SIDE TRACK 5

The Internet: A New Frontier for Human Rights

If we believe in human rights in the real world, we should extend those rights into the online world.

There are very good reasons that *The Rights' Future* is to be found where it is: the internet offers unique and invaluable advantages and opportunities for proponents of human rights.

At the same time, hitherto unparalleled threats to human rights have also emerged as the internet has developed – and as those whose interests oppose human rights have begun to understand the potential of the new technology.

This paradox is becoming increasingly apparent – recent developments such as the Wikileaks saga have brought it very much to the public attention. As human rights activists, it is time for us to pay much closer attention to the internet, and to start to understand more about the impact that it can have. The internet should no longer be considered something peripheral, something primarily of interest to geeks and nerds –

it's something that we all need to think about, and think about soon.

Unless we start to set out what we think is important, the standards, principles and rights that we believe should apply to our online lives, the darker, more threatening aspects of the technology could overwhelm the positives.

WHY DOES THE INTERNET MATTER?

The first and perhaps most important thing to understand is that now, in this modern world of ours, the internet has become an intrinsic part of normal life – and not just for the wealthy and privileged inhabitants of rich countries.

The internet provides not just access to crucial information and the opportunity to communicate, but it allows access to government services, to commerce and to a whole raft of social life. Moreover, if you don't have access to the net, you suffer serious disadvantages – from access to information to financial disadvantages that are growing all the time. You pay more for goods and services, have less choice and spend more time in fulfilling your needs.

It's for all these reasons that the internet (and indeed high speed internet) is being increasingly considered a basic human right

- according to a BBC poll in 2010, almost 80% of people around the world consider access to the net a 'fundamental right'
- access to the internet is already a legal right in Estonia, Finland, France, Greece and Spain

- the World Summit on the Information Society has been pushing the idea of such a right since 2003.

Whether you consider it a basic right or an instrumental right, internet access is certainly something of huge importance to vast numbers of people around the world.

AN OPPORTUNITY FOR HUMAN RIGHTS….

The internet provides a great platform for what might loosely be described as human flourishing: opportunities that are informative, creative, communicative and social. It provides space for progress, for democratisation, and for freedom in many different ways.

Some of what are often considered fundamental freedoms – and civil liberties – can be both supported and realised using the online environment: freedom of assembly, freedom of association, freedom of expression, freedom of religion, even freedom of thought. The internet both provides a medium for online meeting, communication and sharing of information and thoughts and facilitates the organisation of offline ('real world') meeting, association, communication and so forth.

What better tool for coordinating actions has ever been developed?

The internet provides a tool for the 'little people', giving paupers opportunities once the preserve only of princes – it can, if properly used, be a tool for equality of remarkable effectiveness.

AND A THREAT

At the same time, the threats to human rights that arise through the internet are equally unparalleled.

Activities on the internet can be tracked in ways that activities in the 'real' world are much harder to monitor. Our every online action can be recorded, aggregated and analysed, and compared with the actions of all those other millions (billions?) using the net, and used to profile, predict and even corral and control us.

Not only is this possible, but it is increasingly happening – to date, this has primarily been for commercial purposes, but the political applications of this kind of approach are becoming increasingly apparent. What is more, the internet is more and more in the hands of big business (which in itself offers both opportunities and threats, as discussed in T12 - Supping with Mammon) and governments all over the world are doing their best to take more control over what they seem to see as a threat to stability and as a potential tool for criminals and terrorists – or indeed for unrest or popular uprising. The events of the last week in Egypt have demonstrated this all too graphically – the authorities effectively shut down the internet in Egypt, preventing people in

Egypt accessing the internet (and hence organising protests and unrest), and stopped people from accessing Egyptian websites.

THE SPECTRE OF COUNTER-TERRORISM

The supposed needs of the 'War on Terror' have provided the 'logic' behind some of the most extensive surveillance legislation on the internet.

In the US, the PATRIOT Act includes provisions that significantly extend government opportunities to monitor civilians' activities, while in Europe the Data Retention Directive, passed weeks after the London bombings in 2007 and referring to those bombings in its preamble, requires communications providers to retain communications data on all users – who they communicate with, which websites they visit and so forth – and make that data available to governments when they need it. Peter Hustinx, the European Data Protection Supervisor, has called this 'the most privacy-invasive piece of legislation ever adopted by the European Union' and said that it had 'never been fully justified'.

The idea behind data retention is essentially that in order to fight terrorism we need to monitor all people all of the time. Complete surveillance – Big Brother would have loved to have the technology to do it. What's more, online surveillance can have an effect on the real world – as the Chinese dissidents located through leaks of their Yahoo data, and very recently Tunisian protesters whose Facebook accounts were hacked have learned to their cost.

THE POWER OF THE COPYRIGHT LOBBY

Powerful as the forces of governments are, they might be matched by the commercial lobbies of the 'creative industries' – the fight against the illegal downloading of music and movies appears to be regarded as almost as important as the fight against terrorism. Legal attempts have been made throughout the world – the HADOPI law in France, the Digital Economy Act in the UK, and equivalents in Ireland and other countries – which ultimately could require ISPs to cut-off internet access for people suspected of illegal downloading. This kind of measure also, almost in passing, requires close monitoring of internet activity, to check whether any such illegal activities are taking place – and given that, as noted above, internet access is considered by many to be a basic right, the idea that it could be cut off just on the basis of suspicion of infringement of copyright would seem more than a little disproportionate.

WIKILEAKS, ANONYMOUS AND THE US GOVERNMENT

The Wikileaks saga has been headline news over recent months – and there are many human rights aspects to it, from the idea of freedom of information, the ability of individuals to take a stand against authorities, the revelation of war crimes and so forth, as well as the questions of whether states should have the right to keep information private and whether the release of some of this information has put peoples' lives in danger. What is of particular interest

to people interested in human rights on the internet, however, have been the reactions to it, both from those against Wikileaks (starting with the US government) and those who support it and in particular the hacker groups, including the increasingly notorious ‘Anonymous’.

Looking first at the US Government, much more important than the posturing of politicians like Sarah Palin has been the way in which they have brought their power over business into play – PayPal, VISA, MasterCard and Bank of America stopped cooperating with Wikileaks, a Swiss bank froze Julian Assange’s assets the Wikileaks domain was shut down and Amazon refused to provide Wikileaks hosting services. The US Government also tried to legally compel Twitter to provide personal and private data about individuals connected with Wikileaks – at the same time trying to use a ‘gag order’ to prevent Twitter publicising the fact that they were being asked to provide this data, or even inform the individuals concerned.

Twitter challenged the gag order – successfully – and then informed the people involved, thus becoming heroes to a large part of the hacker community. That community had already been very active in the defence of Wikileaks, with the hacker group ‘Anonymous’ orchestrating attacks on all those they saw as complicit with the US governments attempts to squash Wikileaks, temporarily taking down the web services of VISA, Mastercard and Paypal amongst others.

This conflict is far from over.

The US government’s attempts to crush Wikileaks have not yet succeeded – they still function on the internet, and more and more information is still being released – but those attempts are still ongoing and can only be expected to intensify. Whatever you think about Wikileaks as an organisation or about Julian Assange as an individual, it is a conflict of great significance in terms of how the internet functions, and will function in the future.

- Who is in control? The governments and big businesses, or the ‘internet community’ of individuals and hacker groups.

- How ‘free’ is the internet – and how ‘free’ is it going to be in the future?

WHAT KIND OF FUTURE?

That is the big question – do we want an internet that is ‘free’, if potentially risky, or one that is ‘safe’ but ultimately a tool of control and regulation?

Most human rights activists would prefer the first – particularly as the risks involved with a freer internet are, as Peter Hustinx has said, far from proven. Where there is doubt – and just as there is so often when counter-terrorism is involved – surely the benefit of that doubt should be given to freedom? As noted above, the potential of the internet is immense, and it is now a fundamental part of our lives.

That must mean that its freedom is worth fighting for.

The extent of governmental control over the internet, and the opportunities for surveillance it provides, has led some – most recently Evgeny Morozov in his new book 'The Net Delusion: How Not To Liberate the World" – to suggest that the internet, far from being a democratising and liberating force, has allowed dictators to strengthen their grip, and threatens rather than empowers dissidents and human rights advocates. I believe that Morozov is unduly pessimistic – but there is a lot behind his argument, and it is something that we need to be aware of, and to do everything we can to prevent.

WHAT CAN BE DONE?

The first and most important thing is to pay attention to what's going on, and – where things are wrong – to make sure that people know about them – and that where they are very wrong, make a stand.

The debate needs to be shifted – when Wikileaks is discussed, the focus has all too often been highly misleading, with the emphasis on the risks of the leaks, rather than the substance of the leaks themselves or whether it had been right for them to be kept secret – though it's notable that the veracity of the information leaked has hardly been challenged. Where good things are done – as Twitter has done in challenging the gag order about Wikileaks – they should be applauded and supported.

A DECLARATION OF ON-LINE RIGHTS?

The next stage is to start to think more clearly about what we believe our rights should be when we use the internet.

- What kind of privacy rights do we have?
- What rights do we have over the data that is gathered and held about us?
- Do we, for example, have the right to delete that data?
- Do we have the right to anonymity?
- If we do have these rights, under what terms – because privacy and anonymity can be double-edged swords – and as shown in T8 – Down with Constantine, rights can be used by the powerful in negative ways?

When we're clearer about these rights, we should make a declaration of them, loud and clear.

Even the Obama administration in the US has recently come to a somewhat similar conclusion, in a much more limited context, calling for a 'privacy bill of rights', though what was being envisaged as being protected against was the commercial use of data. A declaration of rights could help to crystallise what

is currently a somewhat confused and disparate world – and could help to make human rights a selling point for the commercial forces that currently dominate the internet, and, perhaps, getting those forces onto the side of human rights, rather than being effectively in opposition.

If we believe in human rights in the real world, we should extend those rights into the online world. It can still be done – there have been victories for privacy and freedom on the internet over recent years, as well as setbacks, and the overall trend is far from clear. The potential benefits are huge – and the potential downside disastrous.