Online Civil Rights After September 11th

The threat to the right to protest online from the war against terrorism

prepared by *the electrohippie collective*, November 2001, for the ICA's *Being an Obstacle* weekend

The online world represents a new 'space' in society where the public can work together on issues of common concern; to lobby, to protest, and to take action. But even before this potential has been broadly realised, the new 'war against terrorism', and the new legal sanctions against terrorism, threatens the rights of the public to use the Internet as a medium of public discourse and dissent.

The War Against Terrorism and the Internet

In the wake of the terrorist attacks of September 11th states across the globe are introducing new laws to control the Internet, and to control the dissent, online or otherwise, of those who disagree with the current government policy, or the status quo in general. Whilst controls over 'real world' dissent are difficult, because of civil liberties laws and conventions, the control over the Internet is far simpler. Many states do not officially recognise the Internet as forming part of 'civil society', and so do not agree that civil rights extend into the virtual world.

The War Against Terrorism − TWAT − has enabled new laws to be speedily implemented that have damaging implications for civil rights. And yet, in relation to the Internet, there is precious little hard evidence that closer monitoring of the Internet will have any impact on terrorism. By declaring a 'war' against terrorism, states are able to 'militarise' the issue of controlling undesirable activities by certain groups in society, and thereby justify extreme measures to control these activities. Likewise, by declaring a single terrorist incident to be the prelude to 'the first war of the Twenty−First Century', the politicians who support TWAT are able to take absolute control of the public and political agendas under the guise of a 'military emergency'.

In reality, whilst the events of September 11th do require action to bring those responsible to justice, the response of many states has been to use terrorism as an excuse to settle old scores with troublesome organisations. However, the main target of these new laws will be the use of the Internet by civil society as a form of low cost communication, an uncensored mass media, and a space for unrepressed political debate.

Civil rights and the Internet

The message that *the electrohippie collective* would wish people to take away from this weekend is this: *Protest on the Internet is not a novelty, or an annoyance, or an abuse of electronic networks, it is a human right granted alongside all our other civil rights; this right existed before the Internet was conceived, but by its design it protects the use of the Internet as a means of public debate, discourse and action.*

As conflict has moved from a 'cold war' between nation states, towards an 'asymmetrical' conflict of ideologies between states and minority groups, the ideas of freedom of thought, conscience, religion and association have been redefined. The various conventions drafted immediately after the Second World War are being redefined by the everyday availability of digital technology. Not only does this technology create new opportunities for human expression, it also creates new and low cost opportunities for state monitoring, surveillance and targeted repression of its citizens.

The *UN Universal Declaration of Human Rights*[1] and the *European Convention on Human Rights*[2] contain standards relating to freedom of thought, expression and association. In relation to the Internet, Article 19 of the UN Declaration (replicated in Article 10 of the European Convention) has particular relevance:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

The UN Declaration/European Convention rights are recognised within our everyday life in the real world. But the development of these rights within the networked society has been conveniently ignored by many states on the basis that the Internet is a privatised entity. So far there has been no progress in getting states to legislate for Internet rights. Legislators regard people's connection to the Internet to be purely a contractual relationship and therefore beyond the reasonable bounds of regulation. Such an argument is a non sequitur given that the regulation of other contracted public utilities, such as power or telephones, is already carried out in the 'public interest'.

TWAT provides a focus for debating human rights on the

Internet because of the new laws that aim to provide monitoring of Internet traffic, or to criminalise certain activities relating to expression or dissent, in ways which directly challenge our human rights. For example, in the USA, in a presentation to the US Senate the Director of the FBI stated that groups such as *Reclaim the Streets* were to be considered as 'terrorist organisations'[3]. But also in the USA, the new *USA Patriot Act* is being challenged under the rights granted in the US Constitution. Other similar laws are being prepared in other states, and these too may be subject to challenge − but such challenges can only take place retroactively, once the laws have been introduced. In any case, these new laws may not stop terrorism as many of them seek to provide greater surveillance of new communications technologies. As some commentators have noted[4], this may in itself lead to further failures by state security services where those planning action deliberately use low−tech methods.

The new UK anti−terrorism framework

The interesting case, and exemplary to other states currently planning new laws to control the public's use of the Internet, is the UK. The 'new' laws introduce elsewhere to extend the definition of terrorism post September 11th were enacted in the UK a year ago. The UK was one of the main parties promoting a new European *Cybercrime Convention*[5], and the implementation of recent laws in the UK creates a new legal framework that implemented this agreement before the negotiations were concluded. This new legal framework comprises three parts:

- *The Police Act 1997*[6] and the *Security Services Act 1996*[7] enact the principle of 'common purpose';
- *The Terrorism Act 2000*[8] extends the definition of terrorism, and the power of the state to investigate terrorism;
- *The Regulation of Investigatory Powers* (RIP) *Act 2000*[9] enacts new powers to monitor communications, and to require the decryption of encrypted data.

The RIP Act creates a new framework for state surveillance to cope with the new digital media. As well as permitting the bugging of people's homes or workplaces, and the tapping of telephones, it also requires communications service providers (telephone and Internet providers) to enable the state to monitor the communications flowing through their systems.

The RIP Act differentiates between the *content* of a communication, and the *communications data* that is attached to the communication. *Communications data* describes the form of the communication, where it came from, and where it is going to, and how long it took to transmit. Although the communications data does not contain a message it can, when databased with the communications data of others, provide an extremely accurate profile of a person's life, political or social activities, and the network of contacts or friends with whom they carry out these activities.

Once databased and archived, communications data can be used, with very little cost or effort involved, to produce 'data profiles' on thousands or tens of thousands of people. It is for this reason that the collection of communications data represents a threat to civil liberties. As was seen in the recent legal action against the Metropolitan Police by the McLibel Two[10] there are instances where the authorities may release information covertly to non−governmental agencies − in this case the former policemen who made up the McDonalds corporation's corporate security team. There have also been instances, such as the *Bignell case*[11], where information held by security or police authorities can be accessed for private, and perhaps even criminal uses. Also, as recently confirmed by the former head of the Security Service, Stella Rimmington[12], that at the behest of the Conservative government MI5 routinely monitored trade unionists and anti−nuclear campaigners[13]. Given past experience is likely that such a database of personal information could be easily used for overtly political objectives by party politicians. In these situations the data profiles held on individuals could be misused, or used for purposes that are directly contrary to that individuals private or human rights.

In conjunction with the RIP Act, the other significant aspect of the 'non−terrorism' legislation of recent years is the 'common purpose principle. The Police Act and The Security Services Act state that '*conduct which constitutes one or more offences shall be regarded as serious crime*' where it involves '*conduct by a large number of persons in pursuit of a common purpose*'. This may encompass traditional criminal activities, but it would also encompass the civil disobedience actions associated with social or environmental protests. This means that very minor offences, such as marching in the street without informing the police, or trespassing on land, may be investigated as 'serious crime' (equivalent to terrorism or violent robbery) when they are carried out by a large number of people.

Finally, the Terrorism Act itself creates the powers that stitch these other laws together. The Terrorism Act creates powers relating to 'terrorist investigations' that give effect to the common purpose principle. The Terrorism Act also creates the need for greater surveillance that is satisfied by the RIP Act.

The primary problem with the Terrorism Act is that its definition of 'terrorism' is so broad that it will encompass the activities of some online campaigners, and some real world groups that use direct action as part of their work − for example the groups that rip up genetically engineered crops such as *genetiX snowball*, or those that trespass or block roads such as *Reclaim the Streets*. To be a terrorist a person or group must:

- carry out or propose action that involves '*serious violence against a person*', '*serious damage to property*', '*endangers a person's life', 'creates a serious risk to the health or safety of the public '*, or '*is designed seriously to interfere with or seriously to disrupt an electronic system'*, and

- the proposed action advances '*a political, religious or ideological cause*', and
- the proposed action '*is designed to influence the government or to intimidate the public or a section of the public*'.

This last point is the one that challenges civil liberties. Intimidating the public to influence the government is the traditional objective of terrorism. But the ability to undertake action '*designed to influence government*' without threatening violence is the primary guarantee of a democratic society. The use if the word '*or*' in the Act means that the two elements of this clause are logically separated. For those who are sceptical of the impact of these new laws it is important to realise that, in the mind of the government ministers proposing this legislation, the actions concerned need not involve violence. As noted in the recent government guidance to local government officers in the UK on the implications of the Terrorism Act the Act is intended to target:

> *... acts that may not in themselves be violent but which nonetheless but have a significant impact on modern life...*[14]

What this means, when taken together with the RIP Act and the common purpose principle, is that any protest action that involves minor infringements of the law, such as trespass, or obstruction of the highway, could be investigated as terrorism. For those engaged in online campaigns it means that if an action causes 'disruption' −which can mean something a minor as sending someone more e−mails than can be easily read in their in tray, or running a fax machine out of paper − can also be investigated as a potentially 'terrorist' action.

In the political climate post−September 11th, those undertaking any sort of protest action, particularly if it involves any sort of direct action, must weigh carefully the likelihood that they might invite upon themselves some sort of 'terrorist investigation' under the new Act. Such an investigation is unlikely to lead to any serious prosecution, and in fact the securing of prosecutions may not the the primary objective of the new legislation. Instead, many campaigners have found that such investigations can be extremely disruptive to their lives and campaign activities. But in the mindset of those defending globalisation, any action that seeks to challenge globalisation will be perceived as representing the same philosophy that motivated the attack on the World Trade Centre[17].

Online Action Post−September 11th

Following the terrorist attacks some newspapers have trumpeted the end of anti−capitalist protests[15]. Others have since wrote articles disagreeing[16], but it is clear that many now regard anti−capitalist action, inclusive of any kind of online protest action, as symptomatic of the same philosophy that motivated the September 11th attacks[17]. The one thing that may break this perception is the current war against Afghanistan. If this continues, and results in a humanitarian disaster, the resulting anti−war protest action may itself provide a valuable role for online, internationalised protest against the neo−liberal 'new world order' that is the root cause of many protests against the US and other states, and the foundation of the anti−capitalist movement.

But irrespective of the arguments about September 11th, those working online to '*change the mind of governments*' have to come to terms with the fact that these new laws exist (see the following 'conclusion' section on direct responses to this). In terms of the current forms of online action taking place today the following can be said:

- Passive actions, such as web pages, online petitions and pledges will be pretty much unaffected. Unless these types of action advocate breaking the law (see next point below) they will not be caught within the new definitions of 'terrorism'.
- Web sites that promote any type of direct action that involves breaking the law, even if this is only minor offences such as trespassing on land, or attending a demonstration that is not registered under the public order act, could result in those promoting that site being investigated. This is unlikely, except in cases where those promoting the site are advocating violence, to result in any prosecution, but the impact of the investigation may result in that group's Internet Service Provider closing down the site as a result of pressure from the police or Home Office.
- Groups that make available information on direct action, or on how to undertake direct action, may find themselves investigated under the new Section 58 of the Terrorism Act that relates to '*possession of information useful to terrorists*'. There is no definition or explanation of precisely what kind of documentation might be useful to terrorists, and the section applies to both paper and electronic documents. A person may be charged with this offence even if the police have no evidence that they are involved with any terrorist action. An example of how these powers might be used are the trials of activists for 'conspiracy with persons unknown', for example the recent trial of the 'GandALF Six'[18].
- Groups that promote online action that results in 'disruption' of electronic networks, which can be as little as running a fax machine out of paper, or asking people to e−mail someone en masse, all the way up to cyber−sit−ins, are likely to attract the attention of the state. This is because, post−September 11th, many politicians and security groups are not asking that any disruption of the Internet be regarded as terrorism. This does not include those groups who engage in the cracking of security systems or who spread computer viruses as part of this group − they can already be prosecuted under existing computer abuse legislation.

In the coming months the pressure on online activists will not only be legal. Increasingly Internet Service Providers will be pressured to remove content that is deemed

'subversive'. Already, in the US, protest sites are being deleted from servers. If the current move towards marginalising protest action continues, and many protest groups are reclassified as 'terrorists' (see the Director of the FBI's speech noted earlier for the scope of such changes) this trend may is likely to increase.

Conclusion − redefining online protest

In order to move beyond the impasse some campaigners have identified following the September 11th attacks, we have to move forward to redefine online action not as some strange kind of computer hacking, but as a legitimate and necessary form of protest within the new 'information society'. In particular, we must base online protests not on the basis of '*we can do this*', but rather on our '*rights*' to communicate and express our dissatisfaction with the state under the UN Universal Declaration of Human Rights or the European Convention on Human Rights.

By advocating online action we are in fact stating something more. In those states where computer networks have become pervasive we are advocating the 'right to communicate'. But at the same time, for the poorest in those states, and the majority of the world's population in developing countries, we also are arguing for a 'right to access networks'. This last point is key − if people are excluded from this new information society because they lack the equipment or money to get online, we merely reinforce the economic divisions created by the 'industrial society' of the past 250 years. By proposing that online action forms part of a functional democracy, we must also advocate that those in our own and other states must also be given access to the information society, irrespective of means, or of language barriers.

Finally, the online community must show solidarity within its own ranks. In the view of *the electrohippie collective*, TWAT, and the new anti−terrorist powers spawned as part of TWAT, represent an attack on our fundamental human rights. We must support each other when our rights are attacked by the state or private corporations. This in itself is significant. But given that, whether we like it or not, electronic networks will form the core of our society over the coming years, to deny our rights to protest and take action online is to deny the fundamental guarantee of democracy in the new information society − the ability to say no, and say it loudly so that others may hear also. ***Online protest must exist for democratic society to operate in the information age***

Notes:

1. UN Universal Declaration of Human Rights − http://www.un.org/Overview/rights.html
2. European Declaration of Human Rights − http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm
3. *Statement for the Record − Louis J. Freeh, Director Federal Bureau of Investigation − on the Threat of Terrorism to the United States*, 5th October, 2001 − http://www.fbi.gov/congress/congress01/freeh051001.htm
4. *How the plotters slipped US net*, Duncan Campbell, *The Guardian*, Thursday September 27, 2001 − http://www.guardian.co.uk/waronterror/story/0,1361,558371,00.html
5. Council of Europe Cybercrime Treaty − http://conventions.coe.int/treaty/en/projets/cybercrime.htm
6. Section 93, Police Act 1997 − http://www.legislation.hmso.gov.uk/acts/acts1997/1997050.htm
7. Section 2, Security Services Act 1996 − http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm
8. The Terrorism Act 2000 − http://www.hmso.gov.uk/acts/acts2000/20000011.htm
9. Regulation of Investigatory Powers Act 2000 − http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
10. The McLibel Two brought a suit against the Metropolitan Police for 'malfeasance in public office' after it was revealed the police passed personal information to McDonalds security staff. This was settled out of court earlier this years, following a payment to the Two, and a public apology from the Police Commissioner.
11. The *Director of Public Prosecutions* (DPP) *v. Bignell* case (1998) relates to a failed prosecution against police officers who obtained information from the Police National Computer (PNC) for personal use.
12. *Open Secret: The Autobiography of the Former Director−General of MI5*, Stella Rimington, published by Hutchinson, ISBN 0091793602
13. *Thatcher spying order during miners' strike*, The Times, Saturday 8th September 2001, http://www.thetimes.co.uk/article/0,,2−2001312219,00.html
14. Home Office Circular 03/01 − *Terrorism Act 2000*, March 2001. http://www.homeoffice.gov.uk/circulars/hoc0301.htm
15. *Clamour Against Capitalism Stifled*, Financial Times, 10.10.01 − http://globalarchive.ft.com/globalarchive/article.html?id=011010001107
16. *Between McWorld and Jihad*, Naomi Klein, The Guardian, 27th October 2001 − http://www.guardian.co.uk/Archive/Article/0,4273,4284884,00.html
17. *G7 activists no better than Bin Laden*, This is London − http://www.thisislondon.co.uk/dynamic/news/top_story.html?in_review_id=471397&in_review_text_id=425613
18. *The Green Anarchist and Animal Liberation Front trial* − see http://www.tlio.demon.co.uk/gandalf.htm, and http://www.oneworld.org/index_oc/greenanarchist.html

Note also that, coincidentally, 'TWAT' is a 17th Century English term of abuse meaning 'an unpleasant or stupid person'