (GPS) is a series of 31 satellites maintained by the US Air Force in medium earth orbit. Each satellite carries a very accurate (atomic) clock and maintains a precise orbit. Each satellite broadcasts a message that includes the time the signal was sent and the satellite's orbit. By analysing the signal from a satellite the receiver can determine its distances from a known location.

Using a process of trilateration[22] (the intersection of overlapping spheres representing the signals broadcast from the satellites) the receiver is able to determine its location.

Satellite signals propagate at the speed of light. This propagation must be timed to determine distance. This would require a very accurate (and very expensive) clock in the receiver. Instead the signal from a fourth satellite (with a very accurate clock only three signals are necessary) is used to provide precision. At least 6 satellites are visible at any time. The accuracy of GPS is typically better than 10 metres [22].

Russia has a similar system *GLObal NAvigation Satellite System (GLONASS)*, but this only covers Russia.

The EU is planning a system, *Galileo* (this will not be operational for some time). China is also planning a satellite navigation system.

GPS receivers are common place in high and mid range smartphones.

4.2 Cell ID

Every mobile phone base station has a unique identity, the Cell ID (CID), and is in a known location. If a device (a mobile phone) is receiving a signal from a base station it is within a certain distance of that base-station, this distance can be estimated based on signal propagation. If a device can detect multiple base stations, it is possible to determine its position by trilateration. The accuracy of CID positioning is typically 100-2000 metres.

[22] Similar to, and often confused with triangulation. Trilateration measures distances to known points, whereas triangulation measures angles to known points.

4.3 A-GPS

Assisted-GPS (A-GPS) mainly uses a combination of GPS and mobile network services to provide a faster more accurate fix, especially in urban areas. In built up urban environments, satellites may not be visible (or may be intermittently visible), and signals can be reflected on buildings, both of which reduce GPS performance and accuracy.

4.4 IP Geolocation

Internet Protocol (IP) geolocation determines a user's position based on their IP address. All internet traffic requires a source and destination IP address. The *Internet Assigned Numbers Authority* (IANA)[23] manages the global IP address space. IANA works with Regional Internet Registries - *Réseaux IP Européens Network Coordination Centre* (RIPE NCC)[24] in the case of the UK – to assigned IP address blocks to local internet registries or Internet Service Providers (ISPs). ISPs assign IP addresses to individual consumers and organisations. The accuracy of IP Geolocation is typically to the nearest town or city.

4.5 Applications

Following are some potential applications of LBS

- Finding/advertising nearby services/supplies/events.
- Tracking vehicles/deliveries/assets.
- Tracking people e.g. lone workers, prisoners, children.
- Congestion charging.
- Emergency services.
- Social - 'Are any of my friends at the shopping centre?'
- Geotagging of photos and video (adding geographic information to record where they were shot).
- Navigation.
- Providing location to emergency or recovery services.
- Location recording and tracking for social networking.

4.6 Risks

While LBS bring useful new functionality and convenience they are not without risk. The primary concerns are related to tracking and privacy; location *could* be considered personal information and it does increase the *value* of other personal information e.g. knowing a certain customer is in a particular location. The questions that needs to be asked are

- How safe/secure is location data?
- Is it shared by the service providers?
- If it is shared, is it anonymised first?
- How do 'free' LBSs sustain themselves? *(ad supported, billing events are services, selling a service with more functionality, etc)*
- Is it easy /possible to opt-out?

[23] http://iana.org

[24] http://ripe.net

Of course there is no one-size-fits-all answer to such concerns; it varies between providers, and what users are willing to accept. *A good provider*[25] *should have a clear policy and an easy to follow cancellation/opt-out process.*

The UK mobile industry has a code of practice concerning the passive[26] use of location services by location services providers [20]. It promotes informed consent, user centricity, and child protection. However, there is evidence of corporations collecting and storing location information without consent or good reason [21].

What would be the consequences of location data being compromised i.e. 'falling into the wrong hands'? There are two conceivable ways for the data to be compromised, from a provider database or direct from the device.

Unless the data can be linked to an individual it poses little risk. Providers collecting such data *should* anonymise it. If it is linked to an identifiable individual it should be encrypted (making it indecipherable in the event it is lost or stolen – this applies to all personal data). Mobile operators are legally obligated[27] to retain Cell ID (and other subscriber information) for 12 months.

What if the data is linked to an individual e.g. it has been extracted from the end device? *Google Android* indexes the last 200 base stations and 50 Wi-Fi access points the device has connected to, the *iPhone 4* stores months, potentially years worth of location data in an easy-to-read file [88]. *What could this mean?*

If an individual was able to obtain such information it would provide an historic account (*not* live real-time tracking) of where the device (and presumably its owner had been). Analysis of this data *could* (if the data includes data and time stamps) reveal patterns useful in predicting behaviour *e.g. weekdays between 08.00-08.36 the owner takes X route [to work]*.

[25] E.g. http://www.google.com/mobile/privacy.html

[26] Once activated, the phone can be located by third parties.

[27] Article 5 of the The Data Retention (EC Directive) Regulations 2009 - http://robbratby.com/2011/03/28/mobile-operators-obliged-to-retain-location-information-across-europe/

5. PERSONAL DATA

Personal data – *What is it? Why should it be kept safe?* Personal data is information that can be used to identify an individual. Examples of personal information includes:

- Full name.
- Phone number.
- Email address.
- Credit card or banking details.
- Photographs and video.
- Date of birth.
- National Insurance number.
- Full address.

Other information that does not identify a specific individual but could be combined to identify an individual include:

- School, college or place of work/employer.
- Username (if a username has been reused across indexed parts of the internet).
- Neighbourhood or town.
- Clubs or organisations the individual is a member of.

5.1 Who wants Personal Information?

Personal information is the backbone of sales and marketing, and customer management [70]. It is frequently used make purchase recommendations and promote products based on purchase history e.g. supermarket loyalty cards. It can also used and sold to third parties by providers of 'free' services to cover the cost of the service e.g. Google uses such information to tailor adverts in its free services.

There are organisations[28] that believe governments and corporations cannot be entirely trusted and that individuals should minimise the amount of personal data provided to them. This helps minimise the risk they can pose to privacy and civil liberties. There is some evidence that some educators and employers are actively data mining individuals based on data that is publicly available on the internet [33] [34]. Such information is also valuable to fraudsters attempting to clone an individual's identity (identity theft). For the purposes of identity theft the *Holy Grail* of personal information is

- Full name.
- Address.
- Date of birth.
- Bank account or other financial details.

With the first three is usually possible to obtain identity documents and open bank accounts. With the latter fraudsters are able to secure credit.

There is concern that developers of 'free' applications (particularly in social networks) have access to personal data and no obligation to use it responsibly. Users are disclosing this information without really understanding how it will be used [39] [40].

[28] E.g. Privacy International (https://www.privacyinternational.org/)

Personal details that are held with service providers (online) are often stored, on computers (sometimes in caches) and phones. People should at least be aware that usernames, passwords, bank details etc remain on computer hard disks (even after deleting), they may not be aware that such information also lasts on smartphones [41]. They need to be aware of this and practice good information hygiene when upgrading, selling or disposing of handsets.

5.2 Social Networks

Posting youthful 'indiscretions' on the internet may be one of the biggest risks facing youth. Indeed, it has been suggested that young people will in the future automatically be presented with the option of changing their name to escape from their social networking history [42].

There has been much speculation, bordering on hysteria [37], about child abusers using details gleaned from social networks to contact children. While there are instances of sexual crimes against minors taking place on social networks with offenders using personal information posted in profiles, this represents a very small fraction [38] of children using social networks.

2010 saw a significant increase in botnets targeting bank details [43], despite high profile takedowns, users must not become complacent and need to keep their systems up to date with regular patching, and exercising suspicion before opening messages and clicking on links.

Typically personal information has to be linked before it is of any use/risk – compromising photos on the internet are not a problem unless the viewer recognises individuals in the photo. If the photos are linked to other personal information, e.g. the photos are tagged (or a user leaves an opinionated comment and their email address), and the information is readily searchable. Additionally knowing a bank account number is not (usually) sufficient to fraudulently extract funds from that account – other information is necessary.

Exposure of any *one* piece of personal information is not a catastrophe, neither is posting personal information on a social network, indeed even having no SNS presence and by practising excellent security and data hygiene, an individual may still find themselves subject to identity theft. However, minimising the amount of publicly available personal data (and embarrassing information), engaging SNS privacy controls and following good practice will make an individual a 'smaller target'.

Most people are probably familiar with at least one instance of an organisation losing unencrypted data (e.g. a CD or memory stick) containing personal information [44] [45]. Encryption makes data unreadable without a key (e.g. a password). With increasing amounts of personal and private data on mobiles and smartphones, users should consider encrypting the contents of the phones (and other devices) in the event it is lost or stolen. Some smartphone encryption has been attacked by the security community for being insubstantial [46], but such products will still likely foil thieves lacking intermediate[29] IT skills.

With ever increasing amounts of important data on smartphones (and other devices), people need to consider backing up data.

5.3 Cloud Computing – A Silver Lining?

Cloud[30] computing is the concept of running traditional applications and services in the network rather than on the physical device. A good example of this is *YouTube* – videos can be stored, edited and viewed 'in the cloud'. Cloud computing has become a mainstream alternative in the enterprise and is becoming more common in consumer applications. Cloud computing applications are available for smartphones and traditional computers.

Cloud storage could help address some of the issues around personal information stored on local devices (security, integrity, backups) whether this is phone or computer based. Typically the vast majority of storage is local (on or attached to the end device). This could be set to change. A recent *Google* prototype Laptop, the *cr-48,* has no local storage or applications [47] - everything is based in the cloud. This approach is probably not suitable for individuals with large media collections (at least in the short term), but this could represent a major shift for many users. This *could* negate many of the concerns of encryption, backup and data security, but potentially at the price of greater privacy intrusion [48].

Cloud based storage brings with it advantages:

- Managed service – the user does not need to worry about security, integrity, backups, viruses, losing the device etc.

And uncertainties:

- Is the provider a viable organisation (will they go out of business)?
- Is the data encrypted?
- Can the data be easily ported between devices? (if for example the users buy a new phone).
- Does the service provide any assurances (e.g. guaranteed backup – especially free services).
- If the service is free, how does it pay for itself?
- Are bandwidth and storage limits clear?
- What happens if a user exceeds their allowance of storage or bandwidth?
- In which legal jurisdiction will the data be physically stored?

A good provider should have a clear policy, and data should be stored in standard formats to allow porting between platforms.

[29] Advanced skills are not usually necessary, once a security measure has been broken the methodology (usually the software required) are typically made publicly available - this is known as full disclosure. It also allows those with only limited skills (often called 'script kiddies') to easily bypass security. An example of this is jailbreaking the *iPhone.*

[30] Cloud computing ('in the cloud') refers to the provision of computer services via a network, the term is an abstraction (the implementation is unimportant).

6. INTERNET PROTOCOLS, STANDARDS, AND TECHNOLOGIES

The following will all have an indirect affect on the internet and mobility by influencing the design, provision and performance of features and services.

6.1 HTML 5

HyperText Markup Language (HTML) is the language used to construct webpages. A new version, version 5, is being developed and though the standard is still in draft [49], significant parts of it are already supported by browsers.

HTML5 will not be obvious to the user; it may not even be noticeable. What it does is provide web developers with more options and greater convenience, for example video can be added to webpages without the need for browser add-ons, geolocation can be implemented without additional software to directly interrogate the device, and local storage will make webpages and applications faster and persistent.

This will have little impact on the user experience but it will provide developers the freedom and flexibility to deliver new more capable services.

6.2 IPv6

Internet Protocol (IP) underlies all internet traffic, every internet capable device has an IP address, and all internet traffic needs a source and destination IP address. The current version of IP, IPv4, has run out of addresses[31] [50]. IPv6[32], the next version of the protocol, offers security features such as authentication and encryption which should help reduce some cyber attacks and provide additional privacy. However during the initial stages of the protocol rollout, users should expect to see some unreliability and even reduced security until the situation stabilises.

6.3 Net Neutrality

Net Neutrality is the principle that all public internet traffic is treated equally by service providers. The idea behind this principle is that the internet remains a free environment with an ‘even playing field’. Supporters of net neutrality fear that big organisations will be able to pay to have their traffic prioritised, indirectly (perhaps even directly) lowering the priority of a competitors traffic e.g. *Google* buys so much bandwidth, that access to *Yahoo* slows and becomes unreliable. Net neutrality sees all traffic[33] handled without prejudice if a link is oversubscribed (has more traffic than available bandwidth) and traffic is not prioritised.

Downloading or streaming media and P2P applications can exhaust available bandwidth on networks (bandwidth can be exhausted without these applications). This can be mitigated by applying Quality-of-Service (QoS) (also called traffic shaping or throttling) to networks. QoS is often used on private networks and outbound traffic to prioritise real-time

[31] The central pool has been exhausted; RIRs are expected to run out in September. ISPs and major organisations will still be able to accept new subscribers and field new equipment for sometime.

[32] the next version is known as IPv6

[33] Traffic on private parts of the internet – walled gardens and VPNs would not be subject to such restrictions.

applications such as voice, and video conferencing over web browsing and email. QoS *could* be used on the internet to prioritise time sensitive applications such as VoIP, video calling and browsing over email and file sharing.

With net neutrality, the internet may struggle to support high bandwidth and time sensitive applications. Without it, 'free' applications and smaller providers may struggle to survive.

The UK government's current position is that laws on net neutrality are at present unnecessary because of healthy competition in the service provider market [64] i.e. a user can switch provider if they are unhappy with the service. However, the global nature of the internet means the issue is larger than a single government. A substantial change in practice elsewhere (especially in the US, which hosts a significant amount of content) could affect the UK user experience. Furthermore, in Europe major telcos have asked for permission to bill content providers (e.g. *iPlayer* and *YouTube*) for data that traverses their networks in exchange for next generation network investment [66].

6.4 4G

4G refers to the fourth generation of mobile telecommunications equipment. The International Telecommunications Union (ITU) defines the standard for 4G, which among other requirements specifies a peak data transfer speed of 100Mb/s, when in motion and 1Gb/s when stationary. Some technologies such as Long Term Evolution (LTE) and WiMAX are marketed as 4G, despite failing to meet this requirement; however the ITU has decreed this *is* acceptable [60]. Here the term 4G shall have this more relaxed meaning.

4G is a secure, all IP network able to dynamically scale bandwidth on-the-fly to deliver high quality multimedia. The evolution to 4G and the technical changes it brings means wireless internet speeds could rival fixed line performance. The headline performance figures of 4G are largely meaningless, as they describe only optimum conditions. Many base stations lack the backhaul capacity (a fast enough connection to the internet) to provide the bandwidth the protocol can support [61].

4G can provide streaming media on-the-move and may see users no longer requiring fixed line internet connections (certainly lower bandwidth users).

6.5 Video on Demand (streaming)

Video on Demand (VoD) is the ability to stream[34] media from networks, typically the internet. Readers will probably be familiar with *Youtube*[35] and *BBC iPlayer*[36]*. Youtube, iPlayer,* and other VoD services are already available on smartphones. TV is the primary entertainment media for all age groups, except 15-24 year olds who use the internet as their main source of entertainment [63] with TV being regarded as a secondary activity (i.e. on 'in the background'). VoD will likely become increasingly popular on mobile devices, especially

[34] Streaming is playing content from a network source by downloading it first. YouTube is an example of streaming media.

[35] http://www.youtube.com/ (accessed 20 April 2011)

[36] http://www.bbc.co.uk/iplayer/ (accessed 20 April 2011)

as bandwidth costs continue to fall and quality improves through more powerful devices and better codecs[37]. This will see more HD capable smartphones.

6.6 eBooks

An eBook is a book published for consumption on an electronic device such as a computer, smartphone or dedicated eBook reader e.g. the *Amazon Kindle*. Dedicated eBook readers typically have a screen unlike that found in tradition digital devices which is more reminiscent of reading from paper. A single digital device can store hundreds or thousands of titles, and the ability to change the font size or use text-to- speech make these useful for the visually impaired. *Amazon* sells more eBooks than hard copies [77], this is expected to continue with eBooks becoming more popular.

7. CONCLUSIONS

What big developments in internet and mobility are on the horizon? How will these affect young people? What risks do they bring with them? Smartphones and tablets are and will be the next big thing; they provide a truly mobile computing and messaging experience. Smartphones provide features such as high speed internet connectivity, media capabilities, navigation, messaging and social networking. Tablets provide many of these same features but with a bigger screen to improve the experience. The key players in this space are Symbian (in decline), RIM, Apple, Android, and Microsoft.

The tablet can be considered largely an extension of the smartphone, devices with very similar capabilities but the tablet having a larger form factor. This allows for a larger screen which improves the media and internet experience. The key players are Apple and Android, though RIM has a device soon to launch, and others too may expand into this market. Tablet PCs may initially appear similar to tablets, however they are more properly considered laptops with touch screens – they have significantly more power and capability at the expense of portability and battery life.

The portability of these devices makes parental oversight considerably more onerous, especially with moody, boundary testing teenagers seeking privacy and independence (these are developmentally normal behaviours). The risks – sexting, cyberbullying, identity theft and fraud, exposure to harmful material, solicitation and grooming – have evolved in step with digital technology, but none of them are new threats. While technology has a part to play in mitigating these risks they are best handled with education, strong child-parent relationships and social support structures.

In addition to these social risks, the technology itself presents new risks, primarily in the form of mobile malware and botnets (networks of zombie machines). All new technology is subject to vulnerabilities, but lessons learned from the PC security model (user centricity, cryptographically signed software, privilege escalation), and heterogeneous technology (as opposed to *Windows* which dominate the desktop) serve to mitigate the likelihood and impact of such risks.

[37] Codec (coder-decoder) describes a method for converting sound and video into a digital format.

Location Based Services (LBS) provide the user access to information and services based on the device's geographic location. With more powerful applications, and GPS' ubiquity, the use of LBS is becoming more common. LBS typically concerns mobile devices though it also refers to fixed computing. *The author considers that the use of LBS will rise considerablye in in the short to midterm.* Along with convenient new services, LBS brings with it a threat to privacy from passive location and tracking. Several of the major smartphone manufacturers are currently (May 2011) embroiled in a scandal surrounding the recording and retention of location data.

For several years, issues surrounding personal data have been prominent in the public conscience. Losses of personal data by government departments and organisations are largely beyond the control of individuals. However, social networking and Web2.0 are seeing individuals posting personal information on the internet. Some of this is semi-private, but some is entirely public. The posting of personal information carries with it three key risks: identity theft and fraud; exposure of embarrassing or compromising information; and becoming the target of sexual predation. The risk of identity theft[38] from social networking data is probably less than other sources (e.g. corporate customer records database), and this may be a lesser problem for children (not being on the electoral register and with no credit history credit should be harder to obtain).

Everybody does things that at some point they later regret, especially when they are young. Most people also engage in activities (though not necessarily illegal) they would not like their parents, teachers, employer or other authority figures to know about. Evidence suggests that employers and college admissions tutors are searching social networks for information about candidates.

There has been considerable anxiety surrounding sexual predation on social networks, but there is little evidence that the risk from social networking is greater than other internet activities.

Platform convergence is a term that loosely describes a device that has the capability to perform tasks that previously required multiple devices e.g. a phone with a camera. It also describes the conflation of previously separate but similar services e.g. voice, VoIP (e.g. *Skype*), SMS, IM, email, and social network messaging, and how this perceived by the user. All the indicators suggest that such internet services and portable electronic devices will continue to converge to smartphone and tablet (type) devices which will become pervasive. Convergence will not necessarily replace individual devices, particularly in specialised applications such as DSLR cameras.

HTML 5, the new standard for web pages, IPv6, the next generation address structure of the internet, and 4G, the next generation of mobile networks will have little direct impact on the end user but their indirect impact could be considerable. They promise new features, capabilities and performance for the next generation of network services and applications.

The Net Neutrality argument revolves around the ability of service providers to prioritise traffic traversing their networks. With net neutrality, all traffic is created equally but at the

[38] Assuming the primary reason for identity theft is financial.

risk of the poor performance (slowly loading webpages, jittery streaming media, and excessive latency in voice traffic). Traffic shaping prioritises the delivery of some traffic above others; this allows Quality of Service for time sensitive applications at the risk of corporations abusing their positions in a deliberately anti-competitive manner, or as a side effect of monopolising service provider resources.

Video on demand, a technology with which many are already familiar, will continue to increase in popularity on both fixed and mobile devices. VoD also relates closely to the previous technologies. HTML 5 will help simplify web based video delivery and 4G will improve delivery to mobile devices. Net neutrality will allow traffic to arrive without being restricted (or paid for), or it may allow it be delivered promptly and smoothly.

At present the UK operates an opt-in filtering model; the internet is provided as an unfiltered pipe (by default all content is available), users have to ‘opt-in’ to content filtering. At present there are discussions about moving to an opt-out model where content considered potentially harmful is filtered out by default, to access such content a user would need to ‘opt-out’ of the filter.

Filtering is far from 100% reliable, and analysis based filtering typically degrades internet performance. A filtering technique called DNS blackholing can be used to block a considerable amount of harmful content; it is less flexible than other methods but incurs almost negligible cost and performance penalties.

8. DISCUSSION

Technology brings with it opportunity and risk, much as users need education to take advantage of these opportunities they must also be educated about the risks and shown how to protect themselves whether they are parents or children. Older children in particular need to think seriously about material posted to a social network profile or other public forum (‘would you want your parents to see it?’, ‘will it still be funny/clever next year?’). Parents need to learn about the technology and risks (and understand that there is very little that is totally new, and there is nothing magical or mysterious about the technology) in order to help protect their families. This does not need to be complex or overly technical – *Thinkuknow*[39] from *CEOP*, covers much of the important information and could be covered in an evening.

The ‘new’ risks *are* the old risks; they are a product of human behaviour in society; bullying, sexual predation, exposure to unwanted material, etc and will continue to be a feature of society, much as crime and substance use will. How these risks manifest (the implementation details) has changed with digital technology, but the underlying nature of the risks and drivers behind them have remained the same – they are independent of technology.

Parents and legislators need to consider how children behave and what is developmentally normal, not how they might like ‘model children’ to behave. For example, not revealing any personal information on social networks is considered unreasonable and widely ignored; having rules that are ignored provides no safety or security, worse it may provide a false

[39] http://thinkuknow.co.uk (access 05 May 2011)

sense of security. *The Crimes Against Children Research Center*[40] [sic] has produced an excellent guide - *Internet Safety Education for Teens: Getting It Right* [67], it gives parents evidence based facts, offers effective dialogue to better engage teens and suggests realistic and achievable safety tips. Working with children to agree reasonable rules that will be followed is far better, especially when combined with parental oversight - rule breaking and boundary testing is, on occasion to be expected.

Users need to be aware of 'free' applications on social networks (and elsewhere) that require user details, or *Facebook* groups that require you to join before you can see a funny/shocking photo. This doesn't necessarily involve entering your personal details, allowing an application access to your profile will often allow the program's author significant access to your details.

Many of the new and existing threats can be mitigated with the exercise of scepticism, privacy considerations (social networking privacy settings) and basic security hygiene – updating and patching, running anti-virus, anti-malware software, PIN protection and encryption of smartphones (much of this is even free).

When discussing filtering (or any internet safety technology) stakeholders need to be made aware this is a bit player (far from 100% reliable) and not a panacea. Internet censorship cannot be usefully compared to 'top shelf' magazines, the 9pm watershed, or BBFC or PEGI ratings (or the censorship of *any* traditional media). Each of these has significant production and distribution requirements, as such they are simple to monitor, regulate and enforce. The internet crosses multiple legal jurisdictions – there are no financial, logistical or technical barriers to entry - anyone can create and publish content.

The internet contains over 200 million websites [68] and in excess of one trillion pages of indexed content [69]. In addition, there is no reliable means for content providers to identify users or determine if they meet specific criteria (e.g. over 18), though responsible pornographers make use of landing pages with warnings about explicit content and follow a code of ethics [70].

Every minute, 10 hours of content is uploaded to *YouTube* [71]; such a volume cannot be effectively screened by people[41] and automated video analysis and classification is still very much a research, not production grade technology. If, and when inappropriate content is uploaded, it is freely accessible until a member of public reports it (at which point it is reviewed and if necessary removed). When dealing with file sharing websites and peer-to-peer (P2P) technologies, the problem is even harder as such services are frequently used to distribute illegal material [73][74].

Filtering technology is useful in protecting younger children from accidental exposure to potentially harmful material, but it is far less effective at shielding teenagers who are often actively seeking such content [75]. Strong, open relationships, parental oversight, and agreed rules and online behaviour will continue to offer a greater level of protection for the foreseeable future (probably at least the next 5 years).

[40] http://www.unh.edu/ccrc/ (accessed 11 May 2011).

[41] It would take a minimum of 1,800 people working 8 shifts without a break to manually review this content.

9. REFERENCES

[1] A. Orlowski. (2011, 11 February). It's official: Nokia bets on microsoft for smartphones • the register. [Online]. 2011(3/7/2011), Available: http://www.theregister.co.uk/2011/02/11/nokia_microsoft_smartphone_agreement/.

[2] Anonymous (2008, 18 November). Apple rescinds version change app store ban • the register. [Online]. 2011(3/7/2011), Available: http://www.theregister.co.uk/2008/11/18/apple_reinstates_castcatcher/.

[3] Anonymous Dev-team blog. [Online]. 2011(3/7/2011), Available: http://blog.iphone-dev.org/.

[4] T. Smith. (2011, 2 February). Sales show WinPho 7 off to a flying start • reghardware. [Online]. 2011(3/8/2011), Available: http://www.reghardware.com/2011/02/02/smartphone_sales_q4_2010/.

[5] T. Morgan. (2011, 8 February). Smartphones 'out sell' PCs for first time • the register. [Online]. 2011(3/8/2011), Available: http://www.theregister.co.uk/2011/02/08/idc_smartphone_pc_shipments/.

[6] J. Wilcox. (2011, 9 February). Gartner: Android smartphone sales surged 888.8% in 2010 | wireless news - betanews. [Online]. 2011(3/8/2011), Available: http://www.betanews.com/joewilcox/article/Gartner-Android-smartphone-sales-surged-8888-in-2010/1297309933.

[7] B. Ray. (2011, 28 February). Bank of America retrofits BlackBerrys with NFC • the register. [Online]. 2011(3/8/2011), Available: http://www.theregister.co.uk/2011/02/28/bank_of_america_nfc/.

[8] C. Kloet. (2011, 16 February). Samsung beam i8520: Android-powered projector phone | crave | CNET UK. [Online]. 2011(3/8/2011), Available: http://crave.cnet.co.uk/mobiles/samsung-beam-i8520-android-powered-projector-phone-49305032/.

[9] N. Mokey. (2011, 15 February). Power to the pocket: The next generation of superphones. [Online]. 2011(3/8/2011), Available: http://www.digitaltrends.com/mobile/power-to-the-pocket-the-next-generation-of-superphones/.

[10] S. Wolpin. (2011, 7 February). Sprint echo hands on preview. [Online]. 2011(3/8/2011), Available: http://www.digitaltrends.com/mobile/sprint-echo-hands-on-preview/.

[11] Anonymous Synlab: Projects. [Online]. 2011(3/8/2011), Available: http://synlab.gatech.edu/project.php?id=15.

[12] M. Ericsson. (2010, September). Future of screens – experience video | the TAT blog. [Online]. 2011(3/8/2011), Available: http://www.tat.se/blog/future-of-screens-experience-video/.

[13] Anonymous Myriad 3D multimedia platform. [Online]. 2011(3/9/2011), Available: http://www.movidius.com/myriad-3d-platform/?PHPSESSID=5c598698d234a4c92eadc3857770b235.

[14] K. Martin. (2005, 28 January). Mobile virus epidemics: Don't panic • the register. [Online]. 2011(3/9/2011), Available: http://www.theregister.co.uk/2005/01/28/mobile_phone_viruses/.

[15] J. Leyden. (2008, 30 September). Attack of the 50-foot mobile virus risk • the register. [Online]. 2011(3/9/2011), Available: http://www.theregister.co.uk/2008/09/30/mobile_malware_imminent/.

[16] I. Thomson. (2010, 07 July). Symbian malware creating mobile botnet - IT news from V3.co.uk. [Online]. 2011(3/9/2011), Available: http://www.v3.co.uk/v3-uk/news/1944989/symbian-malware-creating-mobile-botnet.

[17] K. Higgins. (2010, 5 March). Dark reading | protect the business - enable access - security news analysis - smartphone weather app builds A mobile botnet. [Online]. 2011(3/9/2011), Available: http://mobile.darkreading.com/9287/show/7e667b11d79afac90754745a08d268fe&t=8ada01a29d42cd8c3c913526c15d5004.

[18] R. Jennings. (2010, 25 January). Linux market share grows vs. windows and mac OS X shrinkage - computerworld blogs. [Online]. 2011(3/9/2011), Available: http://blogs.computerworld.com/15462/linux_market_share_grows_vs_windows_and_mac_os_x_shrinkage.

[19] A. Orlowski. (2011, 10 March). Why Nokia failed: 'wasted 2,000 man years' on UIs that didn't work • the register. [Online]. 2011(3/13/2011), Available: http://www.theregister.co.uk/2011/03/10/nokia_ui_saga/.

[20] 3, Britannic 3G Service, Child Locate, Creativity Software, Et al, "Industry Code of Practice For the use of mobile phone technology to provide passive location services in UK," version 1.1, 1 October, 2006.

[21] D. Goodin. (2011, 27 April). TomTom sorry for giving customer driving data to cops • the register. [Online]. 2011(4/30/2011), Available: http://www.theregister.co.uk/2011/04/27/tomtom_customer_data_flap/.

[22] S. Wang, J. Min and B. Yi, "Location based services for mobiles: Technologies and standards," in IEEE International Conference on Communication (ICC), Bejing, China, 2008, .

[23] G. Clark. (2010, 7 January). Ghost of gates' tablet haunts Microsoft's future • the register. [Online]. 2011(3/21/2011), Available: http://www.theregister.co.uk/2010/01/07/microsoft_tablet_pc_slate/.

[24] Anonymous Toughbook H1 medical MCA - Panasonic toughbook healthcare rugged tablet PC 2011(3/21/2011).

[25] P. Bright. (2010, August). Ballmer (and Microsoft) still doesn't get the iPad. [Online]. 2011(3/22/2011), Available: http://arstechnica.com/microsoft/news/2010/07/ballmer-and-microsoft-still-doesnt-get-the-ipad.ars.

[26] Relaxness. (2011, 6 January). Tablet sales expected to soar as new devices arrive on the market in 2011 - gadgets & tech, life & style - *The Independent*. 2011(3/22/2011).

[27] C. Metz. (2010, 27 September). RIM unveils the BlackPad BlackBerry PlayBook • the register. [Online]. 2011(3/23/2011), Available: http://www.theregister.co.uk/2010/09/27/blackberry_devcon_keynote/.

[28] D. Courbanou. (2011, 7 January). CES 2011: Microsoft windows 7 and the tablet challenge | the VAR guy. [Online]. 2011(3/23/2011), Available: http://www.thevarguy.com/2011/01/07/ces-2011-microsoft-windows-7-and-the-tablet-challenge/.

[29] C. Kloet. Motorola xoom | reviews | CNET UK. [Online]. 2011(3/23/2011), Available: http://reviews.cnet.co.uk/ipad-and-tablets/motorola-xoom-review-50002121/.

[30] K. Fiveash. (2010, 14 December). Microsoft boss to wave tablets in CES faces – again • the register. [Online]. 2011(3/23/2011), Available: http://www.theregister.co.uk/2010/12/14/microsoft_ces_steve_ballmer_again_with_the_tablet/.

[31] E. Schonfeld. (2010, 17 June). Forrester projects tablets will outsell netbooks by 2012, desktops by 2013. [Online]. 2011(3/24/2011), Available: http://techcrunch.com/2010/06/17/forrester-tablets-outsell-netbooks/.

[32] B. Brown. (2010, 15 October). Gartner: Nearly 20 million tablets to be sold in 2010. [Online]. 2011(3/24/2011), Available: http://www.networkworld.com/news/2010/101510-gartner-tablets-ipad.html.

[33] G. Fish. BusinessWeek debate room employers, get outta my Facebook. [Online]. 2009(10/02/2009), pp. 1. Available: http://www.businessweek.com/debateroom/archives/2008/03/employers_get_o.html

[34] R. Bennett. (25 March, 2008). Plea to ban employers trawling Facebook - times online. [Online]. 2009(10/02/2009), pp. 1. Available: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3613896.ece.

[35] M. L. Ybarra and K. J. Mitchell. (2008, Feb). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics 121(2),* pp. e350-7.

[36] J. Wolak, D. Finkelhor, K. Mitchell and M. Ybarra, "Online "Predators" and Their Victims Myths, Realities and Implications for Prevention and Treatment," *American Psychologist,* vol. 63, pp. 111-128, March 2008. 2008.

[37] d. boyd. (2009, 6 February). Apophenia: Doing the math on MySpace and registered sex offenders. [Online]. *2009(11/08/2009),* pp. 1. Available: http://www.zephoria.org/thoughts/archives/2009/02/06/doing_the_math.html

[38] K. J. Mitchell, D. Finkelhor, L. M. Jones and J. Wolak. (2010, Aug). Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization J. Adolesc. Health 47(2), pp. 183-190.

[39] J. Leyden. (2011, 18 January). Facebook suspends personal data-sharing feature • the register. [Online]. 2011(3/29/2011), Available: http://www.theregister.co.uk/2011/01/18/facebook_suspends_data_sharing_feature/.

[40] D. Goodin. (2010, 30 June). Facebook apps must now seek permission for user data • the register. [Online]. 2011(3/29/2011), Available: http://www.theregister.co.uk/2010/06/30/facebook_privacy/.

[41] J. Leyden. (2011, 22 March). Sensitive data easily swiped from eBayed mobiles • the register. [Online]. 2011(3/30/2011), Available: http://www.theregister.co.uk/2011/03/22/sensitive_data_ebayed_mobiles/.

[42] J. Deans. (2010, Wed, 18 Aug). Google chief warns on social networking dangers. Technology: Eric Schmidt | Guardian.Co.Uk [Online]. Available: http://www.guardian.co.uk/technology/eric-schmidt.

[43] D. Goodin. (2011, 16 February). Botnets claim 7-fold increase in victims • the register. [Online]. 2011(3/31/2011), Available: http://www.theregister.co.uk/2011/02/16/botnet_increases/.

[44] G. Cluley. (2008, 16 September). Lost memory stick contained confidential patient records | naked security. [Online]. 2011(4/1/2011), Available: http://nakedsecurity.sophos.com/2008/09/16/lost-memory-stick-contained-confidential-patient-records/.

[45] D. Raywood. (2010, 21 September). Unencrypted NHS USB stick lost which contained details of patients' conditions and medication - SC magazine UK. [Online]. 2011(4/1/2011), Available: http://www.scmagazineuk.com/unencrypted-nhs-usb-stick-lost-which-contained-details-of-patients-conditions-and-medication/article/179248/.

[46] C. Foresman. (2011, Early). Security expert: IPhone password hack shows flawed security model. [Online]. 2011(4/2/2011), Available: http://arstechnica.com/apple/news/2011/02/six-minute-keychain-hack-highlights-busted-iphone-security-model.ars.

[47] I. Thomson. (2010, 13 December). Google's cr-48 chrome laptop first look - V3.co.uk labs - a blog from V3.co.uk. [Online]. 2011(4/4/2011), Available: http://www.v3.co.uk//v3-uk/v3-co-uk-labs-blog/2019377/googles-cr-48-chrome-laptop-look.

[48] A. Orlowski. (2011, 4 April). Baby googles: The answer to the chocolate factory dominance? • the register. [Online]. 2011(4/4/2011), Available: http://www.theregister.co.uk/2011/04/04/baby_googles/.

[49] I. Hickson. (2011, 13 January). HTML5. [Online]. 2011(4/4/2011), Available: http://www.w3.org/TR/html5/.

[50] K. Murphy. (2011, 1 February). IPv4 addresses to run out thursday | DomainIncite - domain name news & opinion. [Online]. 2011(4/5/2011), Available: http://domainincite.com/ipv4-addresses-to-run-out-thursday/.

[51] Internet Safety Technical Taskforce. (2008, 31 December 2008). Enhancing child safety and online technologies. The Berkman Center for Internet and Society, Harvard University. [Online]. Available: http://cyber.law.harvard.edu/pubrelease/isttf/

[52] M. Ybarra and K. Mitchell, "Online aggressor/target, aggressorsand targets: a comparison of associated youth characteristics," Journal of Child Psychology and Psychiatry, vol. 45, pp. 1308-1316, 2004.

[53] M. Campbell. (2005, Cyber bullying: An old problem in a new guise? Australian Journal of Guidance and Counselling [Online]. 15(1), pp. 68-76. Available: http://www.atypon-link.com/AAP/doi/abs/10.1375/ajgc.15.1.68.

[54] J. Patchin and S. Hinduja, "Bullies Move Beyond the Schoolyard - A Preliminary Look at Cyberbullying," Youth Violence and Juvenile Justice, vol. 4, pp. 148-169, April, 2006.

[55] J. Ozimek. (2011, 3 February). IWF chief steps down • the register. [Online]. 2011(4/7/2011), Available: http://www.theregister.co.uk/2011/02/03/iwf_chief_steps_down/.

[56] N. D. Connick-Smith. (2008, Pedophilia - the cultural history of pedophilia, the serial pedophile of the 1990s - encyclopedia of children and childhood in history and society. [Online]. 2011(4/7/2011), Available: http://www.faqs.org/childhood/Pa-Re/Pedophilia.html.

[57] K. Lanning, "Child molesters: A behavioral analysis," National Centre for Missing & Exploited Children, Tech. Rep. Fourth Edition, September 2001, 2001.

[58] Deloitte. (2008, November). Safer internet - completed projects - filtering & rating - SIP-BENCH - synthesis report 2008 edition. EU. [Online]. Available: http://ec.europa.eu/information_society/activities/sip/projects/completed/filtering_content_labelling/filtering/sip_bench/index_en.htm

[59] Australian Communications and Media Authority (ACMA), "Closed environment testing of ISP−Level internet content filters - report to the minister for broadband, communications and the digital economy," ACMA, Canberra, Australia, June. 2008.

[60] B. Ray. (2010, 22 December). WiMAX and LTE grab 4G moniker • the register. [Online]. 2011(4/15/2011), Available: http://www.theregister.co.uk/2010/12/22/4g_itu/.

[61] M. Fitch, "Wireless Lab Presentation," 2008.

[62] G. Brown and B. Leis. (2010, How are youth rewriting the future of messaging? | mobileYouth®. [http://www.mobileyouth.org/post/how-are-youth-rewriting-the-future-of-messaging/]. 2011(4/20/2011, Available: Online.

[63] J. Hemmingsen. (2011, April). Trends in TV and video on demand :: MediaCom. [Online]. 2011(4/20/2011), Available: http://www.mediacom.com/en/news--insights/blink/issues/edition-2-2011/trends-in-tv-and-video-on-demand.aspx.

[64] C. Williams. (2010, 17 November). UK.gov ignores 'net neutrality' campaigners • the register. [Online]. 2011(4/21/2011), Available: http://www.theregister.co.uk/2010/11/17/vaizey_net_neut_no/.

[65] V. Jobling. Anonymity: The default identity for cyber-bullies on social networks - online conference on networks and communities. Presented at Online Conference on Networks and Communities. [Online]. Available: http://networkconference.netstudies.org/2011/04/anonymity-the-default-identity-for-cyber-bullies-on-social-networks/

[66] A. Parker, "Europe telecom groups target Google," 26 April, 2011. [Online]. Available : http://www.ft.com/cms/s/0/867742dc-7036-11e0-bea7-00144feabdc0.html

[67] Crimes Against Children Research Center, "Internet Safety Education for Teens: Getting It Right," pp. 1-4, 05 May, 2008. [Online[] Available: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Internet%20Safety%20Education.pdf

[68] [Versign]. (2010, 23 December). The total number of web domain names. [Online]. 2011(3/15/2011), Available: http://www.labnol.org/internet/total-web-domain-names/18395/.

[69] Anonymous (2008, 25 July). Official google blog: We knew the web was big... [Online]. 2011(3/15/2011), Available: http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html.

[70] T. Martin, C. Durbin, M. Pawlewski and D. Parish. (2010), Future vision of identity. *IJLSE* [Online]. *3(1/2),* pp. 86-98. Available: http://www.inderscience.com/search/index.php?action=record&rec_id=31825&prevQuery=&ps=10&m=or

[71] ASACP: Association of Sites Advocating Child Protection. Industry best practices. [Online]. *2010(22/07/2010),* pp. 1. Available: http://www.asacp.org/index.php?content=best_practices&PHPSESSID=a41065591cb64fea95c37d9cfdab0757.

[72] J. Ozimek. (2008, 20 October). UK.gov says: Regulate the internet • the register. [Online]. *2010(11/02/2010),* Available: http://www.theregister.co.uk/2008/10/20/government_internet_regulation/

[73] K. Fiveash. (2009, 24 June). Rapidshare stung with €24m fine • the register. [Online]. 2011(5/11/2011), Available: http://www.theregister.co.uk/2009/06/24/rapidshare_gema/.

[74] J. Libbemga. (2010, 19 July). Pirate bay owners fined by dutch court • the register. [Online]. 2011(5/11/2011), Available: http://www.theregister.co.uk/2010/07/19/pirate_bay_fine/.

[75] Ofcom. (2010, 26 March). UK children's media literacy: Annex Ofcom. [Online]. Available: http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/medlitpub/medlitpubrss/ukchildrensml/.

[76] C. Cox. (2011, 13 May). Samsung shows screen that folds seamlessly • reghardware. [Online]. 2011(5/23/2011), Available: http://www.reghardware.com/2011/05/13/scientists_develop_foldable_phone_displays/.

[77] L. Campbell. (2011, 28 January). Kindle sales outstrip paperbacks as amazon has first $10bn quarter | the bookseller. [Online]. 2011(5/31/2011), Available: http://www.thebookseller.com/news/kindle-sales-outstrip-paperbacks-amazon-has-first-10bn-quarter.html.

[78] Near Field Communications World. (2011, 30 May). List of NFC phones. [Online]. 2011(5/31/2011), Available: http://www.nearfieldcommunicationsworld.com/nfc-phones-list/#available.

[79] Near Field Communications World. (2011, 1 June). List of NFC trials, pilots, tests and commercial deployments. [Online]. 2011(5/31/2011), Available: http://www.nearfieldcommunicationsworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/.

[80] Australian Library and Information Association, Civil Liberties Australia, A. Byrne, GetUp!, Liberty Victoria, National Association for the Visual Arts, National Children's & Youth Law Centre, NSW Council for Civil Liberties, QLD Council for Civil Liberties and Save the Children, "Joint Statement on Internet Censorship," pp. 1, July, 2009. Available: http://www.cla.asn.au/0805/index.php/articles/2009/active-anti-censorship-campaign-starts

[81] L. Johnson, R. Smith, H. Willis, A. Levine and K. Haywood. (2011, The 2011 horizon report. [Online]. 2011(6/2/2011), pp. 33. Available: http://www.educause.edu/Resources/2011HorizonReport/223122.

[82] E. Blass. (2010, 03 December). LG eying dual-screen smartphones. [Online]. 2011(6/2/2011), Available: http://pocketnow.com/tech-news/lg-eying-dual-screen-smartphones.

[83] J. Wolak, D. Finkelhor, K. Mitchell and M. Ybarra, "Online "Predators" and Their Victims Myths, Realities and Implications for Prevention and Treatment," American Psychologist, vol. 63, pp. 111-128, March 2008. 2008.

[84] Internet Safety Technical Taskforce. (2008, 31 December 2008). Enhancing child safety and online technologies. The Berkman Center for Internet and Society, Harvard University. [Online]. Available: http://cyber.law.harvard.edu/pubrelease/isttf

[85] S. Jones. (2009, 4 February). MySpace: 90,000 sex offenders removed from site | technology | guardian.co.uk. [Online]. 2009(07/08/2009), Available: http://www.guardian.co.uk/technology/2009/feb/04/myspace-social-networking-sex-offenders

[86] d. boyd. (2009, 6 February). Apophenia: Doing the math on MySpace and registered sex offenders. [Online]. 2009(11/08/2009), pp. 1. Available: http://www.zephoria.org/thoughts/archives/2009/02/06/doing_the_math.html

[87] M. L. Ybarra and K. J. Mitchell. (2008, Feb). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. Pediatrics 121(2), pp. 350-7.

[88] D. Goodin. (2011, 27 April). Windows phones send user location to microsoft • the register. [Online]. 2011(6/8/2011), Available: http://www.theregister.co.uk/2011/04/27/windows_phone_location_tracking/.