The internet has transformed the way we live, work and play. But with the speed and convenience of everything from online shopping to smart government databases come new threats to our security, from extremist websites to virtual identity theft to cyber-espionage and viruses that can crash whole computer systems. Do the risks outweigh the benefits, and what should the balance be between freedom and security online?

The internet as we know it has its origins in the Cold War, with the USA putting money into information technology research in a bid to gain competitive advantage over the Soviet Union, not least for military purposes. It went through various early forms in universities and other institutions before the development of email and at last the World Wide Web in the 1990s. The technology gradually took on a very different culture, owing less to its military and academic origins than a wealth of ‘virtual communities’ and entrepreneurial businesses who began using and developing the internet early on. Rather than a closed system for the use of governments and universities, the internet became increasingly popular, and infused with an ethos of discovery and openness captured by the slogan, ‘Information wants to be free’.

With the new technology, however, came new challenges. The interconnectedness of the internet allowed the possibility of ‘hacking’, whereby people with sophisticated computer skills could access other people’s computers – including those of businesses and government agencies – whether for criminal purposes or simply out of mischief, or indeed more sinister political ends, such as spying for rival governments. This led to the development of a cyber security industry, seeking to come up with ever more watertight systems to protect governments, businesses and individual computer users from attacks. There are other concerns arising from the open and essentially unregulated nature of the internet, however. Since anyone can publish websites and they can be hard to trace, the internet is sometimes used by child pornographers, for example, and indeed supporters of terrorism, arguably posing a serious threat to society.

Police and security services therefore put a lot of resources into monitoring the internet and identifying security threats. But does this undermine the ethos of the internet as a forum for the free exchange of information and ideas? It is not only criminals who would prefer their online activities to remain private, but ordinary users, who often value the internet precisely because it allows them to control what they make public and what they keep private. So is giving up privacy a price worth paying for security? Or should cyber security be about protecting users from official snoopers as well as cyber villains?
Cyber Security: Head 2 Head Debate

Motion: The internet needs to be regulated

For motion: Robin Simcox, Research Fellow, Centre for Social Cohesion
Robin is also section director of the Britain in the World department at the Henry Jackson Society. He took his BA in History International at the University of Leeds, including a year spent at the University of Newcastle, Australia, and holds an MSc in US Foreign Policy from the Institute for the Study of the Americas, University of London

Against motion: Frank Fisher, Blogger and writer
Frank is a blogger and writer who has covered web censorship almost since the inception of the web. He studied philosophy, physics and astrophysics, so naturally works in software development.

Round One: For motion
A lack of regulation on the internet can be a terrific thing. When the cartoons of Muhammad were printed in Danish newspaper Jyllands-Posten but largely censored in print elsewhere in the west, internet bloggers made the images widely available. When the mainstream media in western democracies slip into self-censorship, the internet can vitally step in. Furthermore, reduced internet regulation in the world’s most repressive nations would be hugely welcome – the censorship of websites deemed ‘subversive’ in the likes of China and Iran has undoubtedly stymied pro-democracy forces there.

In the west, we rightly see the internet as an astonishingly useful outlet for freedom of speech, which is the bedrock of any truly liberal society. However freedom of speech is only absolute providing that it stays within the law, and the internet cannot be exempt from this any more than any other form of publishing outlet is. Absolute freedom of speech does not extend to having the impunity to write and distribute illegal material which could, for example, incite murder or racial hatred.

Yet material online regularly does so. The internet has been absolutely crucial to al-Qaeda, its affiliates and its sympathisers in disseminating their millenarian message. Any potential jihadist can not only download information on the nuts and bolts of how to commit a terrorist act – providing instruction in the assembling of bombs, suicide vests and the like – they also have at their fingertips al-Qaeda’s ideological justification for such acts. The grisly consequences are then posted online as further recruiting tools. Videos of suicide bombings, hostages being beheaded and al-Qaeda fighters training for ‘martyrdom’ are staple jihadist propaganda materials.

In the UK, major Islamist terrorist plots invariably have an online angle. Extremists will occasionally have been radicalised online, and are often found to be in possession of vast amounts of al-Qaeda inspired material that they will have acquired via the internet. For example: Abdulla Ali and Adam Khatib, sentenced to life for their roles in the transatlantic liquid bomb cell to destroy planes mid-flight, researched how to make the explosive devices on the internet.

Bilal Abdulla, the 2007 suicide bomber at Glasgow airport, researched bomb-making techniques on the internet and obtained advice on circuitry on internet chatrooms. Tariq al-Daour, Waseem Mughal and Younes Tsouli were all convicted for inciting terrorism via the internet.

This resource has been produced in collaboration with the RCUK Global Uncertainties programme and the Institute of Ideas Debating Matters Competition.
Cyber Security: Head 2 Head Debate

Motion: The internet needs to be regulated

**Round One: For motion continued**
Aabid Khan – convicted of terrorist offences in 2008 – began looking at extremist material online at the age of 12. By the time he was charged (nearly a decade later), he had 33 hard drives, 90 floppy disks, USB drives and MP3 players, 450 audiotapes, 188 videos, 53 mobile phone SIM cards and over 600 CDs and DVDs of extremist material. The contents of one hard drive would have filled 1.3 million pages of A4 paper. Nicky Reilly and Andrew Ibrahim – two white converts to Islam – not only researched how to make the bombs online, but were also radicalised over the internet. Reilly attempted a suicide bombing in an Exeter restaurant, while Ibrahim was planning a suicide bombing in a Bristol shopping mall.

This barely scratches the surface of the amount of cases that could be cited, including white supremacist extremists making similar use of the internet. So regulation is not just a moral or philosophical issue – it has very real domestic security ramifications. The internet cannot just be a marketplace of competing ideas – someone who gets their kicks from watching videos of hostage beheadings should not have the same opportunity to satisfy his curiosities as those trying to research a provocative piece of art.

If the internet were not regulated at all, this problem – critical at the moment – would only be amplified. However with more effective regulation, the problem can at least be better controlled, even if it is impossible to rectify entirely. Maintaining our freedom of speech over a regulated internet capable of strengthening national security is a worthwhile aspiration.

**Round One: Against motion**
So the internet needs to be regulated? It already is. A comprehensive technical framework has developed to match the expanding internet. Each and every aspect is crafted to mesh with each and every other. A host of international bodies have developed and implemented standards and procedures over the decades, to keep the servers humming, the data flowing, the right information packets ending up at the right PC. But of course, that isn’t what the “regulation” fans mean by regulation. What they mean is censorship, content rating, access controls, criminal penalties for non-compliance, enforced disconnection and more.

But here’s the rub; I didn’t raise the technical regulation of the net simply to obfuscate. Technical regulation works because it’s uniform – it’s applied identically everywhere. Like gravity, a DNS server works the same way in Laos as it does in London. Do we think we could get a similarly universal system of censorship applied? The same standardised restrictions on content applying in both the USA and Uzbekistan? Not a chance. So when people talk about enforcing regulation on the internet what they’re actually talking about is fencing off one corner, and applying their own rules there. Building a defensive firewall that keeps the “bad” stuff out, and lets them decide what their people can talk about – the Great Firewall of China being the most frequently quoted example.

Well is that so bad? A nationally divvied up internet, every sector rigorously controlled and policed? Let’s look for a moment at what that would involve. There’d be universal technical protocols agreed for sure, but this time not to permit free exchange of information and ideas, but rather to block, to monitor, to silence. A global architecture of control. An architecture we’d help put in place with, I accept, the best of intentions, but these good intentions would give tyrannical regimes worldwide the tools they’d need to police their own backyards.
Round One: Against motion continued

We’ve already seen it. US filtering software developed in the 1990s to block porn from company networks was the direct ancestor of that used today by China, Iran and Singapore. Worse, any moral authority the West might have had to denounce political censorship was blown away by our own governments’ enthusiastic clampdowns on our “red lines”, and how those red lines have since spread. Can we really tell the developing world censorship is an evil, when the material thought worthy of pursuit here in the UK has mushroomed so rapidly? Where once it was child pornography alone that required policing, soon racially incendiary material was added to the list, then extreme pornography was defined and declared off-limits, at the same time the courts held that watching a hostage being beheaded constituted some kind of assault, and then sharing copyrighted music files took centre stage as a threat to British industry, before the ugly phrase “domestic extremism” jumped up to embrace everything from Islamism to Neo-Nazism. What might require the censor’s knife next? Climate change denial? It has been suggested...

We are already half way down the slippery slope to the Chinese model. Limits on conversation that would be, one hopes, unthinkable if imposed in pubs, are becoming routine in UK-hosted forums. Our internet is fast becoming more like a corporate intranet where all conversation is tightly controlled; is this the direction we want to be travelling in? That’s not a rhetorical question – I’m genuinely curious. One the one hand we have ministers telling us that unruly bloggers must be gagged, that outlawed groups denied speech on campus should be denied it online too, that “hate speech” of a dozen different hues should be deleted, and we have Twitter mobs howling for the head of anyone who dares cross the moral boundary du jour... yet at the same time, the idea mooted in Australia of banning anonymous political comment, or disconnecting illegal file-sharers, draws widespread condemnation.

It seems to me that when the actual mechanisms required to enforce internet controls are spelled out, Joe Public is not keen. While he might not be in favour of allowing lunatic Islamists to crow about terrorist attacks, neither is he keen on the key fundamental underpinning any effective censorship of forums, newsgroups or chatrooms; the removal of anonymity, for everyone.

This, above all else, is the lesson that history teaches us about clampdowns on free expression; what happens to your neighbour today, will happen to you tomorrow.
Round Two: For motion

Frank regards the idea of a regulated internet as something akin to a police state – something which aims ‘to block, to monitor, to silence’. What I advocate would not look to block, monitor or silence freedom of speech online any more than the police would look to block, monitor or silence freedom of speech on the street. It is simply a case of making sure that internet material does not breach the law. Frank needs to have greater faith in British democracy – we are not going to become North Korea anytime soon.

He also regards regulation as giving ‘tyrannical regimes worldwide the tools they’d need to police their own backyards’. But what is the end point of this line of thinking? Free countries should not benefit from anything if others may suffer? Should we have not pursued nuclear power – and the scientific advances that this has prompted – because one day rogue states such as Iran would also go nuclear? At what point do we decide that we no longer have a right to progress as a society and strengthen our own rule of law out of fears it could cause others to regress further?

The idea that the west will lose moral authority is also a red herring. It is delusional to think that the authoritarian governments most likely to abuse internet regulation would reform and liberalise if only we hadn’t have shut down a few too many jihad-friendly websites. Authoritarians of all forms will always discover ways in which the west is at fault for something somewhere in the world. Remember, Osama bin Laden once said the reason al-Qaeda wanted to turn aircrafts into missiles in order to kill Americans on 9/11 was because their carbon emissions were too high.

Furthermore, by comparing those who want illegal hate speech to be monitored with those who condemn the idea of disconnecting file-sharers, Frank is clearly conflating issues. While both may be technically illegal, stopping someone acquiring suicide bomb instruction should obviously be given a slightly higher priority than stopping someone acquiring Lily Allen’s latest album for free.

This, above all else, is the lesson that history teaches us about clampdowns on free expression; what happens to your neighbour today, will happen to you tomorrow.

Round Two: Against motion

Robin Simcox’s proposals are a confused blend of wishful thinking and overt authoritarianism, with no suggestion as to how proposed “regulation” might actually function.

Robin suggests that freedom of speech is only to be tolerated providing it stays within the law – to which the obvious response is, whose law? UK law? US law? Iranian law? What Robin is demanding is a British internet in which contentious content simply cannot be accessed –content that is not contentious in many jurisdictions. Given that we can’t insist our laws be followed overseas, Robin’s solution can only be a national content blocking system, similar to the IWF’s anti child-porn system. This saw UK ISPs hide chunks of Wikipedia for a short time in 2008/09; it also sparked a revolt that eventually saw the IWF back down, indicating that the British public won’t support a censored internet that impacts on them, no matter how “good” the cause.
Round Two: Against motion continued
Further, the “extremist” materials Robin mentions are by no means easy to define – legally or otherwise – and most are accessible offline as well as on. Even the harshest internet censorship would not stop people talking about “ideological justifications” for terrorism, even if we wanted to live in the type of country that prohibited certain ideologies, or their discussion. Nor does restricting explosives manuals online remove chemistry textbooks from schools, or remove handbooks on “improvised munitions” from Amazon in the USA, where they’re sold perfectly legally. Or does Robin favour blocking Amazon as a dangerous terrorist resource?

Who decides Robin? What ministry or quango will work grind through the entire internet, choosing which domains to censor from UK eyes? And who will guard the guards, Robin?

We live on a small island with increasingly restrictive laws and increasingly ill-informed and narrow debate – further censorship will invite derision at home and contempt abroad. Yet it won’t stop terrorism or terrorists’ propaganda. The best counter to a dangerous ideology is not a gag, nor is it to burn books or imprison ideologues; it is to out-argue them. We will never do this if they can portray our society as frightened, censorious and tyrannical. If the only way in which we can “save” Western liberal democracy is to revoke the liberal and democratic parts…. then we have already lost.

Round Three: For motion
The Wikipedia censorship that Frank refers to was of an image on a rock band’s album cover that could be deemed offensive, but was not illegal. He cannot genuinely think that this case is proof that ‘the British public won’t support a censored internet that impacts on them, no matter how “good” the cause’. The British public may not favour censoring legal images on heavy metal bands album covers, but there is every chance there’ll be less accepting of beheading websites.

The laws passed to counter terrorism are still developing, but Frank is incorrect to say the extremist materials I refer to are not easy to legally define. It is done in terrorism cases all the time, where individuals are prosecuted for possessing a document or record likely to be useful for committing or preparing a terrorist act. All regulation would do is try and make it harder for jihadist websites to host such material. Of course where there’s a will, there’s normally a way – but currently the way is far too easy to find. And no, restricting explosives manuals online certainly does not remove chemistry textbooks from schools – but then again Key Stage 4 doesn’t instruct children on how to make explosives that will kill the maximum amount of people possible.

In an ideal world the best counter to a dangerous ideology would be, as Frank says, to out-argue the other side. But it was not the strength of liberal democratic arguments that stopped Islamist clerics such as Abu Qatada and Abu Hamza telling British Muslims to leave behind their lives in the west in order to try and kill people they do not know in countries they have often never been to. It was putting them in jail. No one wants open discussion and ideological debate to be shut down. But that such hate-preaching continues virtually unhindered online is to the detriment of us all.
Round Three: Against motion

Robin suggests I “regard the idea of a regulated internet as something akin to a police state” – indeed I do, when such pains are taken to conceal the actual meaning of “regulated”. Be straight about it Robin. What’s being proposed can only come to fruition if a national censorship structure is imposed on British ISPs.

When Robin and I started this exchange it was still just possible to dismiss this as a paranoid fear – no longer. As I write, ISPs are reeling from an amendment to the Digital Copyright Bill passed by the House of Lords last night which will compel *exactly* this kind of mass blocking. On receipt of a court order provoked by an allegation of copyright infringement, ISPs will need to take down UK hosted sites, and also block foreign sites completely.

Direct comparisons were made in the Lords between measures designed to tackle child porn, and those to tackle copyright infringement. That’s how much further we have inched down that slippery slope I spoke of just a few days ago. And what comes after paedophiles and filesharers, the political extremists, as Robin favours? The legislators’ logic would seem to be driving them that way.

It’s weaselling to talk of only blocking “illegal” content, as if that made the censorship tolerable – unless a jury has ruled on it, no content is illegal Robin – even in today’s Britain where the censor’s favourite excuse, “hate speech”, is redefined on an almost daily basis.

Further, what might “extremism” be anyway? Disagreeing with the majority? Saying that some things are worth fighting for? Isn’t that something this country used to pride itself on? Are we to have a state-sanctioned censorship body picking through news footage of war crimes from around the world to determine if it’s too inflammatory to be viewed? If a foreign army, or even the British army, kills children, then I want to know about it – I don’t want this to be concealed under the guise of preventing “justification” for terrorism.

A democracy requires transparency, it requires free speech, it must permit dissent. A state that permits none of those isn’t a democracy, no matter how many futile votes it might give us. This is the “regulation” of Big Brother.