the electrohippies collective – communiqué December 2000

Cyberlaw UK: *Civil rights and protest on the Internet*

produced by *the electrohippies collective*, December 2000
website: http://www.gn.apc.org/pmhp/ehippies/ email: ehippies@gn.apc.org

Since early Summer 2000, *the electrohippies* have been rather 'quiet'. This is because the majority of *the e'hippies* are based in the UK, and during 2000 the British government has been developing new laws to 'police' British cyberspace. This potentially makes the actions of *the electrohippies collective* in the UK, whilst not illegal, potentially subject to a disruptive investigations by the state.

Over the past six months *the electrohippies* have been investigating these new laws. In our view, whilst not affecting 'mainstream' Internet users in the UK, these laws impact on the rights of ordinary people who wish to protest or take some form of protest action on the Internet. This clearly affects the work of *the electrohippies collective*, but many other groups in the UK also.

In our view, these new laws are in conflict with our democratic rights. There should be no distinction between rights of protest in real life and in cyberspace. These laws create this distinction, and threaten the development of a true civil society within the new public arena created by electronic communications. The government cannot allocate this space arbitrarily to one group in society – the e-commerce corporations – and deny everyone else rights to develop their own activities and communities.

Both the Department of Trade and industry and the Department of Media Culture and Sport are introducing new policies to move Britain's media and commerce laws into the 21st Century. But these developments are moving hand-in-hand with parallel initiatives through the Home Office (the UK's department of the Interior) that are seeking to 'police' the Internet. But these new laws, rather than enabling the free use of the Internet by all, are seeking to blur the distinction between public protest, crime, and terrorism, in order to provide a 'safe environment' for corporations to do their deals.

'Sanitising' the Internet to remove the potential for public pressure on commercial operations removes the prime control mechanism on corporations. Corporations must operate within the moral and normative framework of society. Without this control their practices would become more and more excessive.

Providing an area for corporations to do business without the 'interference' of the wider society offends one of the key democratic principles that underpins civil society – it disenfranchises society from corporate governance. In essence, the British Government is seeking to define a 'virtual corporate free state', akin to the economic colonies of Africa and Asia established during the Nineteenth Century, where corporation can do business free of public pressure. The motivation for this is a perceived benefit to the economy. In fact, it merely concedes to the wishes of corporations who want be able to 'do business' without having people protest about environmental impacts, sweatshop labour or quality and safety standards.

Therefore, during 2001, *the electrohippies collective* will be developing tools and actions that seek to directly challenge these new laws, and expose the contradictions between the new e-commerce revolution being pushed by the government, and the government's other major project – the incorporation of the European Convention on Human Rights into UK law. As well as seeking to develop D-I-Y e-action tools, we'll be looking to provide our expertise to campaigns in the UK, to provide our support, but also to find a platform for action that can take-on these new laws directly.

Over the coming months we'll be announcing new actions and resources on our website.

Watch this (cyber)space!

Background

The British government has a policy of making the UK, '*one of the best places for e-commerce in the world*'. This policy of course comes from a Prime Minister who, from his own admission, gets most of his information about the Internet from his kids.

There are two new laws that significantly change the rights of British citizens to freely use the Internet for political and protest action:

- *The Terrorism Act 2000*; and
- *The Regulation of Investigatory Powers Act 2000*.

The main legislation on e-commerce trumpeted by the government is *The Electronic Communications Act 2000*. The draft legislation for this Act included proposals on the restriction of cryptography, but these were removed by the government because confusion this would create with the powers of the Home Office. Therefore *The Electronic Communications Act*:

- Enables the Government to set up a register of '*approved cryptography suppliers*'. This does not ban the use of cryptography by anyone else, but it will mean that certain companies will be able to claim government approval for the selling cryptography services, such as digital signatures, to others.
- Linked to the approval of cryptographic services, the Act gives legal weight to the setting up of digital signatures.
- As a side issue, in section 14, the Act creates a prohibition on the introduction of key escrow systems (systems where you can use encryption, but you must give a copy of your key to the government) by the UK government.

But the government still wanted to reform cryptography and surveillance laws. So, because of opposition from politicians and civil servants, instead of their inclusion in *The Electronic Communication Act* the government created new powers in a new Act intended to bring the police forces of the UK into the Twenty First Century – *The Regulation of Investigatory Power Act 2000*.

The 'RIP' Act creates:

- New powers to intercept communications, and use 'covert sources' to obtain information: New procedures are introduced to enable the police and security services to install surveillance equipment, tap both voice and data communications, and to use 'informants' as part of their investigations of groups or individuals. These new powers cover the 'grey areas' under previous law such as electronic communication like emails, and communications data (the phone numbers you dial from your phone line etc.).
- A requirement for Internet Service Providers to '*maintain an interception capability*' on their hardware: In plain language this means that all UK Internet Service Providers, if requested by the Government, must fit a 'black box' to their servers that will rely a copy of all data sent through the system to the state security service – MI5. This should only happen when the security services obtain a court warrant. But the black box will be on all the time, and will be switched on- and off by the security services themselves at their end of the line. For those ISP's who object, it is likely that the 'backbone' providers, who provide the high capacity lines to the ISP, will install the black box relay 'at source'.
- A requirement to disclose encryption keys: If the police or security services intercept or obtain encrypted data from a person, they can get a court order to require the person to provide the encryption key to decrypt the data, or face prosecution, with a penalty of up to two years imprisonment, for refusal to do so.

The RIP Act creates powers of investigation. *The Terrorism Act* goes one step further by blurring the division between the sort of activities that campaigners/protestors undertake, and terrorism. The problem rests on one word – '*OR*'.

When the draft legislation was made it was a terrorist offence to '*seek to intimidate the public*'. No problem there. But in it's last stages in the House of Lords this definition was changed to action where, '*the use or threat is designed to influence the government OR to intimidate the public or a section of the public*' (our emphasis). The use of the word 'or' means that the terms can be considered separately, and therefore it could be interpreted as a '*terrorist act*' if an action '*sought to influence the government*'!

The Act also specifies various types of action or motivation that, combined with the objective noted above, could be construed as '*terrorism*'. To be a terrorist act, it is a condition that the action must be, '*advancing a political, religious or ideological cause*'. Nearly all protest action would fulfil one of these objectives, or could be argued to, and therefore this condition is easily satisfied. Finally, the action must satisfy one item in a list of possible actions that are engaged in by terrorists. Whilst conditions such as 'violence against people' or 'endangering the life of others' are acceptable, there are two possible clauses that can be satisfied as part of a number of types of protest action – that they:

- 'involve serious damage to property'; or
- 'are designed seriously to interfere with or seriously to disrupt an electronic system'.

Whilst the first of these could result from a real world action, the second is more likely to happen with a virtual action. This second point goes far beyond the existing UK computer misuse legislation – the *Computer Misuse Act 1986*. Currently, to commit an offence under the computer misuse laws of many states (including the UK) you must change the operational parameters of the computer system in order to break the law. Under *The Terrorism Act,* you would just have disrupt the operation of the system without any modification involved. For example, an email campaign that sent thousands of emails to a government minister, so causing problems with the minister's office because of the deluge of public communications, could be considered a 'terrorist act' under the current interrelation of definitions under the Act. That would be potentially unlawful. But if carried out using the postal system, so disrupting the function of the whole office, it would not.

These new laws are clearly aimed not just at formal crimes, but also at the 'difficult' cases involving active protest groups. In the UK over recent years anti-roads protestors, animal rights protestors, countryside campaigners, and even the recent fuel price protests, have been difficult to police because the mode of the action, whilst causing disruption, was essentially legal. Many security consultants are concerned that such actions, transferred to the Internet, could be equally effective. But these new laws enable Internet-based protest, if operated from the UK, to result in state investigation of those involved.

Related resources:

Here are a number of links to material on the *Terrorism*, *Electronic Communications* and *RIP* Acts:

- Copies of *The Electronic Communications* (EC) *Act*, *The Terrorism Act* and *The RIP Act* are available online:
  - HTML versions are available from the HMSO website –
    - The Terrorism Act `http://www.hmso.gov.uk/acts/acts2000/20000011.htm`
    - The RIP Act `http://www.hmso.gov.uk/acts/acts2000/20000023.htm`
    - The EC Act `http://www.hmso.gov.uk/acts/acts2000/20000007.htm`
  - Adobe Acrobat versions are available from the electrohippies collective's website –
    - The Terrorism Act `http://www.gn.apc.org/pmhp/ehippies/archive/terr-act.pdf`
    - The RIP Act `http://www.gn.apc.org/pmhp/ehippies/archive/rip-act.pdf`
- GreenNet's *Civil Society Internet Rights* site has a number of briefing on issues related to online democracy: `http://www.gn.apc.org/action/csir/index.html`
- Further information on *the electrohippies collective's* online actions and tools will be placed on our website during 2001: `http://www.gn.apc.org/pmhp/ehippies/`