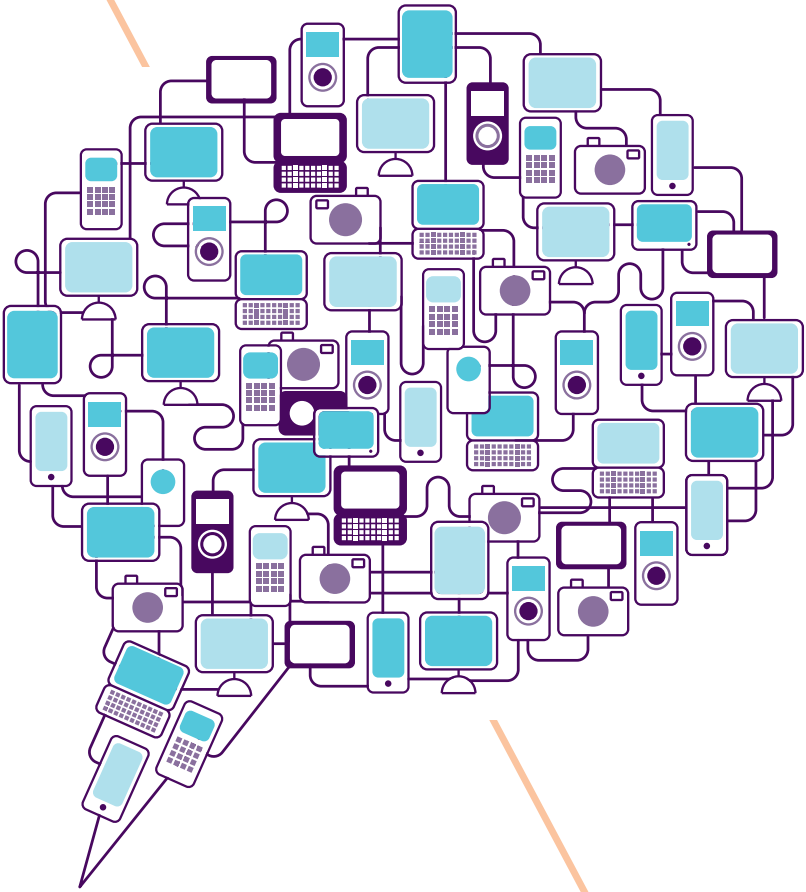
IPPR



METIS

The journal of IPPR@universities,
the student thinktank network
IPPR@universities

Edited by Nathan Tanswell

Volume 4, 2013 / © IPPR

CONNECTIVITY

CONTENTS

ABOUT IPPR

IPPR, the Institute for Public Policy Research, is the UK's leading progressive thinktank. We are an independent charitable organisation with more than 40 staff members, paid interns and visiting fellows. Our main office is in London, with IPPR North, IPPR's dedicated thinktank for the North of England, operating out of offices in Newcastle and Manchester.

The purpose of our work is to assist all those who want to create a society where every citizen lives a decent and fulfilled life, in reciprocal relationships with the people they care about. We believe that a society of this sort cannot be legislated for or guaranteed by the state. And it certainly won't be achieved by markets alone. It requires people to act together and take responsibility for themselves and each other.

IPPR
4th Floor
14 Buckingham Street
London WC2N 6DF
Registered charity no. 800065

T: +44 (0)20 7470 6100
E: info@ippr.org
www.ippr.org

ABOUT IPPR@UNIVERSITIES

IPPR@universities involves the formation of partnerships between IPPR and student-led thinktank societies. The aim of the initiative is to extend our networks and draw students into the policymaking domain.

For the students participating in the IPPR@universities programme, we believe it offers an opportunity for them to enhance their understanding of policymaking and politics, to see their thinking reach a wider audience, and to build their enthusiasm and skills in policymaking, potentially equipping them for a future career in the area.

For more, visit http://www.ippr.org/universities

IPPR@universities

FOREWORD

Nathan Tanswell
Executive Editor

Since its commencement in 2010, the IPPR@universities programme has gone from strength to strength, year on year. The programme offers students of the universities of Sheffield, Warwick and York the opportunity to engage in real-world policymaking decisions, with the chance for their work to appear in *Metis*, a national journal, and undertake ever-valuable work experience at the IPPR and IPPR North offices. The skills of writing, researching, editing and collaborating that students gain from this process – not to mention the detailed and in-depth feedback writers receive on their articles from researchers at IPPR itself – are highly valuable in today's challenging climate.

This year the focus of *Metis* is connectivity, an ever-important issue in an age of continuing globalisation. Unsurprisingly, the majority of articles focus on the internet, the fastest-growing and most versatile method of digital communication. Articles have tackled the topic from various angles, drawing upon the disciplines of economics, geography, law, politics and philosophy. The articles fall roughly into two distinct camps: the internet and economic development, and internet freedom versus censorship. While Elettra Ardissino analyses the prospects of the internet and economic development in Sub-Saharan Africa, Finlay Green takes a slightly different focus by examining internet usage as a tool to tackle social exclusion in the UK. On the theme of internet freedom vis-à-vis legislation and censorship, Samuel Matthews takes a broad look at the debate between internet freedom and internet censorship, arriving at some very interesting conclusions. Ben Fischer, meanwhile, evaluates the case for universal internet access as a worldwide right upheld by an international enforcement body, and Calum Young looks at the legal acceptability of problematic social media activity – a highly controversial issue that comes up in the news media almost daily. Both Emily Owen and Gary Fawdrey discuss the cases for and against censorship in the context of pro-anorexia websites and online pornography respectively. Finally, Michael Shneerson examines what happens to personal information held online upon death, investigating LinkedIn profiles, Facebook memorial pages, and beyond. These eight articles together provide a broad look at the controversies and contentions that plague the digital age of connectivity.

The considerable range and depth of these eight fantastic articles understandably took some effort and intelligence to write, as well as organise, edit and collate. None of this would have been possible

without the affiliated university societies, namely *Canvas* at the University of Sheffield Students' Union, the Warwick Think Tank Society at the University of Warwick Students' Union and the York Student Think Tank at the University of York Students' Union. All involved in this considerable effort – writers, editors and researchers – deserve many congratulations for the result. Thanks is also due to those IPPR staff who took up valuable time to provide feedback: Bhrmie Balaram, Matt Cavanagh, Richard Darlington, Tessa Evans, Tim Finch, Glenn Gottfried, Jenny Pennington, Damian Tambini and Nigel Warner; particular thanks go to Tim and Glenn for the other work they did to make this journal possible. Thanks also to the IPPR liaisons at the respective universities – Eleanor Corcoran at Sheffield, Ben Frew at Warwick and Gary Fawdrey at York – and, of course, to the sub-editors: Katerine Bruce, Nick Gore and Sara Mhaidli of the University of Sheffield, and Ben Frew and Josh Funnell of the University of Warwick.

UNIVERSAL INTERNET ACCESS

THE ARGUMENT FOR A NEW INTERNATIONAL BODY TO PROMOTE AND ENFORCE IT

Ben Fischer
University of Sheffield

Although still in its primary stages of development, the internet has become an incredibly powerful and useful tool for people from all walks of life. Frank La Rue, the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, argues that the internet has become a 'catalyst' for the right to freedom of expression, as well as an enabler of several other economic and cultural rights (UN 2011: 7). This article will go further, arguing that internet access is not only valuable because it is instrumental to other rights, but that it represents an inherently valuable right in itself. This article will set out a new policy proposal in light of the recent failed talks in Dubai at the World Conference on International Telecommunications (WCIT) (L.S. 2012). It will aim to direct the current, negative international discourse towards a more positive one. At the moment, this agenda is focused on how to regulate the internet, but the international community should instead focus on providing greater access to it. However, this article will also define and provide a solution to the problem of 'necessary regulation'. The onus of this regulation should be placed on a new international governing body rather than on individual governments.

The internet as an inherently valuable right

The internet is unique in its ability to empower. In a world where it can dominate every aspect of our lives, to arbitrarily decide who gets to benefit from this empowerment (and who does not) is fundamentally wrong. It is vital that the international community recognises this, and acknowledges the practical importance of universal internet access. As Damian Tambini (2000) notes, true universality of internet leads to clear advances in the economy, innovation, education, science, technology… the list is endless.

Based on the immeasurable number of opportunities the internet presents, to actively deny someone access to it is almost equivalent to a direct abuse of any other right. 'Almost' is used purposefully here, because the worth of internet access is clearly secondary to all other human rights. If someone's use of the internet violates any other human right, the protection of that human right must take precedence over the protection of the offender's right to internet access.

The ineffectiveness of individual government regulation

Almost 80 per cent of people across the world believe internet access to be a 'fundamental right' (BBC News 2010). Yet in recent years, governments, corporations, internet service providers (ISPs)

and other organisations have clashed over who has the right to regulate the internet. Some private companies justify regulation as a copyright issue, while some governments justify it as a legal or moral issue. There has been a lot of confusion recently over who can regulate, and how. For example, some British MPs believe there should be an 'automatic block' of internet pornography (BBC News 2012). The original draft of the Digital Economy act 2010 also called for the blocking of websites which broke copyright laws (BBC News 2011). However this provision was dropped, as was the proposal. Both initiatives failed to properly understand the complex structures of the internet, and therefore the ineffectiveness of regulation. As Aviel Rubin (2003: 5) explains, 'there is an arms race between censorship and censorship circumvention, because if you tell me what you are using to censor I can tell you what to do to get around it'.

Any act of censorship by a single body is practically useless. The global interconnectivity of the internet means that no body or group of bodies can effectively regulate it. Furthermore, just 36 per cent of internet users across the world believe that their governments should regulate internet use more than they currently do (WIP 2012: 67). Government regulation in its current form is unpopular, ineffective and a complete waste of resources.

Some believe that the UN's International Telecommunication Union (ITU) should also work on issues related to the internet. However, this article strongly opposes the ITU's assertion in the International Telecommunication Regulations (ITR) that it is the 'sovereign right of each country to regulate its telecommunications' (ITR 1989: 3). Some may argue that it is surely up to the people of any one nation to decide what they can and cannot access. However, this position is essentially arguing that the people of a nation have the right to arbitrarily disempower and silence others. This is fundamentally wrong – the right to internet access cannot simply be disregarded on the basis of simple sovereignty. In any case, as previously argued, regulation and censorship by individual governments can always be circumvented, making it largely ineffective at any rate. Both the practical and moral shortcomings of individual state regulation of the internet necessitate an alternative.

So how can we regulate?

Despite the arguments presented above, there are nevertheless certain cases in which regulation is necessary. These cases, such as child pornography, involve the abuse of other human rights, as La Rue (UN 2011: 19–20) notes. However, unlike the special rapporteur, this article believes that states should not have the right to regulate this. This presents a policy problem: states (or any other organisation, company or body) should not have the right to regulate citizens' access to the internet, on both moral and practical grounds; yet some regulation must be warranted if we are to protect other inalienable human rights.

It is imperative, therefore, that governments transfer their right of internet regulation to a single, universal body. This global body should be able to order all states to regulate certain areas, if necessary. Through global action, the regulation of content which poses a direct threat to human rights would be effectively enforced. It would also ensure that all states cooperate in granting full, unregulated internet access to their citizens, so long as no other human rights are thereby directly violated. Only through such an international body can states truly tackle the problems of the internet. A brief look into one of these problems – the construction of China's Golden Shield project (GSP) – will further demonstrate why only international action will work. The GSP is one of many methods of surveillance that China uses to control internet access. Its technological purpose is to monitor, filter and censor content on the internet (August 2007). This eight-year-long built scheme was actually created from the hardware supplied by Cisco and other US companies (ibid). Therefore, collaborative atrocities such as this must and can only be stopped by the international efforts of a universal body.

What steps should be taken to create and fund this body?
This global body must have coercive power in order to be effective. Punitive powers must be granted to ensure that states such as China may face hefty fines and sanctions. It would seem practical to place this universal governing power in the hands of a UN organisation, given the structural resources already at their disposal. As previously mentioned, some may point to the ITU as an existing body that should deal with the internet. However, the ITU is acting on an outdated (with regards to the internet) treaty written in 1988 (the ITR) – the internet and its global presence have undergone dramatic changes since then. As Terry Kramer, US ambassador to the WCIT, argues, the ITR's focus 'should be on the telecom sector, not the internet sector' (Olson 2012). In order to avoid further failures on negotiating conditions of internet access, as in the recent WCIT talks (L.S. 2012), we must avoid the mistake of confusing telecommunications governance with internet governance. We therefore need a new, separate body within the UN with a specific focus on internet governance to ensure that states comply in granting full access to their citizens, or limiting access where human rights are at threat of being violated.

Of course there remains the question of how this apparently large project will be funded. However, given the absurd amounts of spending currently devoted to internet regulation at the national level, this should not be a problem. For example, China's GSP alone cost US$700 million (August 2007) and is still an ineffective regulator. At most, all governments would have to do is reallocate the funds they currently devote to internet regulation to this new body – assuming that they have a genuine desire to regulate effectively. The ITU's revenue forecast from 2012 to 2015 is 632 million Swiss francs (approximately US$680 million) (ITU News 2010: 45). With a similar

budget, the new specialised body should have no problems in operating: this is a generous figure, given that the ITU focuses on many mediums whereas this new body would focus only on the internet. This singular focus naturally leads to a more efficient and less costly use of resources.

So how will internet access be improved?
La Rue (UN 2011: 1) acknowledges the multidimensional nature of 'internet access', specifically:

1. free, unfiltered access to content, and
2. access to the technical infrastructure needed for internet use.

Using these criteria, the policy proposal presented in this article tackles the issue of internet access via a two-pronged approach. The aforementioned policy of establishing a specialised, authoritative UN body is aimed specifically at point 1, and should successfully ensure universal access. With regards to point 2, the ITU could still play a role in issues related to the internet. As the ITR states, nations 'shall promote the implementation of international telecommunication services and shall endeavour to make such services generally available to the public in their national networks' (1989: 7). As argued above, the ITU should not confuse internet and telecommunication governance. However, the technological infrastructure that the internet requires (the laying down of fibre optic cables, for example) could easily fit within the existing governance framework for telecommunication services. The ITU's future relationship with the internet should not be a coercive one in which it attempts to manage its content, but one in which it helps to provide and develop the internet's structural necessities. For instance, the ITU could play a cooperative role in facilitating development for those nations which currently lack the infrastructure required for the internet.

In such a scenario, some may express concern about the possibility that states could wilfully destroy their infrastructures in order to regulate the internet by preventing structural access almost entirely. Considering that the ITU will lack the coercive power of the new internet-focused UN body, this may seem a troubling possibility. However, these concerns can easily be put to rest by considering the fact that the future of everything in this world will, within a few decades, lie almost solely in the internet. Any government that willingly destroys its infrastructures will be destroying its own future. Furthermore, while the ITU lacks specific coercive powers, it can be argued that coercion already exists in the sense that maintaining a high-quality internet infrastructure is a necessity for the future progression of a nation's technological, social and economic endeavours.

Conclusion
A new specialised body within the UN, focused entirely on the internet, must be set up. It must have a reasonable amount of authoritative power to ensure universal internet access and the

protection of human rights. While some may question whether states would allow such a body to be set up in the first place, if regulation is what they want then this is the most effective means of achieving it, free from circumvention. As Damian Tambini (2000) notes, true universality of internet access leads to clear advances in the economy, innovation, education, science, technology – the list is endless. This is something that surely all legitimate governments would wish for their citizens. Furthermore, the ITU should only focus on the internet in so far as it cooperates with states to build the necessary infrastructure. Tackling both dimensions of access to the internet would enable us to live in a world of true universal connectivity, where people can flourish through a free, open internet, while also being protected from any potential threats arising from its use.

August O (2007) 'The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online', *Wired* 15(11), November 2007

BBC News (2010) 'Internet Access is "a fundamental right"', BBC News Online, 8 March 2010. http://news.bbc.co.uk/1/hi/8548190.stm

BBC News (2011) 'Government drops website blocking', BBC News Online, 3 August 2011. http://www.bbc.co.uk/news/technology-14372698

BBC News (2012) 'Internet Porn: Automatic Block Rejected', BBC News Online, 15 December 2012. http://www.bbc.co.uk/news/uk-politics-20738746

International Telecommunication Regulations [ITR] (1989) 'Final Acts of the World Administrative Telegraph and Telephone Conference', Melbourne: International Telecommunication Union. http://www.itu.int/dms_pub/itu-t/oth/3F/01/T3F010000010001PDFE.pdf

ITU News (2010) 'Financial Plan for the years 2012–2015', November 2010. http://www.itu.int/dms_pub/itu-s/oth/02/01/S020100003A4E05PDFE.pdf

L.S. (2012) 'Internet Regulation: A Digital Cold War?', *Economist* Babbage blog, 14 December 2012. http://www.economist.com/blogs/babbage/2012/12/internet-regulation

Olson P (2012) 'Future Of The Internet May Rest On Definitions At Dubai Conference', *Forbes* website, 6 December 2012. http://www.forbes.com/sites/parmyolson/2012/12/06/future-of-the-internet-may-rest-on-definitions-at-dubai-conference/

Rubin A (2003) 'Statement of Aviel Rubin', in 'China's Cyber-Wall: Can Technology Break Through?: roundtable before the congressional-executive commission on China', Washington, D C: Government Printing Office. http://www.gpo.gov/fdsys/pkg/CHRG-107hhrg83512/pdf/CHRG-107hhrg83512.pdf

Tambini D (2000) *Universal Internet Access: A Realistic View*, London: IPPR and Swindon: Citizens Online. http://eprints.lse.ac.uk/22528/1/Universal_Internet_Access_in.pdf

United Nations [UN] (2011) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', New York, NY: United Nations General Assembly, Human Rights Council, 17th session. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

World Internet Project [WIP] (2012) 'World Internet Project: International Report, 4th Edition'. http://www.worldinternetproject.net/_files/_Published/_oldis/770_2012wip_report4th_ed.pdf

‘PRO-ANA’ SITES

LIMITING FREEDOM IS THE PRICE WE HAVE TO PAY TO PROTECT VULNERABLE PEOPLE

Emily Owen
University of Sheffield

Pro-anorexia websites: Definitions and dangers

Many websites concerned with anorexia offer advice, helplines and practical support. However, recently there has also been a significant rise in the number of pro-anorexia websites, which are growing at a faster rate than any other form of harmful online content, with a 470 per cent increase, from under 300 to nearly 1,600, between 2006 and 2008 (Optenet 2008). Pro-anorexia websites adopt an anti-recovery approach to eating disorders (Tierney 2006), often promoting anorexia as a lifestyle choice. This approach involves encouraging individuals to not seek help, while encouraging a continuation of unhealthy eating behaviours (Csipke and Horne 2007). The majority of these sites are set up by sufferers, who often fully disclose their unhealthy behaviours for other sufferers to read about. They also often include ‘thinspiration’ (images of underweight people portrayed positively) and tips on how to avoid food, lose weight and, perhaps most worryingly, conceal the illness from others (Norris et al 2006). Viewing pro-anorexia websites does not cause anorexia, but the sites feed into negative aspects of the illness, and can cause an instant increase in preoccupation with weight control and lower self-esteem amongst non-sufferers too (Bardone-Cone and Cass 2007).

The difference between support sites and pro-anorexia websites is that the latter tend to focus on negative self-image, accepting the illness and continuing to engage in disordered behaviours and distorted body-image. Some pro-anorexia sites do recognise the seriousness of anorexia, with many offering disclaimers and warnings that only actual sufferers of anorexia should enter the site. However, it is to these vulnerable sufferers that such websites do the most damage.

The dangers of pro-anorexia websites do not arise purely from the content itself, but the way in which this content plays on the more harmful aspects of sufferers’ personalities. Those with eating disorders often feel isolated, lack self-esteem, and have a desire for control. Pro-anorexia sites allow sufferers to feel part of a community, and for many this can be seen as a positive. However, belonging to this community also involves increased pressure to continue the dangerous behaviours that are normalised within it (such as severely limiting calorie intake) in order to continue to belong (Bond 2012). Within these communities, being drastically underweight is seen as a sign of success, and one which others encourage (ibid). Pro-anorexia sites also play on the competitive natures of many sufferers, who encourage competition by sharing

stories, tips, and images of themselves (often when they are extremely undernourished).

What has already been done?

It is important to consider the current position on monitoring dangerous websites. The UK Council for Child Internet Safety (UKCCIS) was set up in 2008, and aims to promote safe regulation of the internet by the industry, and extend education to increase safety on the internet for children (UKCCIS 2012). While this is a positive step, the UKCCIS does not focus on eating disorder sites specifically, nor does its remit include the protection of adults who may be mentally unwell and who may consequently use such sites. Similarly, the Department for Sports, Media and Culture has a more general focus on the self-regulation of the industry. This means that currently there is little direct government policy with regards to content. Some internet service providers (ISPs), namely BT, have moved towards greater monitoring of the internet, though not in regards to pro-anorexia websites. The Cleanfeed system established by BT in 2004 uses blacklists from the Internet Watch Foundation (IWF) to block illegal sites that contain child pornography (BBC 2006). However, this is only one ISP, and the Cleanfeed system and the IWF focus only on child pornography.

Social media such as Tumblr and Facebook have in recent years increased the shutting down of pro-anorexia websites, with Tumblr blocking results for search terms such as 'pro-ana'. However, again, the success of these campaigns has been limited. Many pro-anorexia sites are hosted by free homepage providers; yet all of these websites disregard at least one term of the homepage providers' user requirements (Norris et al 2006). Clearly, either the providers and social media websites aren't doing enough, or websites are not being monitored effectively by ISPs. The continuing existence and accessibility of these dangerous websites shows that the current self-regulation policy is not enough. It may be difficult for the UK government to police webpage providers, ensuring both that their user terms are explicit and that they are adhered to by users, as many are not based in the UK. ISP monitoring of pro-anorexia websites, however, could be more easily controlled.

The issue of freedom

Suggesting government intervention into what people can and cannot access online can lead to uncomfortable questions about the balance between freedom and protection. Many argue that increased government intervention on the internet would limit freedom of expression. This is unavoidably true – any policy that restricts internet content narrows what individuals can publish online. Nevertheless, in certain cases this is necessary in order to protect the vulnerable. It is worth considering that anorexia is a severe mental illness which often affects sufferers' capacities to make logical decisions. Indeed, the restriction of content to protect vulnerable individuals is already happening through initiatives such

as the Cleanfeed system. While the issues are different, the IWF could use similar methods to monitor pro-anorexia websites too.

Recommendations

This article argues that there is a serious case for increasing restrictions on the viewing and maintenance of pro-ana sites. As previously suggested, policing the creation of these websites under UK law may be difficult, as many website providers are international. Therefore, a change in government policy should instead put pressure on national ISPs, with explicit reference to pro-anorexia websites. This could be done through the creation of a law that made ISPs legally obliged to implement a monitoring system that explicitly blocks harmful pro-anorexia content. ISPs would therefore be responsible for financing and implementing such a system, or be in violation of the law. In some ways this would be similar to a law proposed in the European Parliament in 2009, which would make ISPs legally responsible for monitoring and blocking child pornography sites under national law (Williams 2009). A law forcing ISPs to implement a system similar to Cleanfeed for pro anorexia websites would perhaps also be a cheaper and more viable option for government and would be, to an extent, in-keeping with the current policy of self-regulation, while giving greater incentives for providers to block access to harmful websites.

Such a move would make pro-anorexia sites effectively illegal. However, the responsibility – and therefore the punishment – would lie with ISPs rather than the creators of the websites. This is an important distinction, compared to a 2008 French bill which sought to make pro-anorexia websites illegal but punish the creators of the websites with up to two years in prison or a large fine (Lichfield 2008). This bill failed to be passed by the senate; however, a law such as the one suggested in this article is more moderate, with responsibility lying with ISPs rather than vulnerable anorexia sufferers. Most likely the creator of a pro-ana site will be a vulnerable individual him- or herself, struggling with an eating disorder. To criminalise people in this way could have a profoundly detrimental effect by forcing sufferers underground. Instead, this article's proposed change in policy would in effect impose a ban on harmful pro-anorexia content, but without threatening the creators of that content with criminal consequences.

The last thing a change in policy should do is inadvertently close down areas of genuine support for anorexia sufferers. A balance would have to be struck so as not to limit the creation of websites that are genuinely helpful. A policy directed towards only the harmful aspects of pro-anorexia content would leave room for websites that offer the support of pro-ana sites without the unhelpful parts. It would be vital to draw up strict guidelines for what distinguishes a pro-anorexia website from websites of support. The Department of Health could work in partnership with both the IWF and mental health charities to draw up a list of criteria which, if met, would be

enough to block a site on a legal basis. The criteria could include factors such as inciting others to harm themselves, and could therefore also cover other dangerous sites, such as pro-suicide sites. Funding for this collaboration could come from a variety of sources – donations to the charities, the Department of Health's budget and funding from the European Union, which already funds the IWF.

Another aspect of the new law could be that when a page that someone is trying to view is blocked by the ISP system for harmful pro-anorexia content, they are redirected to a reputable pro-recovery information website for eating disorders.

Of course, there may be difficulties in the implementation of these polices. The nature of the internet means that it can be difficult to monitor, and harmful websites can often be recreated elsewhere if they are closed down, making them difficult to track (Economist 2012). However, while internet governance may be difficult to coordinate, that doesn't mean that policies such as those suggested are in any way unachievable or pointless. Pro-anorexia websites are an important and harmful feature of the internet that must be addressed, and any steps that the UK takes towards implementing such policies would be hugely beneficial to broader efforts to tackle these websites. If ISPs played their role in blocking pro-anorexia websites, they would become much more inaccessible in the UK. Indeed, the UK, as one of the most developed internet markets in the world, could even prompt other countries to follow suit. The foundations are there – France has already attempted to pass a law making pro anorexia websites illegal, and there has already been discussion within the EU about enabling national governments to pass laws to force ISPs to implement a monitoring system (with regards to child pornography). The role of the UK government could be to drive this policy within Europe, setting the precedent as the first country to target ISPs as part of efforts to block access to pro-anorexia sites.

Conclusion

The self-monitoring nature of current internet censorship is not sufficient to effectively tackle the issue of damaging pro-anorexia sites. This article has outlined the reasons why it is so important to limit access to such sites, and has suggested that a law forcing ISPs to implement a monitoring system to block harmful pro-anorexia content could reduce public access to them. It is necessary to stress the importance of striking a balance when considering any controversial policies related to freedom of expression and access to information, especially when it could have a large effect on vulnerable people. For many, the internet is a form of support and therefore it would be important to only target websites that are deemed particularly detrimental. There are many more sites that promote recovery and offer genuine, helpful advice in aid of sufferers attempting to battle the illness, and it is vital that these continue to be promoted in order to ensure that there are plenty of alternatives

to pro-anorexia sites. Undoubtedly, the fight to minimise the harmful content of these websites is part of a much wider battle, with the global nature of the internet making it difficult for any one country to effectively govern it. Nevertheless, a British government policy ensuring that ISPs monitor and block such websites could have a huge positive impact – Britain should lead the way internationally in tackling these damaging websites.

Bardone-Cone A M and Cass K M (2007) 'What does viewing a pro-anorexia website do? An experimental examination of website exposure and moderating effects', *International Journal of Eating Disorders* 40(6): 537–548

BBC (2006) 'BT sounds child web porn warning', BBC News website, 07 February 2006. http://news.bbc.co.uk/1/hi/uk/4687904.stm

Bond E (2012) 'Virtually anorexic – Where's the harm? A research study on the risks of pro-anorexia websites', Ipswich: University Campus Suffolk. http://www.ucs.ac.uk/SchoolsAndNetwork/UCSSchools/SchoolofAppliedSocialSciences/Virtually%20Anorexic.pdf

Csipke E and Horne O (2007) 'Pro-eating disorder websites: users' opinions', *European Eating Disorders Review* 15(3): 196–206

Economist (2012) 'Thin Cases – many find pro-anorexia sites repellent, but banning them is futile', *Economist* website, 01 December 2012. http://www.economist.com/news/international/21567339-many-find-pro-anorexia-websites-repellent-banning-them-futile-thin-cases

Edmonds W (2012) 'Pinterest, Tumblr Policies to Combat Pro-Anorexia Messages Applauded by Eating Disorder Expert Dr. Gregory Jantz of Caring Online', Marketwire website, 03 August 2012. http://www.marketwire.com/press-release/pinterest-tumblr-policies-combat-pro-anorexia-messages-applauded-eating-disorder-expert-1687023.htm

Giles D (2006) 'Constructing identities in cyberspace: The case of eating disorders', *British Journal of Social Psychology* 45: 463–477

Lichfield J (2008) 'France bans websites promoting anorexia "cult"', *Independent* website, 16 April 2008. http://www.independent.co.uk/news/world/europe/france-bans-websites-promoting-anorexia-cult-809617.html

Norris M, Boydell K, Pinhas L and Katzman D (2006) 'Ana and the Internet: A Review of Pro-Anorexia Websites', *International Journal of Eating Disorders* 39 (6): 443–447

Optenet (2008) '2008 International Internet Trends Study', Miami and Madrid. http://www.optenet.com/mailing/pdfs/TrendReport.pdf

Tierney S (2006) 'The dangers and draw of online communication: Pro-anorexia websites and their implications for users, practitioners, and researchers', *Eating Disorders* 14(3): 181–190

UK Council for Child Internet Safety [UKCCIS] (2012) 'FAQs about the UK council for Child Internet Safety', Department for Education website, 26 April 2012. http://www.education.gov.uk/a0076345/faqs-about-the-uk-council-for-child-internet-safety#faq14

Williams C (2009) 'UK gov to get power to force ISPs to block child porn', *Register* website, 02 April 2009. http://www.theregister.co.uk/2009/04/02/eu_filtering_framework/

HOW DO YOU LIKE ME NOW?

CHANGING THE SOCIAL ACCEPTABILITY OF LEGALLY PROBLEMATIC SOCIAL MEDIA ACTIVITY

Calum Young
University of Sheffield

The context

A number of different laws have been enacted, in both criminal law and areas of civil law such as defamation law, to protect various interests surrounding the right to privacy and breaches of confidence. Breaches of these laws result in clear and obvious harms to groups and particularly individuals. These laws have served their purpose for a lengthy period of time, but the enforcement of them is starting to face a number of problems caused mainly by developments in the internet in recent years, and specifically in the area of social media.

The internet allows the dissemination of information through social media at an extremely swift pace. It can be rapidly spread by a large number of users, regardless of whether the content is defamatory, private, or subject to a court order. One need only read the news on any particular day to see frequent examples of this phenomenon. The spread of an accusation against the Conservative peer Lord McAlpine is just one example of the problem: the accusation was severely defamatory and spread rapidly, seemingly without full consideration of the potential legal difficulties involved. This resulted in Lord McAlpine bringing a number of defamation cases against television channels and noted individuals such as Sally Bercow, the wife of the speaker of the House of Commons.

One of the potential reasons behind these ill-informed and in some cases intentional breaches of the law is the general culture surrounding social media. Social media activity now has the informality of a normal day-to-day conversation, as opposed to its true legal significance as a publication analogous to a newspaper or magazine. Many users give little consideration to individuals' privacy or reputation. Furthermore, social media users can find themselves in breach of the law without realising it, as they may not fully understand the significance of court orders, or, on the other hand, they may have a desire to wantonly flout them. This general ignorance of the relationship between social media and the law is the cause of a large number of the problems. The sheer volume of posts also renders many of the relevant laws borderline-unenforceable, leading to more widespread violations of the law.

The solution

In order to solve this problem, what is required is not only a change in the law, but a shift in the image and culture of social media. When users begin to consider postings on social media as potentially actionable publications, the number of potentially problematic posts

could be reduced as they would then be seen as both potentially illegal and socially unacceptable. Changes in the law can frequently be used to alter the social acceptability of certain acts. One example is the way in which drink-driving laws have made drink-driving less acceptable. This example can be applied to the social media situation not by altering the classification of acts, but rather by altering the punishments and damages incurred.

Individuals on social media have profiles of differing significance. This significance can, for example, be measured by the number of followers an individual has on Twitter, or the number of likes a Facebook page receives. A defamatory action undertaken by an individual or account with 'high significance' is much more likely to be seen by a large number of people, and the defamatory content therefore likely to be more widely distributed. The actions of these individuals are also paid greater attention, and consequently carry greater weight. It is the prominence of these individuals that can be used to change the culture surrounding social media.

Currently, neither criminal nor civil law properly reflects the significance of these greater social media presences with regards to punishments enshrined in law. This factor is not taken into account when deciding upon the extent of civil damages, nor is it considered in the Crown Prosecution Service (CPS's) decisions on who to prosecute for breaches of the law through social media. My key contention is that the higher an individual's social media presence, the greater the potential negative consequences should be, as the harms that stem from any breach of the law are greater.

Enshrining this principle in law would mean that certain individuals would face greater damages for civil cases and a higher risk of prosecution for breaches of the criminal law. This could be implemented in both civil and criminal law, and could be applied on a broad scale: individuals with a moderately high social media profile could face a moderately high punishment, and those who play a very significant role in the social media sphere could potentially incur a much higher punishment. There should be a much greater likelihood of prosecution for someone who makes a criminal publication to a large number of Twitter followers, as opposed to merely a few. A potential example of this in practice comes again from the Lord McAlpine situation, in which his legal team sought higher levels of damages from higher profile individuals, such as Sally Bercow, relative to individual, non-famous Twitter users. An example of the other end of the scale, where a criminal offence would be less likely to be prosecuted, would be Facebook posts only seen by a small number of users.

The implementation of this solution should cause few issues. It can be achieved by altering the practice directions given to judges to accord greater weight to the social media aspect of the case when awarding damages, and, on a criminal level, by altering CPS prosecution guidelines to better reflect the role of higher profile

social media users. CPS guidelines have already been somewhat altered to better reflect the realities of social media, but this could easily be taken further in this way.

Consequences

How would this change the culture surrounding social media, and solve the present problems? The activities of social media users with higher profiles are naturally widely discussed by social media users generally. The actions of these individuals are often relayed by other users, which drastically increase their profile and reach. A high-profile social media user receiving a high-profile and stringent punishment for any breach of defamation or criminal law would obviously provoke discussion on the social media network concerned, both about why the material was in breach of the law and how this could potentially be avoided in the future.

A good example of how this sort of culture shift might function in practice was some of the action taken following the Lord McAlpine incident. Shortly after it emerged that the accusations being spread on Twitter were defamatory, a number of prominent figures on Twitter, including journalists and newspaper columnists, made efforts to right the wrong they felt they had committed in a number of different ways. Most relevant to the current discussion is the apology issued by newspaper columnist George Monbiot. Having learned of the falseness of the accusations, his related postings were swiftly removed, and both a retraction and a lengthy apology were issued. The fact that this was so high-profile meant that it was widely discussed, and the defamatory nature of the accusations was also debated. Subsequently, there was a great deal of conversation about why the apology had been issued, – about how comments on social media interacted with the laws of the land, and about the fact that the things being said could potentially result in a legal case.

Were this to be replicated more frequently with figures of equally high social media profiles, by focusing legal cases and consequences on these sorts of prominent individuals, it is not difficult to imagine this effect being similarly replicated amongst social media users. This would lead to greater discussion of the relevant legal issues, with these questions gaining further exposure and prompting yet further discussion. An increase in legal awareness amongst some social media users, caused by the type of the high-profile prosecution suggested, would mean that this information would be further spread by these users, and raise awareness more generally.

Were the suggested measures to be implemented, this discussion, debate, and dissemination of the relevant information about the relationship between the law and social media such as Facebook and Twitter would lead to the necessary culture shift. Seeing other Twitter and Facebook users being sued or prosecuted for their social media actions, and knowing more about potential legal issues,

would make users consider the legality of social media posts more generally. Whenever a prosecution or court action takes place over something posted on a social media website, the legality of the issue is inevitably discussed in the mainstream media, and these articles are subsequently relayed around the social media websites. People receive information on the legality of social media postings written by mainstream media writers in a form that is designed to be easily read and understood.

As explained by the previous drink-driving example, people's reluctance to be seen to be breaking the law can have an effect upon social perceptions. When drink-driving was made illegal, it became less socially acceptable to drink and drive due to it being against the law. The same effect can be imagined with regards to social media postings: the more people know that posts in breach of confidential court orders are illegal, and inflict lasting harm on individuals, the less socially acceptable these posts will be become, as people will not want to be seen to be breaking the law. The prosecution of a high-profile social media user would greatly increase the circulation of knowledge, both through discussion of this prosecution and through other social media users subsequently spreading this knowledge.

The likelihood of prosecution should remain the same for the individual low-profile user, but users should have the information and opportunity to consider their posts more carefully, in full knowledge of the potential legal consequences of their actions. The proposed solution would help to bring this about, as the higher the profile a social media user has, the more publicised the legal action would be. The more people are aware of such legal actions, the more people will consider whether their own actions are in breach of the law. The instinct to avoid breaches of the law, combined with greater awareness of the law, would mean that the number of illegal and potentially harmful social media postings would be reduced.

Crown Prosecution Service [CPS] (2012) 'Interim guidelines on prosecuting cases involving communications sent by social media', London. http://www.cps.gov.uk/consultations/social_media_consultation.pdf

Furness H (2012) 'Lord McAlpine: Guardian will not pay George Monbiot's legal costs', *Telegraph* website, November 16 2012. http://www.telegraph.co.uk/news/uknews/crime/9683457/Lord-McAlpine-Guardian-will-not-pay-George-Monbiots-legal-costs.html

Halliday J (2012) 'Sally Bercow faces Lord McAlpine High Court Battle', *Guardian* website, December 13 2012. http://www.guardian.co.uk/media/2012/dec/13/sally-bercow-lord-mcalpine

HM Government (1998) 'Human Rights Act 1998'. http://www.legislation.gov.uk/ukpga/1998/42/contents

Monbiot G (2012) 'Lord McAlpine – An Abject Apology', November 10 2012. http://www.monbiot.com/2012/11/10/lord-mcalpine-an-abject-apology/.

Scanlon L (2012) 'Twitter and the law: 10 legal risks', *Guardian*, 10 August 2012. http://www.guardian.co.uk/law/2012/aug/10/twitter-legal-risks

Sherwin A (2013) 'Twitter libel: Sally Bercow says she has "learned the hard way" as she settles with Tory peer Lord McAlpine over libellous tweet', *Independent* website, 24 May 2013. http://www.independent.co.uk/news/uk/crime/twitter-libel-sally-bercow-says-she-has-learned-the-hard-way-as-she-settles-with-tory-peer-lord-mcalpine-over-libellous-tweet-8630653.html

Taylor A (2012) 'Why A British Politician Is Planning To Sue "At Least" 10,000 Twitter Users', Business Insider website, November 09 2012. http://www.businessinsider.com/lord-mcalpine-sues-10000-twitter-users-2012-11#ixzz2LGH5afnX

CONNECTING PEOPLE

CHALLENGES AND SOLUTIONS FOR INCREASING INTERNET ACCESS IN SUB-SAHARAN AFRICA

Elettra Ardissino
University of Warwick

Introduction: Why does internet access matter?

The spread of the internet has revolutionised the ease, speed and convenience with which individuals, groups, businesses and governments can exchange information. The positive impact of internet access on economic growth is especially marked in developing countries. A report by the World Bank (2009) found that a 10-per-cent increase in broadband penetration produced additional GDP growth of 1.38 points in low-income countries, compared to 1.21 points in high- and middle-income countries (World Bank 2009). In addition to growth, internet access has the potential to promote efficiency in government transactions with individuals, and greater transparency in its own activities. The *Global Information Technology Report 2012* found that 'a 10-point increase in digitisation [defined by criteria such as the ubiquity, affordability and reliability of internet connections] increases a government's Transparency Index by around 1.2 points' (Dutta and Bilbao-Osorio 2012).

Therefore, increasing the convenience of internet access should be a policy priority as a means of fostering economic growth and social progress in developing regions of the world. Unfortunately, sub-Saharan Africa is currently prevented from reaping the rewards of a digital economy. In a world where internet penetration averages 34.3 per cent (the US and Europe's figures are 78.6 and 63.2 per cent respectively), Africa is significantly below average at 15.6 per cent (Dutta and Bilbao-Osorio 2012). The key reasons for this trend are the absence of a cheap and effective medium of connectivity; a widespread lack of awareness of opportunities for this; and unawareness of the internet's existence entirely.

This article suggests that one way to increase internet penetration in sub-Saharan Africa would be to encourage demand for mobile phones via a mixture of market and government-based solutions.

Cheaper phones: Challenges and solutions

The most traditional medium worldwide for connecting to the internet is the desktop computer. However, this trend is in reversal due to the advent of other platforms of access such as the tablet and the smartphone. In the fourth quarter of 2012, and for the first time in 10 years, worldwide PC shipments declined, by 4.9 per cent (Gartner 2013). Although possible explanations for this range from the weak global economic environment to increased durability of PCs which delays repeat purchases, another significant factor

in this decline is the explosive growth in the sales of smartphones, which can perform standard phone features with the addition of internet connectivity. Add to this their mobility, and it's clear that mobile phones are comparatively more convenient, versatile and flexible than desktop and even laptop computers.

The transition from desktop to mobile browsing is being driven forward by developing countries, especially in Africa. The 2012 Twinpine report on mobile technology in West Africa shows that in Nigeria and Ghana mobile-internet subscriptions are now almost equal to fixed-internet subscriptions. However, the report also notes that 'total internet usage is still below the half-total population mark in both countries' (Twinpine and iHub Research 2012).

Smartphones are a good means of increasing internet access in Africa. The challenge currently is that they are a luxury good, even by Western standards. Studies in Latin America, for example, show that US$10 per person per month is the threshold beyond which ICT expenditure becomes a luxury as opposed to a necessity (Hilbert 2010). The current price of an iPhone 3GS, one of the earliest models, clocks in at US$99; just this would itself cover 85 per cent of the so called 'magical number' of affordability. Yet iPhone-type mobile phones are also delicate and have a short battery-life, as well as many optional features that make it difficult to learn how to operate it.

An alternative is the creation of an inexpensive smartphone with the basic functionalities of texting, calling and connecting to the internet. Nokia has introduced the 2220 phone, which costs US$20, but the model does not support internet connection. The challenge lies in providing an easy-to-use and cheap mobile phone with internet connectivity. This idea provides a dual reward, by not only making a significant difference to internet penetration, but also providing an incentive for firms to act as quickly and efficiently as possible to boost their bottom lines. Three key factors provide an incentive for this venture:

- Firstly, given the huge potential demand for mobile telephony in African countries, the first firm to penetrate the market will be the 'brand of reference', establishing a strong brand image and putting competitors at a disadvantage. The strategy of 'going in early' is especially important because of the following two broader trends in the demography of the African continent.
- In 2012, the Middle East and Africa region has the world's youngest population, with the under-thirties making up a staggering 66.8 per cent of the population. By 2020, the proportion will drop only slightly to 63.9 per cent (Euromonitor 2012). Since under-thirties are the biggest market for technological products, firms can expect future demand to be concentrated in the African market.
- Africa's middle class is emerging at a significantly slower rate than in other developing regions of the world. However, the

proportion of the population in the 'floating class', defined as those straddling the poverty line on expenditures of US$4 a day, are growing much more rapidly, from 14.1 per cent in 2000 to 20.8 per cent in 2010 (AfDB 2011). Expanding internet penetration is likely to be one of the deciding 'push' factors that will stabilize the 'floaters' on a middle-class consumption and income level. As the levels of both rise, demand for differentiated higher-end mobile phones is also likely to rise, which would boost company profit margins. By initially providing cheap mobile phones with limited profit potential, firms are arguably creating a long-term future profit base as the Western market becomes increasingly saturated.

Increasing demand: Challenges and solutions

Boosting demand for internet services through phones would increase internet penetration in two ways. Most obviously, more people will use the internet, and they will use it more often. Furthermore, an increase in the potential market for internet services encourages firms to enter this market, which is likely to increase competition between providers and hence provide lower prices and improved services to the population.

Government can increase household internet usage by digitising its services and transactions. This has the twofold effect of increasing demand for internet services and making the information transfer process more efficient and less costly. For instance, the government could encourage citizens to pay taxes online through a system of mobile-phone money transfer. Currently, African governments collect less tax revenue as a percentage of GDP than their counterparts in other regions. This is partly due to high tax evasion and limited administrative efficiency (Gardner 2012). Enabling citizens to pay taxes online is an effective solution to this problem, since it requires less effort on the part of the citizen (for example, in the form of reduced waiting times and mitigated travel expenses) and also allows the government to monitor tax evaders and eliminate the practice of 'pocketing' by intermediaries. A solution of this kind is currently in the process of being implemented in Kenya, where from June 2013 taxpayers will be able to fill in tax return forms online (Wangui 2013). Of course, adopting these measures relies on there being sufficient security infrastructure to protect users' data from hacking, which may be a significant impediment.

Another way in which demand for mobile phones could be boosted is by extending the facility of mobile financial transactions between individuals, following the Kenyan M-PESA model. Currently, M-PESA allows money transfers between individuals without bank accounts, and cash withdrawals in specific locations. The service is useful because, in the regions where it operates, few individuals have a bank account, and the fact that withdrawal points are distant from rural areas often excludes rural communities from accessing direct money transfer facilities. The M-PESA service is now being used

by 18.9 million people in Kenya alone (CCK 2012). The advantages of mobile-phone money transfer is that it reduces the scope for corruption, since it makes financial transactions easier to track; it reduces the cost and risk of remittances; and it fosters financial inclusion, especially of the poorest segment of the population (Agrawal 2010).

The problem, of course, is that M-PESA is operated by the private telecommunications company Safaricom, and therefore charges a profit. As a solution, governments should set up their own national systems of mobile-phone money transfers, free of transaction charges and therefore within the financial reach of the entire population. Not only would this have the positive effect of reducing the cost of government inefficiency and corruption, but it would also increase economic dynamism and opportunities for the whole population. It would also encourage people to invest in a mobile phone which, as is illustrated above, would in turn encourage people to use the internet.

Conclusion

This report suggests that the problem of low internet penetration in sub-Saharan Africa can be overcome by stimulating demand for mobile phones at the market level through lower prices, and at the government level by making mobile phones a necessity rather than just a luxury. The focus on increasing mobile phone usage in order to increase internet connectivity has an intrinsic, as well as instrumental, value. As we have seen, using mobile-phone money to pay taxes and receive payments reduces the cost of corruption to governments and widens access to financial services, as well as increasing internet penetration. This mixed strategy strengthens the value of the internet by empowering households and creating better business conditions; it should therefore be the preferred policy.

African Development Bank [AfDB] (2011) *The Middle of the Pyramid: Dynamics of the Middle Class in Africa*, Tunis. http://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/The%20Middle%20of%20the%20Pyramid_The%20Middle%20of%20the%20Pyramid.pdf

Agrawal M (2010) 'Socioeconomic Benefits of Mobile Money Transfer', *Telecom Circle*, 27 January 2010. http://www.telecomcircle.com/2010/01/benefits-of-mobile-money-transfer/.

Communications Commission of Kenya [CCK] (2012) *Quarterly Sector Statistics Report*, Nairobi. http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q2_2011-12.pdf

Dutta S and Bilbao-Osorio B (eds) (2012) *The Global Information Technology Report 2012*, Geneva: World Economic Forum and INSEAD. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

Euromonitor (2012) *Special Report: The World's Youngest Populations*, Euromonitor International blog, 13 February 2012. http://blog.euromonitor.com/2012/02/special-report-the-worlds-youngest-populations-.html

Gartner (2011) 'Gartner Says Sales of Mobile Devices Grew 5.6% in Third Quarter of 2011; Smartphone Sales Increased 42 Percent', press release, Gartner Inc., 15 November 2011. http://www.gartner.com/newsroom/id/1848514

Gardner L (2012) 'History matters in assessing Africa's tax collection system', Africa at LSE blog, 19 November 2012. http://blogs.lse.ac.uk/africaatlse/2012/11/19/history-matters-in-assessing-african-tax-systems/.

Gartner (2013) 'Gartner Says Declining Worldwide PC Shipments in Fourth Quarter of 2012 Signal Structural Shift of PC Market', press release, Gartner Inc., 14 January 2013. http://www.gartner.com/newsroom/id/2301715

Hilbert M (2010) 'When is Cheap, Cheap Enough to Bridge the Digital Divide? Modeling Income Related Structural Challenges of Technology Diffusion in Latin America?', *World Development* 38(5): 756–770. http://www.sciencedirect.com/science/article/pii/S0305750X09002174

Twinpine and iHub Research (2012) *An analysis of Mobile Technology in West Africa: The Case Of Nigeria, Ghana and Cote D'Ivoire*, Lagos: Twinpine and iHub Research. http://twinpinenetwork.com/publications/1351001605_819_249.pdf

Wangui J (2013) 'Taxpayers to pay taxes online', *MyNews24* website, 26 February 2013. http://m.news24.com/kenya/MyNews24/Taxpayers-to-pay-taxes-online-20130226

World Bank (2009) *Information and Communication for Development: Extending Reach and Increasing Impact*, Washington D C: World Bank. http://issuu.com/world.bank.publications/docs/9780821376058

REGULATION AND PROTECTION

COMBATING THE DANGERS OF VIOLENT INTERNET PORNOGRAPHY

Gary Fawdrey
University of York

The internet has spread pornography on an unprecedented scale: 25 per cent of all internet searches are of a pornographic nature, up to 20 per cent of all websites are pornographic, and the average age of a child's first exposure to online pornography is 11 (McVeigh 2013a). On top of this, due to the abundance of online pornography there is a growing trend towards ever more extreme and violent images. According to Halla Gunnarsdottir – political adviser to the Icelandic interior minister Ogmundur Jonasson, who recently motioned for the banning of violent pornography in Iceland – 'when a 12-year-old types "porn" into Google, he or she is not going to find photos of naked women out on a country field, but very hard-core and brutal violence' (Associated Press 2013). It is important to note that the effects of violent pornography are contested: for example, in 2009 Montreal University claimed that although 'most boys seek out pornographic material by the age of 10 ... they quickly discard what they don't like and find offensive' (Desjardins 2009). This could well be true but, as 'brutal and hard-core imagery is now the standard' (McVeigh 2013b), young people are increasingly likely to think that these things are normal, even if they initially dismiss them. According to the National Society for the Prevention of Cruelty to Children (NSPCC), feedback from recent focus groups with young people suggests that hardcore pornography is now perceived to be so common as to be 'mundane' (NSPCC 2013). Not only does such material expose children to things that simply aren't suitable for their age, but it is shaping their perceptions and understandings of sex, and what is normal and expected, in unhealthy ways. According to a government consultation carried out in 2012, 'pornography is the issue that parents are most likely to say they want help with to protect their children online' (DfE 2012: 8). This article will outline some policies that could potentially solve this problem. These are:

- greater regulation of violent pornography
- legally enforcing a clear option of parental controls in the set-up of all internet-enabled devices
- the development and expansion of children's sex education.

These policies would go a long way towards reducing the currently excessive power that pornography has to shape young people's perceptions of sex and normal sexual practices.

Greater regulation

The main argument used against the regulation of pornography is that the state has no right to interfere with what consenting adults wish to do in private. This is, of course, true to some extent. However, regulating pornography does not actually constitute interference with what consenting adults do in private. Under this article's proposals, consenting adults would still be able to legally participate in violent sexual activities – they just wouldn't be able to publish images of themselves committing these acts, or to view images of others doing so which are made with the primary aim of arousal. Greater regulation of pornography is thus not an attempt to stop people doing what they want; rather, it is attempting to stop the spread of images that could influence those who view them in harmful ways. Some people have certain so-called 'kinks' when it comes to sex, and these people would still be perfectly able to pursue these with other consenting adults. By removing the ability to spread violent pornographic images, you are not stopping these people from enjoying themselves: you are stopping young, impressionable minds from seeing them, and having their views of what is normal shaped by that. The banning of these images would make it clear to those who wish to enjoy violent sex acts that they can do so with others who wish to, but they cannot expect to act like that with everyone. Currently, if the first example of sex a young person sees is violent, they can think that this is normal, and therefore expect all sexual relationships to be like this. For example, 31 per cent of girls aged 13–16 reported having experienced sexual violence in a recent NSPCC research study (Barter et al 2009: 65). Furthermore, Sue Berelowitz, deputy children's commissioner, believes that teenage boys can struggle to understand the concept of consent, resulting in greatly increased expectations of sex (Hope 2013). The fact that females aged between 16 and 19 are now at the greatest risk of domestic violence, followed by those aged 20–24 (Laville 2011), appears to support this, and suggests that we are already seeing the worrying results of the first generation raised on online, increasingly violent pornography.

Those who claim that pornography is made between consenting adults and is meant to be viewed by consenting adults, and that therefore the state has no right to intervene in it, often don't realise the state already does so in the UK. It is actually illegal to view 'extreme pornography', even if it does show consenting adults, following the implementation of the Criminal Justice and Immigration Act 2008 (MoJ 2009). Extreme pornography is obviously a rather vague term, but according to the act it is an image the primary purpose of which is pornographic, and which is 'grossly offensive, disgusting, or otherwise of an obscene character' – this includes acts that appear to threaten a person's life, acts which are likely to cause serious physical harm to a person's anus, breasts or genitals, and acts involving corpses and animals (MoJ 2009: 2). It is stated within the act that it 'should only catch material which

is already illegal to publish and distribute in England and Wales under the Obscene Publications Act 1959', but that was being legally accessed due to the international nature of the internet (ibid). Despite initially negative press coverage, this act is now largely successful and accepted. There is thus already a precedent in this country for the regulation of adult pornography by the government.

The other commonly voiced concern in response to calls for pornography regulation is that it would also include numerous films and pieces of art which, although they depict unsavoury things, do so for an artistic purpose. These concerns were voiced in the run-up to the passage of the 2008 act. They were, however, unfounded, as the act clearly states that it 'defines a pornographic image as one which must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal' (MoJ 2009: 3). It also goes on to state that 'the intention of Section 64 is to give certainty to members of the public that they will not be at risk of prosecution if they possess a video recording of a film which has been classified by the British Board of Film Classification' (ibid: 4). Therefore, if this law were to be expanded to include not just life-threatening but violent acts, there is no way that this would infringe on the arts or outlaw existing artistic creations. Thus, this article has countered the arguments against the expansion of the 2008 act to include all violent pornography, and not just that which shows apparently life-threatening acts.

Parental controls

The setting up of blocks and filters on a family computer is a widely accepted and encouraged action. However, according to Claire Lilley of the NSPCC, 'the average child now has access to five devices so we are beyond the stage of a parental lock on the family PC' (McVeigh 2013b). After a consultation in 2012, the government urged internet service providers to 'actively encourage' parents to set up parental controls, saying that they want 'to see all internet enabled devices supplied with the tools to keep children safe as a standard feature'(DfE 2012: 11). Despite the conclusions of this report, enforcement has remained very limited – for example, Apple, an industry leader in computers, tablets and smartphones, has publicly refused to make any changes to its products' set-ups, ignoring the government's calls (Chapman 2013). This essay therefore proposes cementing the suggestions of the government consultation into law, making it compulsory for every internet-enabled product sold in the UK to have the option of parental controls included in its set-up, and for information regarding these controls to be supplied at the time of purchase in order to inform the less technologically informed parents of the steps required. Enforcing the use of parental controls would most likely be untenable and unpopular, but ensuring that the option is made available to parents in an obvious way is certainly viable, and would appease a lot of the concerns highlighted by parents in the consultation.

Sex education

The final piece of legislation suggested by this article is one to develop and improve sexual education. A large proportion of people's first sexual experiences come from pornography, and this can lead to misconceptions about what is and isn't normal, with pornography taking the place of sex education (Baker 2013). Psychosexual therapist Karen Lobb-Rossini believes an increasing number of young people are learning about sex through porn, and that this is having a devastating effect on how they view their own bodies (Hsu 2013). If the internet becomes young people's main access to sexual information, then their viewpoint of what is normal can become incredibly warped. This can result in men suffering 'performance anxiety' and women feeling 'pressured to perform' (ibid). This article therefore suggests the expansion of sex education classes delivered in secondary schools, starting from year 7. Research by the children's commissioner found that in one local authority area 100 per cent of year 9 boys, and 50 per cent of year 9 girls, had accessed pornography (Hope 2013). When this is considered alongside the increasingly violent nature of pornography discussed above, it is clear that schools need to pre-empt this online sexual education, to ensure that the extreme things viewed on the internet do not affect children's perceptions of what is normal and thus their future relationships.

To conclude, this article has outlined the problem posed by the growing amount of violent pornography that is readily accessible online – that as it is being regularly viewed by children, it is having dangerous effects on these children's perceptions of what is normal and expected within a consenting sexual relationship. It has also outlined three strategies that would help to alleviate the current problem. Ultimately the government does have the right to regulate what images are viewed for sexual arousal within its borders, and it already exercises this right – yet the amount of violent pornography is increasing, and the number of children viewing pornography is unacceptable. If these three things are considered together it is clear that the policies outlined in this article should be implemented.

Associated Press (2013) 'Iceland seeks internet pornography ban', *Guardian* website, 25 February 2013. http://www.theguardian.com/world/2013/feb/25/iceland-seeks-internet-pornography-ban

Baker N (2013) 'Rape Crisis group backs MEPs' call to ban porn', *Irish Examiner* website, 09 March 2013. http://www.irishexaminer.com/archives/2013/0309/world/rape-crisis-group-backs-mepsapos-call-to-ban-porn-224910.html

Barter C, McCarry M, Berridge D and Evans K (2009) *Partner exploitation and violence in teenage intimate relationships*, London: National Society for the Prevention of Cruelty to Children. www.nspcc.org.uk/Inform/research/findings/partner_exploitation_and_violence_report_wdf70129.pdf

Chapman M (2013) 'Apple ignores government pleas for greater parental controls', *Marketing* magazine website, 09 May 2013. http://www.marketingmagazine.co.uk/article/1181769/apple-ignores-government-pleas-greater-parental-controls

Department for Education [DfE] (2012), 'The Government's response to the consultation on parental internet controls', London

Desjardins, S-J (2009) 'Are the effects of pornography negligible? Universite de Montreal professor refutes demonization of pornography', Eurekalert! website, 01 December 2009. http://www.eurekalert.org/pub_releases/2009-12/uom-ate120109.php

Hope C (2013) 'Entire school year groups have seen porn, children's watchdog says', *Telegraph* website, 03 April 2013. http://www.telegraph.co.uk/news/politics/9970190/Entire-school-year-groups-have-seen-porn-childrens-watchdog-says.html

Hsu C (2013) 'Disturbing new survey reveals how porn is damaging relationships' Medical Daily website, 20 January 2013. http://www.medicaldaily.com/disturbing-new-survey-reveals-how-porn-damaging-relationships-244335

Laville S (2011) 'Teenage domestic violence: "No one did anything to stop it"', *Guardian* website, 16 April 2011. http://www.theguardian.com/society/2011/apr/16/domestic-violence-teenage-girls

McVeigh T (2013a) 'Can Iceland lead the way towards a ban on violent online pornography?', *Guardian* website, 16 February 2013. http://www.theguardian.com/world/2013/feb/16/iceland-online-pornography

McVeigh T (2013b) 'UK "will follow Iceland's lead over ban on internet porn"', *Guardian* website, 16 February 2013. http://www.theguardian.com/culture/2013/feb/16/uk-iceland-ban-internet-porn

Ministry of Justice [MoJ] (2009), 'Possession of Extreme Pornographic Images and increase in the maximum sentence for offences under the Obscene Publications Act 1959: Implementation of Sections 63-67 and Section 71 of the Criminal Justice and Immigration Act 2008', circular no. 2009/01, London

National Society for the Prevention of Cruelty to Children [NSPCC] (2013) 'NSPCC warns of e-safety "time bomb"', press release, 04 February 2013. http://www.nspcc.org.uk/news-and-views/media-centre/press-releases/2013/13-02-05-NSPCC-warns-of-esafety-timebomb/NSPCC-warns-of-esafety-timebomb_wdn94135.html

IMPROVE INTERNET SECURITY WITHOUT RESTRICTING INTERNET FREEDOM

RESTRICTING INTERNET ACCESS TO THOSE WITH UP-TO-DATE ANTI-VIRUS SOFTWARE

Sam Matthews
University of Sheffield

The internet is a unique environment that has provided space for all sectors of society to participate in. Through the internet, technical experts, industry and civil society have quietly revolutionised the way we live our lives. The openness of the internet has, however, left us vulnerable to attacks from criminals. Since 1997 the number of malicious software (malware) attacks has doubled each year (CERT/CC 2009). Despite the huge threat presented to users' information, software and hardware, some surveys estimate that the number of home users lacking basic security software could be as high as 81 per cent (AOL and NCSA 2005). These users are not only placing themselves at risk: once their computers become compromised they can be used to target other PCs or websites. The answer to this problem of home user naïvety is a product-based solution that coerces the public into downloading and updating their anti-virus software. Mandatory anti-virus software could be enforced if internet service providers (ISPs) were obliged to restrict internet access to those who have taken appropriate security measures. I believe a system can be put in place that ensures security precautions are taken without any arbitrary infringement of internet freedom or unnecessary cost to the consumer.

The internet today

Any public policy seeking to alter access to the internet must consider the benefits developed through the internet's open-platform model. The web's inclusive and participatory infrastructure style has reaped enormous benefits. Personal computers with internet access allow us to purchase goods and services without leaving the comfort of our homes. The immediacy with which we can compare online goods and services stimulates competition and creativity. UK consumers spend an average of £1, 083 per year through online shopping (Sedghi 2012). Instant communication is now possible across international borders, with the click of a button providing us with a medium for economic and social interactions. We send an estimated 294 billion emails every day ,and our appetite for social networking sites continues to grow (Pingdom 2011).

On a national level, crucial infrastructure is increasingly aided by online content. For instance, the National Health Service has one of the largest data and communications systems in the world (DCMS and DBIS 2009). Information that would once have been difficult for many to obtain can now be accessed freely and easily through websites such as Wikipedia. The internet has also encouraged freedom of expression, providing citizen journalists with the means

to publish material. Social networks such as Twitter and Facebook have been credited for inspiring and organising mass movements seeking to improve the societies we live in (Ghonim 2012: 43). The multiple services and opportunities described above may serve to emphasise the success of the government's previously laissez-faire attitude towards the internet. Descriptions of the benefits of the internet can, however, all too easily verge on the utopian, and ignore the criminality that has become an increasing threat.

The growth of cyber-crime

The ungoverned and decentralised nature of the internet has allowed it to become a dangerous weapon in the hands of criminals. The anonymity with which online users operate makes it easier to perpetrate crimes as well as avoid detection. Cyber-crime has become one of the most economically damaging forms of crime in human history (Kumar 2003: 2263): the Cabinet Office has estimated that cyber-crime costs the UK £27 billion per annum (Detica and OCSIA 2011). For criminals, malware represents one of the most economically effective forms of cyber-crime, with a clear financial model. For instance, operators of networks of infected computers are reported to charge around £30,000 per day to attack websites (Zittrain 2009: 46).

Particularly popular methods for infecting computers with malware include scareware, spam emails and corrupted websites:

- Fake anti-virus software, known as scareware, taps into the security-related anxieties of computer users. False security alerts fool users into thinking that their systems have a virus (Sophos 2011: 8). Users are then encouraged to purchase fake anti-virus software – meaning that they are paying for the privilege of installing malware on to their own computers. Scareware and fake anti-virus software is estimated to cost the UK £30 million per annum (Symantec 2009: 19).
- Spam emails are probably the best-known method of spreading viruses, simply because of their sheer volume: in 2011, 42 billion spam emails were sent (Symantec 2012: 9). The emails usually contain infected attachments, typically with an exciting or controversial subject line to draw users in.
- Finally, visiting corrupted websites is another major source of viruses. In a 2011 study, Sophos reported that 19,000 new malicious webpages are discovered every day and, of these, 80 per cent are legitimate websites that have been hacked or compromised (Sophos 2011).

Each of these methods offer significant threats to individual users' hardware, software and data. Anti-virus software targets all these forms of malware, yet many users still fail to take basic security precautions that would significantly reduce the chances that they will become a victim of cyber-crime.

Home user vulnerability

Since the mid-1990s there has been an exponential growth in the use of home computers. Before then, most computers were based in workplaces and staffed by 'professional administrators' who knew how to protect their security, staying vigilant to security warnings and updates (Zittrain 2009: 44). Today, home computer users are usually far less technically proficient than the administrators of the past, and yet their importance to the security of the internet has grown. The growth in the online community, combined with the increasing range of devices and services available, means that the home user has a growing number of security-related choices to make. Despite the importance of our security decisions, there has been and continues to be widespread failure to install or update anti-virus software.

A 2012 study by MacAfee, an anti-virus software manufacturer, found that nearly one in six internet users lacked rudimentary security precautions such as basic anti-virus software (MacAfee 2012). While this is a huge number of internet users, the real figures are probably much higher. MacAfee's sample was drawn from users who visited a webpage for 'a free diagnostic tool' for PCs called McAfee Security Scan – their sample was therefore drawn from computer users who were relatively technically proficient, and who were already concerned about computer security. This excludes many of the naïve or uninterested computer users who are unlikely to have anti-virus software. A survey of Australian internet users (who, according to MacAfee's data, are highly comparable to UK users) which sampled users at random on the basis of their home telephone number found that 51 per cent had failed to install anti-virus software (ACMA 2009: 22).

Failure to install anti-virus software endangers users' computers and data. This alone might be reason enough to make anti-virus software mandatory. However, an individual's failure to take security precautions has much wider implications: it endangers the entire online community. Once a computer is compromised it can be manipulated and used to further spread malware and viruses or send spam emails, or be used as a robot in a network of computers known as a 'botnet'. These 'botnets' are created by viruses that compromise PCs, leaving them open to later instructions. A 2010 survey estimated that 4.5 million PCs were unknowingly involved in botnets (Symantec 2010). These zombie computers are thought to be responsible for more than 80 per cent of the world's spam emails (Zittrain 2009: 45). Botnets have been aggressively utilised in distributed denial-of-service (DDoS) attacks, which can prevent even some of the best-protected websites – including Visa and MasterCard – from functioning (BBC 2010). Naïve or uninterested computer users are therefore a risk to both themselves and the security of the internet.

Mandatory anti-virus software

Education is usually offered as the answer to public naïvety over computer security. However, attempts to educate the public, such as 'Safer Internet Day', have been running for a long time, and the existence of such efforts as well as the wide availability of anti-virus software suggests that education alone is not the answer. Instead, a product-based solution that ensures that users take precautions would have far more impact.

The most effective way of ensuring that end-users have taken appropriate security measures is to simply require them to install and update anti-virus software. Internet service providers (ISPs), the companies that provide us with access to the internet, offer an efficient means of coercing the public into using anti-virus software. When a user opens a browser to go on the internet, they should be prompted to install or update their anti-virus software if they have not already done so. Users who already own anti-virus software will simply need to update it. For those without any software, the ISPs should allow them to access certain online pages that allow them to obtain the appropriate software, but not to any other parts of the internet.

ISPs should be obliged to offer a wide selection of software which varies in cost and complexity. End-users must be allowed to pick a software type that suits the way they wish to use the internet, as well as to purchase any extra security measures that they require. Anti-virus software can be purchased at a wide range of prices, with many products even available free of charge, which means that no unnecessary burdens should be placed on the consumer. Making anti-virus software compulsory would also increase the volume of clients, and thereby stimulate investment and competition.

One difficulty of this policy is that it would give ISPs control over which anti-virus software was approved. However, as long as ISPs are obliged to offer a suitably wide range of options, there would be no arbitrary infringement on user choice. In fact, it would be a very helpful way of signposting users towards reliable software types, since criminals often sell false anti-virus software.

A second difficulty is the common perception that certain operating systems such as Mac and Linux are immune from viruses. Nearly 70 per cent of Mac users surveyed by Sophos in 2009 were using no anti-virus software (Sophos 2010: 23). While it is certainly true that Mac and Linux face fewer security threats, the need for protection on both platforms is likely to grow. The Austrian independent anti-virus testing lab AV-Comparatives has argued that those who believe that their systems are immune to viruses and malware have 'created an illusion' (AVC 2012: 3). They claim that the relative security of Mac computers is a result of a previously low market share which limited the attention that criminals paid to them, and that with the increasing popularity of Macs they are likely to face a significantly higher number of threats (AVC 2012). Apple has even recommended that users

install anti-virus software (Mills 2008). The same issues apply to Linux platforms. One of their tutorials is particularly concise when answering the question of whether Linux is immune to viruses: 'In a word, no.' (Wallen 2010) The easy availability of free anti-virus software for both platforms means that being required to obtain and install anti-virus protection should not be seen as an unnecessary burden on the consumer, and may well become bring significant benefits.

Benefits

Making anti-virus software mandatory would have a huge impact on the spread of viruses, malware and spyware, and heavily reduce the enormous economic damage that is currently inflicted by these types of software. This would have significant benefits for the UK economy, not least by further improving consumer confidence in the internet which would encourage greater online activity by consumers. On top of this, the extra investment provided by the enlarged market for anti-virus software should generate greater innovation and creativity within the anti-virus industry. When combined with the much wider use of protective measures, this should present a significant setback for online criminals. Ultimately, the benefits of mandatory anti-virus software will be most significant to the home user. They would be prompted to download software that they know is genuine and won't damage their computers. Promoting anti-virus software in this way would make less technically proficient home computer users far more secure. All anti-virus software will have the basic functions of: scanning existing files to see if any of them pose a threat to computer security; assess the safety of downloads; warn about corrupted websites; and scan emails for any attached viruses.

Limitations

Mandatory anti-virus software will not, of course, solve the problem of cyber-crime. End-users will continue to make decisions that put their computer's security at risk. Given the opportunity to bypass the anti-virus software and download material that has been designated as dangerous, reckless users will continue to make the wrong security choices. However, the installation of basic security software will ensure that naïve or uninterested users have a much-improved level of online safety.

Internet freedom

The internet has grown out of our insatiable desire for superior methods of communication. Its foundation on the tenet of information sharing is what made it so revolutionary. As Jonathan Zittrain has written, 'If the internet had been designed with security as its centerpiece, it would never have achieved the kind of success it was enjoying even as early as 1988' (Zittrain 2009: 41). However, to accept that the internet should not become a place where the state is heavily involved is not the same as conceding that the internet should be lawless. The analogy between internet use and car use is illuminating. We expect drivers to pass a test in order to obtain a licence because bad driving puts themselves and other

road users at risk. In just the same way we should expect internet users to take security precautions, because not doing so puts information, software and hardware belonging to themselves and to others at risk. Although it is a third party that inflicts the harm, the home user who fails to take basic precautions is seriously negligent. The potential for computers to cause serious harm, particularly to vital infrastructure, means that regulation to ensure basic computer security is necessary.

Any legislation pertaining to the internet has the ability to renegotiate the balance of power between the public and the state. There will, of course, be fierce opposition to any legislation which enforces basic security measures. With this in mind, any such legislation must protect the values of individual freedom and their place on the internet. Individual users will remain free to choose which software to download, and the extent to which they follow its advice, as long as it continues to be updated. The fact that users will remain able to override their anti-virus software and download material that is considered dangerous means that internet freedom will be retained. The significant difference would be that users who previously had no anti-virus software will now be warned that certain downloads are dangerous, and will therefore be protected from a range of threats. If legislators are unable to pass laws that make anti-virus software mandatory then perhaps a middle-ground option would be for ISPs to offer discounted broadband, subsidized by the government, to home users who have anti-virus software. The potential costs to the taxpayer would be well worth the increased security and economic gains of a safer internet.

Conclusion

As we look to shape the future of the internet, we must seek to preserve the characteristics that have made it a success. Without restricting the public's activities online, a policy of mandatory anti-virus software could enhance security without restricting online creativity. The enforcement of security measures through ISPs offers a solution whereby home users can be made to take basic precautions without causing them unnecessary financial burdens or restricting their freedom. The human weak link in the internet's security chain has often been overlooked or ignored, thanks to the common perception that there aren't product-based solutions available to deal with human naïvety and laziness. Demanding that ISPs restrict internet access for those without anti-virus software offers a simple, product-based solution that could go a long way towards strengthening the human link in our internet's security.

America Online and National Cyber Security Alliance [AOL and NCSA] (2005) *AOL/NCSA Online Safety Study*. http://www.bc.edu/content/dam/files/offices/help/pdf/safety_study_2005.pdf

AV-Comparatives [AVC] (2012) *Mac Security Review*, Innsbruck. http://www.av-comparatives.org/images/docs/mac_review_2012_en.pdf

Australian Communications and Media Authority [ACMA] (2009) *Australia in the Digital Economy: Report 1: Trust and confidence*, Sydney. http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf

BBC News (2010) 'Anonymous hacktivists say Wikileaks war to continue', BBC News website, 09 December 2012. http://www.bbc.co.uk/news/technology-11935539

CERT Coordinate Center [CERT/CC] (2009) 'CERT Statistics (Historical)'. http://www.cert.org/stats#incidents

Department for Culture, Media and Sport [DCMS] and Department for Business, Innovation and Skills [DBIS] (2009) *Digital Britain: Final Report*, Norwich: Stationery Office. http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf

Detica and the Office of Cyber Security and Information Assurance [OCSIA] in the Cabinet Office (2011) *The cost of cyber crime*, Guildford: Detica. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

Ghonim W (2012) *Revolution 2.0: The Power of the People is Greater Than the People in Power: A Memoir*, New York: Houghton Mifflin Harcourt

Kumar N (2003) 'Digital Architecture as Crime Control', *Yale Law Journal* 112(8): 2261–2289

MacAfee (2012) 'Consumer Alert: MacAfee Releases Results of Global Unprotected Rates Study', MacAfee Blog Central website, 29 May 2012. http://blogs.mcafee.com/consumer/consumer-threat-alerts/mcafee-releases-results-of-global-unprotected-rates

Mills E (2008) 'Apple Suggests Mac users install antivirus software', CNET website, 01 December 2012. http://news.cnet.com/8301-1009_3-10110852-83.html

Pingdom (2011) 'Internet 2010 in numbers', Pingdom webpage, 01 January 2011. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers

Sedghi A (2012) 'The UK's online obsession: the latest Ofcom figures for media consumption', *Guardian* website, 13 December 2012. http://www.theguardian.com/news/datablog/2012/dec/13/uk-online-obsession-ofcom-latest-figures

Sophos (2010) *Security Threat Report: 2010*, Burlington MA. http://www.sophos.com/en-us/medialibrary/gated%20assets/white%20papers/sophossecuritythreatreportjan2010wpna.pdf

Sophos (2011) *Security Threat Report: Mid-Year 2011*, Burlington MA. http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreportmidyear2011wpna.pdf

Symantec (2009) *Symantec Report on Rogue Security Software: July 08 – June 09*, Mountain View CA. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf

Symantec (2010) *MessageLabs Intelligence: 2010 Annual Security Report*, Mountain View CA. http://www.inteco.es/file/27gHxrzWsYyeyRTFYq8MuQ

Symantec (2012) *Internet Security Threat Report: 2011 Trends* vol. 17, Mountain View CA. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Wallen J (2010) 'Myth Busting: Is Linux Immune to Viruses', Linux.com website. http://www.linux.com/learn/tutorials/284124-myth-busting-is-linux-immune-to-viruses

Zittrain J (2009) *The Future of the Internet: And How to Stop It*, London: Penguin

HOW TO ACHIEVE A DIGITALLY INCLUSIVE BRITAIN

ADDRESSING THE DEMAND SIDE

Finlay Green
University of Sheffield

The incorporation of people who have yet to engage with the internet into the new online world should be at the top of the government's social and economic agenda, yet their current efforts to tackle this issue head-on have been limited. While the government's plans to make public services 'digital by default' are important in battling digital exclusion, they address only the supply side of the problem. Lessons in how to address the demand side are readily available from the successes of the Welsh assembly government – in particular its widely acclaimed Communities@One digital inclusion programme. By adopting the Welsh model of collaboration between public, private and third sectors, while focusing in particular on using a grassroots, community-based approach, the Westminster government could make great strides towards creating a digitally inclusive Britain.

Digital exclusion – the problem

The internet is revolutionising the way we interact with the world. From the goods we consume to the services we use, all are adapting to the digital universe – often at the expense of their presence in its material predecessor. As a result, the 10.8 million people who never use the internet are excluded from those goods, services and opportunities that are more easily, and often exclusively, accessed online (BBC and Ipsos Mori 2012). 71 per cent of these digital outcasts belong to the three lowest socio-economic groups, 51 per cent are aged over 65, and 50 per cent have no formal qualifications (ibid). So it is the poorest, eldest and least employable that constitute the bulk of the digitally excluded, even though these are often the social groups most in need of online services.

For those struggling financially, the internet presents an invaluable opportunity to save money. Comparing prices online is remarkably easy, while free means of communication can replace expensive analogue ones (IPI 2011). According to a report commissioned by the Post Office, if all digitally excluded households went online, savings per household would amount to around £560 per year (SQW Consulting 2008). As for the elderly, internet access allows many to bypass the problem of limited mobility, particularly through access to online shopping services. It can also allow them to overcome the social exclusion that so often sets in with age, and which can lead to depression. A study conducted on 7,000 retirees at the Phoenix Center discovered that internet use led to a 20 per cent decrease in depression rates (Ford and Ford 2009).

For the unemployed, digital inclusion provides a better flow of information on job opportunities and useful online skills. Moreover, by improving digital literacy, the internet can have a significant impact on confidence, which is critical to finding employment (Working Links and Populus 2008). A study by UK Online Centres found that 75 per cent of unemployed internet users are confident of finding another job, compared with just 50 per cent of non-users (Freshminds 2009).

Unemployment, of course, is an economic issue as well as a social one. Digital inclusion, by reducing both frictional and long-term unemployment, can help to soften the burden on the taxpayer to support the unemployed. The same applies to the potential savings it can bring to the poorest groups in society. At a time of economic upheaval, the importance of this opportunity to bolster the government's finances cannot be overlooked.

The economic benefits of digital inclusion do not stop there. Small and medium-sized enterprises (SMEs) are the lifeblood of the British economy, generating 48.8 per cent of private sector turnover and employing 59 per cent of the private-sector workforce (DBIS 2011). In a study of 677 SMEs by Lloyds Banking Group, of those that went online 51 per cent reported increased sales, while 54 per cent reported reduced costs – due mostly to a combination of internet advertising and cloud-based services (a cheaper way of storing data) (LBG 2012). It is therefore particularly worrying that 30 per cent of SMEs in the UK have no intention of using the internet; 37 per cent don't even have a website (ibid).

Evidently, Britain has much to gain from digital inclusion. Leaving the poorest, oldest and least employable groups of society out in the cold both compounds their vulnerability and overlooks the potential of digitisation to improve our public finances. If SMEs don't get online they risk falling behind their larger, internet-savvy competitors – and taking the country with them as they do so. Considering both the social and economic arguments for greater digital inclusion, bringing the digitally excluded online should be a priority for the British government.

Why are they excluded?

The main reasons why all the groups discussed above (the poor, the elderly, those vulnerable in the job market and SMEs) shun the internet are threefold (Dutton and Blank 2011):

- **Access:** The internet can be costly, from the hardware and software to the broadband connection. Among working-age people in Britain, 52 per cent of those offline state that the cost of the internet as their main obstacle to going online; for retirees, the figure is 44 per cent. In an international survey of 3,000 SMEs conducted by Microsoft, 52 per cent stated that they lacked the resources for training employees required to adopt cloud-based services, while 60 per cent lacked the resources to implement such new technologies (Microsoft

2012). Meanwhile, in some rural areas, the poor quality of broadband serves as a disincentive to get online (Ofcom 2011).

- **Awareness:** Many non-users are simply unaware of the benefits of going online. 79 per cent of offline people of working age, and 88 per cent of offline retirees, are simply not interested in internet access. Similarly, 86 per cent of SMEs are unaware of the possible savings available from going online (EON 2012).
- **Skills:** According to research by Booz & Company, 'lack of skills is cited as a key reason many people are not online' (Koss et al 2012: 12). Indeed, 63 per cent of the working-age digitally excluded and 78 per cent of digitally excluded retirees stated that they did not know how to use the internet. With regard to businesses, 43 per cent of SME leaders are uncomfortable using the internet.

Digital by default: Half the answer

A government response must address these three main barriers: access, awareness and a lack of skills. Already the government is upgrading Britain's digital broadband infrastructure, which is essential to breaking down barriers to access. A key method for tackling all three lies in the government becoming digital itself. As Booz & Company note, 'migrating public services online ... gives people a compelling reason to use the internet' (Koss et al 2012: 31). In this area, too, the government has made considerable progress through its programme to make public services 'Digital by Default'.

However, by focusing solely on the supply side of the issue, the Digital by Default strategy provides only half the solution. Even worse, on its own the migration of public services online could further isolate the digitally excluded.

Addressing the demand side: What we can learn from Wales

Except for the indirect positive impact that the Digital by Default programme may have, the government's efforts to address digital exclusion head-on have been minimal. Direct action to tackle the lack of demand among the excluded has been limited to Assisted Digital, a loose collection of initiatives by NGOs such as Age UK, UK Online Centres and Citizens Online, among others.

The approach adopted by the Welsh assembly government demonstrates how the national government could build on the 'piecemeal' efforts of private and third sector initiatives by 'identifying a common goal to be shared' in digital inclusion. It is attempting to provide 'strategic leadership' while 'working closely with public, private and third sectors to align plans and coordinate activities' to tackle digital exclusion (WAG 2010: 6–7). Communities 2.0, the Welsh government's flagship programme for digital inclusion, aims to 'engage people with technologies' through working closely with 'community groups, voluntary sector organisations and enterprises' (Old Bell 3 2011).

This grassroots approach, with its broad, collaborative focus, follows directly from the programme's predecessor, Communities@One, which is 'widely regarded as a ground breaking initiative' (Old Bell 3 2011). The programme worked with third sector organisations through 'Community Brokers', 'staff employed by the Programme working with voluntary and community groups to develop project ideas' (Old Bell 3 2008: iii). These projects covered far more than simply purchasing digital kit – websites were developed, digital infrastructure was improved and existing staff were given ICT mentoring, while technical support staff were trained and employed. These changes were developed not just for third sector groups already working on digital inclusion, but for those that simply wanted to digitally upgrade as well. For the latter, the result was increased awareness and access to the internet in the community, just as Digital by Default aims to do. For the former, the aim was to build on their ongoing projects, and better equipment and better-trained staff bolstered both the scope and depth of their outreach. More drop-in centres giving more lessons on a wider range of digital subjects were demanded and supplied (Old Bell 3 2008).

According to the independent evaluation of Communities@One, the community brokers' role in organising and coordinating projects was critical (Old Bell 3 2008). In particular, they ensured that funding went towards addressing training and mentoring issues – overcoming digital exclusion involves breaking down barriers to access through awareness and skills, as well as through the provision of equipment.

Supporting over 200 projects, Communities@One offered unique opportunities for digitally excluded individuals to improve their access to and confidence with digital technology, particularly with regard to the internet, via third sector organisations (Old Bell 3 2008: 93). Considerable gains were made: following the end of the programme's three years (2006–2008), Ofcom observed that the digital divide between Wales and the rest of the UK had significantly narrowed. Broadband take-up had increased from 24 per cent to 52 per cent, narrowing the gap between the Welsh and UK averages by 6 percentage points (Ofcom 2010). Its methods and results were such that the programme was shortlisted as a finalist in the European Commission's e-inclusion awards, while also being praised by experts in the field (Bradbrook 2009). Due its success, the programme was expanded into what is now Communities 2.0, which has continued the grassroots focus and use of the community broker model.

The British government should learn from Communities@One. There is no reason to believe that a similar strategy for the rest of the UK couldn't replicate the Welsh programme's successes, given that 'there is no evidence that digital exclusion is significantly greater or different in nature in Wales compared to the rest of the UK' (WAC 2009: 1). Following the Welsh example, the government's approach should include:

- A grassroots, community-based focus. As Communities@One demonstrated, improving the digital proficiency of third sector organisations has the potential to significantly reduce the number of digitally excluded people.
- The use of the broker model, which was crucial to the success of Communities@One.
- A focus on training and recruiting digitally literate staff within third sector organisations, in order to tackle barriers to awareness and skills.

The main obstacle to implementing such a policy, which is highlighted in the evaluation of Communities@One, is that advances in digital inclusion may be limited in areas with weaker community and voluntary sectors (Old Bell 3 2008). A more hands-on role may be required from the state in these areas to embolden the third sector's presence. Regardless, a community-based approach represents a significant improvement on the government's current efforts.

Conclusion

A comprehensive approach towards digital inclusion must address both the supply and demand sides of the issue. While the government has made great strides with the former through the Digital by Default strategy, it now needs to address the latter. The digitally excluded will not be drawn into the online universe by a loose collection of third sector initiatives, even with digital-by-default public services. If they are to be engaged, the British government must learn from the Welsh government's successes and make the benefits of going online more visible and easier to access by coordinating and building on the efforts of the public, private and third sectors.

BBC and Ipsos Mori (2012) *Media Literacy: Understanding Digital Capabilities*, London: Ipsos MediaCT. http://downloads.bbc.co.uk/learning/learningoverview/bbcmedialiteracy_26072012.pdf

Bradbrook G (2009), speaking to the House of Commons Welsh affairs committee, London, 28 April 2009. http://www.publications.parliament.uk/pa/cm200809/cmselect/cmwelaf/305/9042804.htm

Department for Business, Innovation and Skills [DBIS] (2011) 'Business Population Estimates for the UK and Regions 2011', statistical release, London. http://www.bis.gov.uk/assets/BISCore/statistics/docs/B/Business-Population-Estimates-2011_Statistical-Release.pdf

Dutton W H and Blank G (2011) *Next Generation Users: The Internet in Britain*, Oxford: Oxford Internet Institute

E.ON (2012) 'Over One Million SMEs Unaware of Energy Savings On Offer In the Cloud', press release, 31 May 2012

Ford G and Ford S (2009) 'Internet Use and Depression Among the Elderly', presentation to Telecommunications Policy Research Conference, Arlington VA, 01–03 October 2009

FreshMinds (2009) *Does The Internet Improve Lives?*, Sheffield: UK Online Centres

Institute for Policy Integrity [IPI] (2011) *Internet Benefits: Consumer Surplus and Net Neutrality*, New York City: New York University School of Law. http://policyintegrity.org/files/publications/Internet_Benefits.pdf

Koss V, Azad S, Gurm A and Rosenthal E (2012) *'This Is for Everyone': The Case for Universal Digitisation*, Booz & Company. http://www.booz.com/media/uploads/BoozCo_This-Is-for-Everyone.pdf

Lloyds Banking Group [LBG] (2012) 'Over a third of small UK firms risk stunted growth through failure to engage with embrace the internet', press release, 08 November 2012. http://www.lloydsbankinggroup.com/media1/press_releases/2012_press_releases_lbg/1108_go_on.asp

Microsoft (2012) *Drivers and Inhibitors to Cloud Adoption for Small and Midsize Businesses*. http://www.microsoft.com/en-us/news/presskits/telecom/docs/SMBCloud.pdf

Ofcom (2010) *The Communications Market 2010: Wales*, London. http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/CMR_2011_Wales.pdf

Ofcom (2011) *Communications Infrastructure Report 2011: Fixed Broadband Data*, London. http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/Fixed_Broadband_June_2011.pdf

Old Bell 3 (2008) *Evaluation of the Communities@One Programme: Final Report*, Cardiff: Welsh Assembly Government

Old Bell 3 (2011) *An Evaluation of Communities Two Point Zero: Initial Process and Scoping Report*, Cardiff: Welsh Assembly Government

Old Bell 3 (2012) *The Evaluation of Communities Two Point Zero: Interim Evaluation Report*, Cardiff: Welsh Assembly Government

SQW Consulting (2008) *Broadband in the Home: An Analysis of the Financial Costs and Benefits: Final report to the Post Office*, London

House of Commons Welsh affairs committee [WAC] (2009) *Digital Inclusion in Wales: Thirteenth Report of Session 2008-09*, HC 305, Norwich: Stationery Office

Welsh Assembly Government [WAG] (2010) *Delivering Digital Inclusion: A Strategic Framework for Wales*, Cardiff. http://wales.gov.uk/docs/dsjlg/publications/comm/101208deliveringdien.pdf

Working Links and Populus (2008) *Breaking Down Barriers*, London: Working Links. http://www.workinglinks.co.uk/pdf/1410%20Research%20Response%20Paper%20A4%20small.pdf

#SIXFEETUNDER
THE INTERNET, SOCIAL NETWORKS AND DEATH

Michael Shneerson
University of Warwick

We need not be reminded of the immense power of the internet. It is curious to think that just over a decade ago, Friendster, the inspiration behind MySpace, had only just been founded. Today, an astonishing 92 per cent of 18–29-year-old internet users are active on Facebook, Twitter or other social networking sites (SNSs) (Zickuhr and Madden 2012). Young people interact online daily, whether tweeting their thoughts and muses, 'tagging' photos, or updating their online calendar. The depth, breadth and frequency of online activity of the 'net generation' – a phrase coined to describe a new generation socialised to read and write on tablet computers – was unimaginable only years ago. For previous generations the internet was a luxury; for young people today it is a default setting (Mayer-Schönberger 2011).

To shift from this optimistic, youthful discourse on technological progression to the relationship between death and social media may seem strange. Death, after all, is largely associated with old age, not modern technology and the tech-savvy youth who utilise the advantages it brings (Massimi and Baecker 2010). However, as the young people who belong to the first cohort of internet users to make wide use of SNS age, it will become imperative to have clear and well-conceived protocols on what to do with SNS accounts following death.

Unlike its users, the internet is immortal. When we die, our online persona lingers on in cyberspace (Odom et al 2010). This has led some to suggest that there is a difference between our physical and social death (Eagleman 2009). Previously, one's social relationships would have ended when one's physical relationships ended, upon death. With social networks, however, the dead live on as social actors (Walter et al 2012). Moreover, the social network accounts of various online agents can continue to interact with the dead in exactly the same manner as they would have were they still alive (Ryan 2008). Recently, there has been a proliferation of 'apps' which allow users to continue to be socially active after death. For example, DeadSoci.al allows users to post specific messages on their death anniversaries, and LivesOn learns a user's likes, interests and writing style in order to carry on tweeting as that user from beyond the grave. Yet currently there is no way of censoring how others interact with one's profile. Concerns have been raised, for example, regarding spam-bots or 'internet trolls' stalking and defacing the profiles of the deceased (Jackson 2010).

This provokes the question: do we want our online profiles and accounts to remain active after our deaths? And if we do, what role should they perform, and what form should they take? While alive, we have the ability to censor what appears on our online profiles: we can 'untag' ourselves from photos, or delete others' posts on our 'timelines'. However, once dead – assuming that we make no prior recommendations regarding the fate of our accounts – we will no longer maintain control over the content of our online profiles.

Indicating their growing awareness of this issue, SNSs are beginning to create procedures for dealing with user deaths. Facebook has introduced 'memorialisation', a process whereby the account of the deceased is frozen. It is not deleted, but nor is access given to family members: the profile remains a memorial on which friends and family can post obituaries, messages and look back at shared memories. Currently, Twitter simply closes the affected account (a policy they apply to any inactive accounts), but do hand over any public tweets to beneficiaries, if requested. LinkedIn also closes accounts, but will not hand over any data, information or passwords. Other internet companies such as Google, Microsoft, Hotmail and Yahoo (which was famously taken to court in 2004 after refusing to hand over the emails of a dead American marine to his family [Sancya 2005]) each have varying policies (Kumar 2012).

The inconsistency of these policies is not the only significant issue. None of these procedures allow for an individual to control the fate of his or her account when he or she dies: an individual can only ask (and then trust) a family member or friend to send the SNS the proof of death needed to delete or close an account. This has led to suggestions that 'digital wills' should be created, to be used alongside conventional wills. In this 'digital will', a user would state exactly what he or she wants to be done with his or her online accounts, emails and digital files, and would have to appoint a 'digital executor' to ensure that his or her desires are put into effect (Carroll and Romano 2010). However, without some sort of legal grounding (which does not presently exist), 'digital wills' would be nothing more than a formal request to family members or friends. This is one of many examples – as illustrated by the story about the US marine and his Yahoo email account – of how legal precedent is lagging behind technological growth.

Beyond legality, there are more practical issues with the concept of 'digital wills'. For example, as a password is a confidential affair between an individual and a website, there is currently no mechanism which would allow for the automatic updating of a 'digital will' every time a user creates a new online account or changes a password. As such, someone would have to constantly update their 'digital will' themselves if it was to be of any use. While conventional wills need to be amended only infrequently, digital wills would need to be updated much more often. In addition, given that only a third of Americans

have a traditional will, it seems unlikely that 'digital wills' will ever really take off, particularly among the younger generations.

It is therefore extraordinarily difficult for someone to articulate their wishes for the fate of their online accounts. Studies have found that there is almost a perfect divide between people who would like their SNS accounts to remain active and those who would want them deleted when dead (Asiimwe 2010). As such, establishing one default setting – whether it be the status quo of keeping accounts active, or deleting them upon death – would not be sufficient.

Thus, a combination of apathy amongst young internet users for whom death is a distant concept, ineffective and impractical tools for creating a 'digital will', and the lack of a general preference for a default option are all reasons why the current individual 'opt-in' system to determine the fate of one's digital legacy is ineffective. In order to prevent a default being required for unstated preferences, and to prevent the need for constant updating of passwords, it should be the social networking sites themselves who are responsible for ensuring that all users state their intentions for their account. This should take the form of an obligatory mechanism by which users are required, upon signing up, to make a conscious decision about what to do with their account in the event of their death.

On a practical level, such a solution would be simple and relatively cheap to implement, as it could very easily be included into the SNSs' current frameworks. SNSs' willingness to cooperate with such a policy could therefore only be hindered by the unwillingness of users to state their preferences – SNSs might fear that users may be discouraged from signing up if they are forced to confront their own death when doing so. In addition, there remains the issue of how websites would determine when a user is dead. The status quo currently requires relatives to send proof of death to all the SNSs used by the deceased. However, this is immensely time-consuming and emotionally stressful, and works only on the assumption that one's relatives are aware of all the online accounts that one has.

A solution to this would be to create a centralised system which links together an individual's medical records with his or her online accounts. Thus, websites would be automatically informed when a user's death had been officially recorded. The websites could then take the relevant course of action, as requested by the user upon signing up, without relatives or friends having to inform a huge array of online entities. However, many people would fundamentally object to a system which links all their online accounts together, and would criticise it as being out of place with the spirit of anonymity treasured by so many internet users.

A final, alternative solution would be for SNSs to ask new users what should be done with their account following inactivity, as opposed to death. Websites could then analyse user activity trends in order to determine when a user is unusually inactive. If and when

a user is identified as being inactive, and after issuing precautionary warnings (perhaps by email or text message) in case a user is taking a voluntary break from activity, a website would then do with the account whatever had previously been agreed by the user upon signing up. Although this would blur the distinction between conventional inactivity (simply stopping using an online service) and death, in cyberspace they are the same thing.

Such a policy would avoid the need to force users to face the discomfort of being asked about their own death. By automating the process, it would also make it quicker and easier for SNSs to determine exactly when to execute users' inactivity requests. It is therefore likely that SNSs would be happy to adopt this solution as a policy.

Ultimately, however, we need to individually decide whether we want our digital legacy to be eternal or finite. While this is not a decision which necessarily needs to be made in the context of death, it is nevertheless one which needs to be made. By requiring users to choose an inactivity policy upon signing up, social networking sites could ensure that users make this decision without requiring them to confront their own mortality.

Asiimwe E N (2010) 'Opinions of social web users on privacy and online DAM', *Journal of Digital Asset Management* 6: 312–318

Carroll E and Romano J (2010) *Your Digital Afterlife: When Facebook, Flickr and Twitter are Your Estate, What's Your Legacy?*, San Francisco: New Riders

Eagleman D (2009) *Sum: Forty Tales from the Afterlives*, Edinburgh: Canongate

Jackson K (2010) 'Internet troll calls Facebook memorial pages "grief tourism"', Nugget.ca website, 19 November 2010. http://www.nugget.ca/2010/11/19/internet-troll-calls-facebook-memorial-pages-grief-tourism-2

Kumar A (2012) 'Digital Assets Management: What Happens To Your Online Accounts After You Die', Geeks Club website, 25 June 2012. http://www.thegeeksclub.com/online-digital-assets-management/

Massimi M and Baecker R M (2010) 'A death in the family: opportunities for designing technologies for the bereaved', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Special Interest Group on Computer–Human Interaction,* New York City: Association for Computing Machinery: 1821–1830

Mayer-Schönberger V (2011) *Delete: The Virtue of Forgetting in the Digital Age,* Princeton: Princeton University Press

Odom W, Harper R, Sellen A, Kirk D and Banks R (2010) 'Passing on & putting to rest: understanding bereavement in the context of interactive technologies', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Special Interest Group on Computer–Human Interaction,* New York City: Association for Computing Machinery: 1831–1840

Ryan J (2008) *The Virtual Campfire: an ethnography of online social networking*, Middletown CT: Wesleyan University

Sancya P (2005) 'Yahoo will give family slain Marine's e-mail account' *USA Today* website, 21 April 2005. http://usatoday30.usatoday.com/tech/news/2005-04-21-marine-e-mail_x.htm?POE=TECISVA

Walker R (2011) 'Cyberspace When You're Dead', *New York Times* website 05 January 5 2011. http://www.nytimes.com/2011/01/09/magazine/09Immortality-t.html

Walter T, Hourizi R, Moncur W and Pitsillides S (2012) 'Does the Internet Change How We Die and Mourn? Overview and Analysis', *Omega: Journal of Death and Dying* 64(4): 275–302

Zickuhr K and Madden M (2012) 'Older adults and internet use', Washington D C: Pew Internet and American Life Project

IPPR@universities