

What price national security?

A day of discussions at the Freedom Forum European Centre,
November 10, 2000



When The Freedom Forum in association with Article XIX, Index on Censorship, and Liberty began organising a major London conference on the issue of national security vs. the right to know, we could not have anticipated what dramatic developments were about to unfold.

At our initial meeting, there was one overwhelming preoccupation: the case of former MI5 officer David Shayler whose defiance of the Official Secrets Act had made him a marked man and put at great risk a number of journalists and publications that had reported and published what he had revealed to them. At that time, Shayler was still in exile in Paris, and his lawyer, Liberty Director John Wadham, was campaigning to get British public and legal opinion to accept that Britain's Official Secrets Act was now invalid as it breached the new European Human Rights Law that was about to be instituted in British law.

By July, the British Appeals Court had given British journalism one of its biggest victories over the Official Secrets Act by defending the rights of reporters at The Guardian and The Observer not to hand over material and emails that related to Shayler's accusations that British intelligence was linked to a plot to try and kill Libya's Gaddafi. The Guardian in its reporting characterised Judge Judge's ruling as a "ringing defence of press freedom and the newspapers' right to publish allegations by whistleblowers."

By the end of August, David Shayler had sailed home after government prosecutors had thrown out the more serious charges against Shayler related to the Gaddafi accusations. Once back on British soil, he turned himself over to British authorities and was arrested on lesser charges related to removing copyrighted materials from MI5 offices.

By the time we met in November, and Shayler would make his first major public appearance, the government was still

determined to try Shayler in secret. If Shayler had won a partial victory, another celebrated whistleblower, Lieutenant Colonel Nigel Wylde, had the satisfaction of seeing all charges against him dropped as the government's case collapsed entirely. Wylde had been one of former Sunday Times' journalist Tony Geraghty's prime sources in his book, *The Irish War*. Geraghty himself had faced prosecution until the government finally dropped its case last December. Geraghty and Wylde would be reunited at our conference and remind everyone how close they came to becoming victims of the OSA.

But when it came to reporting on Northern Ireland, the government was still determined to stop what it considered to be damaging information from being published. Increasingly, it resorted to what Sunday Times Lawyer Alastair Brett described to our conference as "laws of confidence to silence the press." Brett would explain how Sunday Times Northern Ireland editor Liam Clarke had to fight injunctions that were "wheeled out time and time again" to stop his reporting about the activities of the Forces Research Unit (FRU) a secret army intelligence squad.

While American journalists can rightfully point to our First Amendment and Freedom of Information Act that have prevented many of the excesses of the Official Secrets Act, there is no room for complacency as we learned at the conference. Just prior to our event, the Congress had passed a bill that would have according to British investigative journalist Duncan Campbell bestowed on the United States a version of the 1911 Official Secrets Act. Only an 11th hour veto by President Clinton prevented the bill from becoming law.

Bob Haiman a former newspaper editor, and more recently, a Fellow at our First Amendment Centre in New York told the conference: "I believe that the US came very close to the edge of the precipice."

John Owen director, European Centre

Panel 1:

The nature of national security

Moderator:

Nick Fielding (*Sunday Times*)



Nick Fielding
SUNDAY TIMES

Panel:

John Wadham (*Liberty*),
David Shayler (*ex-MI5*),
Rear Admiral Nick Wilkinson
(*D-Notice Committee*),
Glenmore Trenear-Harvey
(*IntelResearch*),
Stephen Dorril (*author*)

I think everyone can agree there has not been this level of interest

and intense debate on national security for many years. There has been a succession of legal cases in the United Kingdom, and most of the debate is taking place in the courts. We've had David Shayler and Richard Tomlinson, [the pseudonymous] "Martin Ingrams," Nigel Wylde, Tony Geraghty, Martin Bright, Liam Clarke, James Steen of Punch, Julie-Ann Davies. The cases are piling one after another through the courts, but have not really been reflected in civil society in terms of debate taking place in Parliament. In fact, Parliament has been left behind in this debate and has almost categorically refused to discuss secrecy issues despite the pledges of this government while in opposition.

[Bill] Clinton's last act before the election was to veto what would have been a very draconian act in the United States. In Europe, we've seen moves recently to tighten up on what was an organisation that prided itself on its openness. The European Commission has introduced a number of restrictions on access to information, mostly on security grounds.

Speakers in this session will be John Wadham, director of Liberty; David Shayler, who is largely responsible for igniting a large part of this debate about national security; Rear Admiral Nick Wilkinson, probably the most enlightened secretary of the D-Notice Committee that has been imposed for many years; Glenmore Trenear-Harvey, a researcher and writer with IntelResearch; and Stephen Dorril, author of a well-received book on MI6.

THE NATURE OF NATIONAL SECURITY



JOHN WADHAM, STEVEN DORRIL, DAVID SHAYLER, REAR ADMIRAL NICK WILKINSON, GLENMORE TRENEAR-HARVEY



John Wadham
LIBERTY

We should start by considering why there isn't anybody from the authorities here today. I've had

great difficulty in the past in engaging anyone from Parliament, government or the security services in any debate on these issues. The best we get is unattributable briefings or briefings from ex-MPs. But we never get anybody talking about what their position is, and that's not acceptable in a democratic society.

When the first report by the Intelligence and Security Committee — the parliamentary committee that's supposed to keep the security forces under surveillance — was debated in Parliament, no one addressed the real issues that were raised by David Shayler and Richard Tomlinson. There was a lot of sniping about individuals, criticism of those whistleblowers, but no one asked a single question about the allegations they raised. How can we have a parliamentary system where nobody raises any of the issues?

I received a letter from a person I can't name, somebody who is the publicity person for the security service. I wrote asking him to come here today, and he replied: "Thank you

very much for your invitation. I do hope the day proves worthwhile and productive. The topics you plan to discuss raise some real issues over which there will be much debate. I hope this debate at the same time generates light rather than heat and better understanding of the issues." But that's not enough. We need that person to attend and to have this debate with us.

I've also got a letter from Tom King, chair of the Intelligence and Security Committee, who I also invited along to this event. He said he was engaged on constituency business that day and wouldn't be able to attend. That's not acceptable. This is the first conference I can think of on issues about national security and freedom of expression, and the parliamentarians that are supposed to support us, those people that are supposed to ensure they are keeping the spooks under surveillance, are not here.

I've got to criticise this government on the Official Secrets Act [OSA]. When the bill was going through Parliament in 1988, they were very critical and voted against it. Many of the members of the current cabinet voted against it because it didn't have a public-interest defence, it didn't have freedom of expression written into it. It allowed whistleblowers to be prosecuted, people who had done a real service to the community. It's a problem that we have a government that votes against the measures going through when they're in opposition, but then consents to the prosecutions.

THE NATURE OF NATIONAL SECURITY

In most criminal cases, there is no involvement by government. Decisions by police officers are made independently and decisions by the Crown Prosecution Service are made in relation to the evidence and the public interest. The OSA, however, has a special provision that's supposed to protect us: the attorney general has to consent to these prosecutions. And Labour attorney generals have consented to the prosecution of Tony Geraghty, Nigel Wyld and David Shayler. That is a real problem if we believe in more openness and freedom of expression.

"This is the first conference I can think of on issues about national security and freedom of expression, and the parliamentarians that are supposed to support us."

We need to have a comprehensive review of the existing legislation, but not by government. People seem to be tainted by being involved in controlling the levers of power and to lose their liberal views once they get into power. Perhaps it's us who should be looking at the review of the OSA and the other laws. We also need a review of all ongoing prosecutions and convictions. There have only been two or three people who have ever been prosecuted and pleaded not guilty. Two of them are sitting here and both are free men so far, and I hope the same result will occur for David [Shayler].

One of the problems we've identified is the judges themselves. One would assume that if the executive was going to use draconian measures against individuals to suppress freedom of expression and that Parliament was failing to take its proper role to review the executive, that the judiciary would take a more robust approach. In the past our judges have not considered properly what national security means and in most cases have failed to address the merits of any particular case. I would hope the Human Rights Act [HRA] in future will make a difference and judges will be forced to confront the real issues, because someone needs to protect us from these draconian laws. And if it's not going to be the executive and it's not going to be Parliament, we may have to rely on the judges. That's a sad state of affairs. We should be looking for support from all of those branches, and so far we haven't got that.



David Shayler
EX-MI5

Thank you for allowing me to speak today. That's obviously a novelty for me because of the OSA. I have to

be very careful about what I say. England is supposedly a country of free speech, and yet if I say the wrong thing today I could be arrested by Special Branch and my bail rescinded. So that gives you an indication of how national security can affect us all.

I want to talk obviously in reference to my own case, which should be more than adequate to show that we don't have the right balance between freedom of expression and national security. Of course the state has a need to protect genuine secrets but the state has never defined national security in Britain. It seems to be an ever-lengthening or ever-shortening piece of elastic that is used when necessary to suppress free speech.

In my case, I tried to make a legal disclosure in July 1998 about an MI5-funded plot to assassinate [Libyan leader Moammar] Gadhafi. When the OSA was first drafted, I don't think people had protecting that kind of information in mind. They were trying to protect genuine state secrets, information that might identify sources or compromise sensitive operational techniques and ongoing operations. In the Gadhafi plot, we saw MI6 working beyond the control of government. And if they work beyond the control of governments they commit offences. Under the 1994 Intelligence Services Act, if they don't have permission, they are liable to the laws of the land in the same way you or I would be if we were to get involved in conspiracy to murder. Despite this, the government used the catchall of national security to have me thrown in prison in France, to arrest supporters of my campaign like Julie-Ann Davies, and to arrest my partner, Annie Machon, for criticising MI5 management.

I published an article in Punch about the failures in the run-up to the Bishopsgate attack in 1993. The article came out earlier this year, and the government decided to use the injunction against Punch for publishing the article and threatened the editor with prison. We should think very hard about a prime minister who wants to use the threat of prison against a journalist who is in fact behaving responsibly. In court the government didn't offer any evidence of damaged

national security, although after the prosecution had rested its case it did come running in with a document claiming to be an assessment by the attorney-general that national security had been damaged. It was ruled inadmissible because the prosecution had rested, and yet the judge still found in favour of the government over the free press. The point that John [Wadham] is making about judges being unfit to decide our liberties is proven by that.

I wonder why or how MI5 can claim that national security can be used to protect files dating back to 1909. The first file ever made by MI5 — PF #1 — is held on somebody called Vladimir Lenin. It's hardly a secret they'd have a file on him in the first place, and it's unclear why they need to protect that information now. When I was in MI5 they were talking about reforming the 100-year rule that generally protects all MI5 documents and extending it in 2009. I said, "How can you do this?" And they said, "It may compromise our operational techniques." Are they really still using the same techniques as in 1909?

"Of course the state has a need to protect genuine secrets but the state has never defined national security in Britain. It seems to be an ever-lengthening or ever-shortening piece of elastic that is used when necessary to suppress free speech."

I went to Parliament recently and was appalled by the lack of understanding of these issues — people trying to tell me what I'd done and what my motives were because they'd blindly followed off-the-record briefings from the intelligence services. This kind of thing verges on totalitarianism, but the only reason Parliament can get away with that is because the free press in this country doesn't make a song and dance when our rights are infringed. When the government tried to imprison the editor of Punch, The Guardian covered it but very few people made enough of a song and dance about it. I agree with John [Wadham] on this: I always thought the problem was 18 years of Conservative government. Now I think the problem is government per se. And until we have a proper Bill of Rights and a proper working definition of national security, it will always be used to suppress free speech.



Nick Wilkinson
*SECRETARY OF THE
D-NOTICE COMMITTEE*

I have a feeling that none of my predecessors would have thought it prudent to be on a panel in company like this. But I'm here because things are changing, especially on the D-Notice Committee, and because I personally believe we should have more openness.

I have a very strange job. I work in the no-man's land between two very powerful and normally battling armies: the army of officials and the army of the media. My job is to offer advice and sometimes to negotiate between these two armies. I have an office in the castle of officialdom and I can sometimes be privy to their Kafkaesque dealings and secrets. I'm not responsible to any government department and I do not therefore speak for them. I spend as much time with journalists as I do with officials. I'm responsible to an independent committee, 13 of whose 17 members are representatives of the media, and they are extremely protective of the independence of the committee and of my role as a servant of the committee and servant of the public.

The system is voluntary and I have no powers other than persuasion. The decision whether or not to use the system — and whether to publish — lies with the editor and the publisher. The standing defence advisory notices have been reduced to five and were again revised and made more limited earlier this year. The details are on the Internet and there's nothing mysterious about the system.

How in practice do I get involved? Either I myself become aware of something of potential interest — for example, in booksellers' guides or in breaking news stories — and I offer my services. Or a journalist or author gets in touch with me about something he or she intends to write or broadcast and asks for my advice or asks that I act as an intermediary with officials. Or an official learns of some potential story and asks me to act as an intermediary. In the latter case, I do not always agree to get involved. For example, I may consider the official is being unjustifiably secretive, or that it's a matter of embarrassment and not a matter of national security.

Which brings me to national security, a term that's frequently used as a justification or as an exemption for an act or a bill. The Official Secrets Act has been mentioned

THE NATURE OF NATIONAL SECURITY

already but there have been others too: the Prevention of Terrorism Act, the Data Protection Act, the Regulation of Investigatory Powers Act and the Freedom of Information Bill. National security is not defined anywhere, I think for two main reasons. The first is that government lawyers believe national security should be what they call an ambulatory concept, a general idea to be interpreted by the courts in the light of particular and unforeseeable circumstances, as they put it.

“...the fault is that of a patchy approach by most of the media to secrecy and freedom of information matters.”

The other main reason is that national security is difficult to define concisely and precisely — as the 13 experienced journalists and four senior civil servants on my committee found earlier this year when they tried to draft a definition to go with the revised defence advisory notices. In the end they fell back on the detailed areas described in the standing notices and they put these notices in a context of scale — namely, involving grave danger to the state. That deliberately excludes many issues covered by the Prevention of Terrorism Act. That's all very well, but that carefully circumscribed concept of national security only applies to the work of the D-Notice Committee and has no legal status. Nor is national security defined in the 1989 OSA, whereas the D-Notice criterion is that there be damage to national security and that applies to all my interventions.

What can be done to reduce the strife between officials and the media? You would expect me to believe that resolving disagreements between the two is best done using the D-Notice system — cheap, quick and precise — rather than going to law and risking blanket injunctions, police investigations and prosecutions. Failure by officials or by the media to use the D-Notice system usually ends in unnecessary unpleasantness. Of course, one could do without the D-Notice system but all that would do in the current climate is lead to more injunctions and more recourse to the legal system. I believe that in any area of media activity a voluntary system is preferable, that is, if the system is applied impartially and in a liberal-minded way and that is my aim.

We've heard about BSE secrecy. The OSA secrecy is of even longer standing — the Cold War habit of attempting to keep everything secret rather than just a very few things that really do need to be kept secret for the time being, as David [Shayler] has said, to prevent genuine damage to lives or to current or future operations.

There are faults on the media side, too — sometimes of sensational inaccuracy that makes officials even more bloody-minded. But, more seriously, the fault is that of a patchy approach by most of the media to secrecy and freedom of information matters. There are certainly some in Whitehall and Westminster who believe nobody outside the Guardian readership cares about freedom of information or reform of the OSA. However, both media and officials are well aware that the culture of secrecy is being challenged by a number of court cases and other events this autumn and through the spring. During this period, we shall possibly be in the run-up to a general election, and Parliament, government and officials are trying to cope with an unusually heavy legislative load. This is not the ideal scenario for calm, rational, open debate. Nevertheless, from where I sit it is clear that change is needed. We need to deal with matters of official secrecy, freedom of information and national security in a more mature and modern way. I therefore welcome discussions such as today's and look forward to helping push things along, both in open debate and behind the scenes.



Glenmore Trenear-Harvey
INTELRESEARCH

I do not and cannot speak for the security intelligence services, so if I'm cast on that side then it ain't necessarily so. I see myself as an interested member of Joe Public. The only involvement I'll admit with intelligence and security was with the misleadingly named organization, the Air Ministry Book Production and Distribution Centre. What we produced were codes and ciphers; I was also a courier. I am an interested enthusiast in intelligence and what I find fascinating is the strange dichotomy between the real world, where there's an immense amount of literature about security and

intelligence, and the Alice in Wonderland part of the government, where denial seems to be the main thing. It wasn't until May 6, 1992, that John Major confirmed the existence of the secret intelligence service, which was extraordinarily dopey because of the amount of literature that was there. The state has to protect genuine secrets, and in his role Nick [Wilkinson] has to ensure that no damage to national security will come about.

Now there is virtually nothing in the public domain that people can't get. If I can give a plug for John Young's Cryptome [www.cryptome.org], which seems to be a clearinghouse for everything that comes through, and the sites of Duncan Campbell [www.gn.apc.org/duncan/] and of the Federation of American Scientists [www.fas.org]. All these sites contain tremendous information and, through the Freedom of Information Act in the US, have great ease of access to information.

Like a lot of people, I thought that when New Labour came to power, with all their pre-election talk about a Freedom of Information Bill, things would free up. Forget defence for a minute; BSE is a prime example. One tends to think there are an awful lot of officials just covering their arses — that's the only reason they claim national security.

I have very mixed feelings about David Shayler; I think a lot of people do. I won't say he's a traitor, though I have called him a traitor in the past. As I have learned more about him I have shifted my position. He said the state has a need to protect genuine state secrets, but who is to determine what is genuine? I think that which, in a military sense, jeopardises troops in Kosovo or what we're doing in Sierra Leone. There are situations when whistleblowers who might be disgruntled over their terms and conditions or because their promotion prospects have been restricted don't just become moaning minnies in the mess but go public with that.

It's ludicrous that the NSA [National Security Agency], CIA and the myriad other intelligence services in the US seem to thrive, with Web sites, public relations officers and former intelligence officers going to local communities explaining their roles within national defence mechanisms. I would like to see something like that happen in this country, while still preserving that core of national secrecy.



Stephen Dorril
AUTHOR

The Labour Party, or the New Labour side at least, has a very authoritarian streak. If you look at

the [Tony] Benn diaries on the freedom of information campaign, he was surprised that the people supporting it back in 1976-77 were the ones that went off to the SDP [Social Democratic Party]. They were the libertarians. The people that remained in the Labour Party — [James] Callaghan, Jack Straw and the rest of them — were against what they regarded as something for the middle classes and not of any consequence for the country.

The Labour Party doesn't know how to deal with national security and the intelligence services. When I tried to get some policy statements out of Jack Straw, Robin Cook and Tony Blair before the general election, they passed the buck between them and said, "It's very interesting, we must do something." We never did hear what they were going to do. We now hear that Tony Blair doesn't even call the Prime Minister's Committee on Intelligence. It's as we always suspected — it's all just left up to officials. The politicians don't want anything to do with it; it's too embarrassing. They don't want to stand up in Parliament and take responsibility.

There is a whole range of laws relating to national security that have a direct impact on some people here in the audience. They also have an indirect impact: the culture of secrecy. Authors come under a lot of pressure to co-operate with the D-Notice Committee. Those authors that refuse have their books passed to the D-Notice Committee without their say-so. If they don't co-operate they are forced into highly expensive lawyering, often using lawyers the publishers insist on using who know very little about the OSA.

The D-Notice Committee is one of those strange half committees that's been in existence for nearly a century. It is in the ring of secrecy but not quite in it. It's been said that it's a voluntary organisation for publishers and editors, but as reporters and authors know, it's compulsory. The reporter has to go along with what the editor says. I dislike the hypocrisy that goes on in this area. It's okay for Christopher Andrew to publish a book that relies on information passed to him by MI6. Alan Judd has just published a biography of

THE NATURE OF NATIONAL SECURITY

the first director of MI6 that is based entirely on records from MI6, which he doesn't acknowledge in his book. It's okay for these people or anybody else within the ring to do this, but if anyone else does it, then the full weight of the law in various guises comes down on them.

There are a number of areas where there should be a counterbalance to the national security laws. One is oversight. The Intelligence and Security Committee isn't giving it, and I think the first area they should deal with is budgeting. The only way to have complete oversight of the security services is to control their budgets. If they do well, give them more money. If they don't, then you cut their budgets. We know from their latest reports that MI5/MI6 have refused access to look at their budgets.

“There is a whole range of laws relating to national security that have a direct impact on some people here in the audience. They also have an indirect impact: the culture of secrecy. Authors come under a lot of pressure to co-operate with the D-Notice Committee. Those authors that refuse have their books passed to the D-Notice Committee without their say-so.”

We need greater openness, a proper freedom of information act. Even the David Clark one, which received high praise, was far too restrictive. The test for a freedom of information act is: Would we come anywhere close to discovering the arms-to-Iraq scandal from the various versions of the FOI Act? We wouldn't. It does not cover defence, intelligence services and commercial interests. It would mean that we know no more about arms to Iraq than we do now.

We have to develop open-source intelligence. This century is going to be about open-source intelligence, and it's time agencies were set up that exploit the mass of information that's coming out. It's time to see intelligence officers operating like good journalists, and to cut the size of

agencies that deal with covert, secret areas to very small organisations. And we need committed backbenchers. No one in Parliament is taking up these issues. We used to have Tam Dalyell, Tony Benn, Ken Livingstone. [Labour MP Dale] Campbell-Savours has now been taken into the ring of secrecy as a member of the Intelligence and Security Committee. We also need more committed journalism. The committed journalists are here today but I think we have a problem with the younger generation of journalists. I lecture on journalism history and I'm struck by the deep cynicism of the students. They're cynical about the world, politics, about this whole area. Everybody lies, they don't trust anybody and they're cynical about journalism.

Finally, I'd just like to break the OSA, and this just shows the ridiculousness of it. Here are three things that are official secrets, which come from Richard Tomlinson. First, MI6 do have exploding suitcases; if you attempt to open one of their suitcases it implodes. Second, Richard Tomlinson was on the counter-proliferation desk. Thirdly, he was the only MI6 officer in the Balkans when he was there. Those three things I was not allowed to put in the book for some reason. It's ridiculous.

I'd like to read from a really good editorial in The Washington Post that also applies to Britain: “A newspaper, we admit, is hardly a neutral commentator on the question of leaks. We sometimes publish leaked information and our reporters solicit all kinds of material, some of it classified. There are good reasons why the US has never had an official secrets law, and those same reasons caution against adopting one. While some leaks harm national security, others serve to expose wrongdoing in government or to provide useful sunshine where government overclassification has needlessly kept citizens in the dark. Classification is sometimes used for no other purpose than to save the government from embarrassment. At the same time, high-level officials in every administration leak classified materials for tactical advantage. Leaks are part of the political system, one that is easy to decry but would quickly be missed if actually chilled.”

Discussion

Nick Radford (Sunday Times): Nick Wilkinson said he thought there should be more openness. Can I ask whether he has any specific measures in mind?

Nick Wilkinson: I've tried to make the D-Notice system more open, which is the limit of my powers. Behind the scenes, I can suggest to officials areas where I think secrecy is counterproductive to them, and that's what I'll continue to do.

Richard Norton-Taylor (The Guardian): National security is difficult to define, and it's being defined increasingly broadly, mostly by the courts. If you read from the Appeal Court ruling in the case of [Shafiq ur] Rehman — a sheik the government wanted to deport to India where he would have been treated badly — the Lord Chief Justice gives a new definition of national security: when an attack on an ally can undermine the security of this country. The promotion of terrorism against any state is capable of being a threat to our own national security. And finally the executive is bound to be in a better position to determine what policy should be adopted on national security than any tribunal, no matter how eminent.

John Wadham: Liberty, Article 19 and others support a much narrower definition, which says it's not national security unless its genuine purpose and demonstrable effect is to protect a country's existence or territorial integrity against the use or threat of force or its capacity to respond to the use of force, whether from an external source or an internal source to overthrow a government. That's a completely different kind of definition and it seems to go right to the heart of issues relating to national security. National security means the security of the state and that means there needs to be a threat to the security of the state. I understand there may be other issues that need to be protected, such as the lives of MI5/6 agents. But in relation to national security, it now means anything that connects on to issues relating to that, such as the Prevention of Terrorism Act, where individuals involved in animal rights activism or road protests or GM crop protesters are defined as terrorists.

David Shayler: Terrorism obviously isn't the same thing as national security, but the reason for the definition of terrorism being extended is in theory to further protect national security. At this year's Labour Party conference, Nelson Mandela got on the platform with Tony Blair. If we'd had the 1998 Prevention of Terrorism Act earlier, Mandela would be in prison. That's how extensive the PTA has become and it's ludicrous to suggest that threats to other countries are a

threat to us. There are many terrorist groups that would attack targets on the West Bank but would never dream of attacking British targets.

Stephen Dorril: It seems the reason we've got that definition of terrorism is pressure from the Americans. I can't see any other reason. We're the only country that supports the US on counter-terrorism policy. We're not threatened by outside terrorism. Most other European countries have cut back on their counter-terrorism budgets.

Robert Henderson: I want to address the complicity of the media in agreeing to suppress information when it isn't suiting their political purpose. In March 1997, Blair and his wife went to the police and tried to get me put in prison because I'd written a few letters to them. They failed miserably. They then sent Special Branch or MI5/6 to spy on me. For the last 3½ years I've been trying to get the media to cover this. Lobster bravely put out an article about this, and I've had one or two pieces in magazines like Right Now or Free Life and the Individual, but I cannot break the censorship. It's all right for the media to say the government is being suppressive. The truth of the matter is that the media is being suppressive.

Martin Bright (The Observer): I'd like to make a suggestion on this idea of media complicity. We do now have quite a robust chair of the Home Affairs Select Committee who has indicated that that committee should take control of the Intelligence and Security Committee. In the case against me and The Guardian, around 50 MPs signed an early day motion supporting me. I would be interested in finding out how we could get those MPs to put pressure on Robin Corbett and the Home Affairs Select Committee to have a proper inquiry of secrecy issues, perhaps via freedom of press issues.

Rasvan Roceanu (Radio Romania): I think we need to answer two questions: Do we feel the Cold War is over? Do we really feel the global clash of interests is over? If we don't really feel that, then one can explain the culture of secrecy. But if we feel that the real Cold War is over, then we cannot explain the culture of secrecy.

Duncan Campbell (investigative journalist): I was very impressed by the speaker from the D-Notice Committee. Twenty-two years ago I arrived at the New Statesman and found in my new desk a file of D-Notices stamped "secret." For the next six years I used them as guide for the best stories to go for. In 1982, I said, "Right,

THE NATURE OF NATIONAL SECURITY

we're going to publish them now." Then I got what every journalist dreams of — the dispatch rider coming round from the Ministry of Defence with the envelope with the official stamps. And he said, "This is terrible. How can you possibly dream of publishing such things?" But we went ahead. I do welcome the fact that you come here now, quite unlike so many of your predecessors, with a real understanding for civil society. In the US nine days ago, when Clinton refused to pass the Intelligence Authorisation Act, the position for all civil servants in the US was going to be that any classified information passed to any person without authority was going to attract a three-year prison sentence — very much like the British OSA of 1911 under which I was prosecuted 22 years ago. Had that act passed into law — or if it does under Bush Jr. — the position in the US has become the complete reverse of the UK. Because on that same day we knew that the trial of Nigel Wylde had come to an end on the test under British law of actual damage to defence issues, which didn't exist in US law. In the US law, there was no test for damage, only: Was the material classified and did the person know it? Had wisdom not prevailed and we had gone to court, I'm sure Nigel would have been thoroughly acquitted. Had he been in the same position in the US, under the act he would have gone to jail. There would have been no possibility of defence. My question is: If that law had passed, would the First Amendment have afforded no protection to an American Colonel Wylde?

Bob Haiman (Freedom Forum First Amendment Center, New York): I think the answer to your question is the one that you fear. The only intervention would be an approach to the US Supreme Court and then we'd see whether this act would be held to be constitutional. There's a great deal of interest in an election in the US at the moment. I am reminded by a column in a newspaper the other day about another election. In 1959 General Nathan Twining, head of Strategic Air Command, gave secret testimony to a Senate Foreign Relations Committee of which a young senator called John F. Kennedy was then a member. He had been lambasting the Eisenhower administration, claiming there was a missile gap between the US and the Soviet Union and they were about to leap far ahead of us. General Twining told the committee specifically that there was no missile gap, that the US could more than surpass the USSR and he proved it to Kennedy. Kennedy accepted Twining's statement but he continued to campaign on this missile gap and went on to win the election. General Twining could not step forward publicly and contradict Kennedy because he would have been dismissed from his position and gone to jail. The act that Bill Clinton vetoed would have extended this

kind of prohibition vastly beyond what it was then. I believe the US came very close to the edge of the precipice.

Laurence Lustgarten (law professor, Southampton University): Richard Norton-Taylor touched on the Rehman case, the significance of which is not well known. Islamophobia is creeping into the definition and understanding of national security, particularly in relation to deportation. I want to pick up on this because of what Stephen Dorril said about this being about American pressure, because it isn't. It's about the British government's conception of worldwide terrorism problems and therefore their understanding that they need to be in league with the governments of Pakistan and India and all the governments they deal with because of the perceived problem of Islamic terrorism in this country. We have therefore come to accept the definition of who is dangerous given by those military governments that we are no longer questioning. I think journalists are going to have to step outside the law and be the bold ones.

Phillip Knightley (author, *The First Casualty*): Has Mr Wilkinson seen the memoirs of [former MI5 chief] Stella Rimmington? Maybe you could tell us what's in them.

Nick Wilkinson: I have not seen them. The system is that memoirs of insiders or ex-insiders go straight to the agency or ministry involved, not through the D-Notice Committee.

Tim Gopsill (National Union of Journalists): The big cases the Labour government brought in the 1970s started with the deportation of [ex-CIA agent and author] Philip Agee under the national security provisions of the 1971 Immigration Act. People who are deported under these provisions are given no evidence of the charges against them. We need to remember that provision if we're going to talk about the unjust operations going unexposed by the media.

Alistair Brett (Sunday Times lawyer): What we should be concentrating on is getting a public-interest defence built into the OSA. It was a crap piece of legislation. It shouldn't have been brought in the first place, and the government must do something about it. There's always going to be a conflict between national security and cases where it is going to be in the public interest, and the public has a right to know what's going on. That's what we should be concentrating on.

Barry White (Campaign for Press and Broadcasting Freedom): Richard Ayre, former deputy chief executive of BBC News and former member of the D-

Notice Committee, has called on the media to end its support for the D-Notice system. He says that, in return for continuing its support of this discredited system, the media get nothing in return. Alerting the admiral to your scoop story won't even earn you a promise that you won't be prosecuted under the OSA. Worse, the very act of alerting the admiral and, through him, the spooks might lead the government to seek an injunction to prevent you publishing a story about which they otherwise would have been unaware. What is the panel's view of whether the media should cease its support for the D-Notice system?

Tony Geraghty: Will Admiral Wilkinson please confirm that some of his predecessors have not been as committed as he has been to an open game? They have covertly worked for agencies, including MI5 and the Ministry of Defence, without saying so.

Nigel Wylde: During the 23 months of my suspension from normal life, with the OSA case against me, I was largely kept out of affairs in the UK. The Americans have invited me to many a CIA conference at which I have been a guest lecturer and have been privy to some extraordinary events, including lunch with George Bush Sr. The reason I mention this is that the Republicans have gone to great lengths to publicise information about how the Cold War ended. We were given vast amounts of material that until 1992 was classified at very high levels and had the great "NOFOR" — No Foreigners — stamp all over it. They defined national security as a threat to the existence of the US. They were not interested in trivia. What they were looking at was a genuine and open threat to the US. Everything they said was sensible and was classified by paragraph so there was no blanket classification, as we have in this country — if you've got a sentence in the document that's secret, the whole document is secret regardless of the classification. The US system is more liberal, and I'm glad Clinton put his foot down to stop the draconian legislation going through.

John Wadham: I would take up Alistair's suggestion and say that we should have a campaign to reform the OSA, and I hope other people will join it. We need money, and the media need to put their hand in their pockets and help us.

David Shayler: The protection we have at the moment under the OSA makes it a crime to report a crime. If MI5 were planning to bump off Blair, it would be an offence for you to make the police aware of that. That should suggest to us that we've got the law totally wrong and it needs reform. On the D-Notice Committee: We need a proper committee

with a bit more teeth — a committee of MPs who would be some kind of intermediary between the intelligence service and perhaps journalists. The trouble is if you submit to them first you run the risk of an injunction later. In the US, it's impossible to take out prior restraint of the press, so unless we have that measure in place people will not submit information first because they fear prosecution and injunction. I agree with the idea of the free press leading the attack on the OSA. When I went on the record, I was amazed by the level of ignorance and arrogance and plain old bullying. I did what I did because I love my country and I am not traitor, but the OSA seems to want to make me a traitor.

Nick Wilkinson: To answer Tony's question, without doing a lot of research I can't tell you what my predecessors' views were. I hope that in the next two or three years the history of the D-Notice system will be written. Secondly, could we abolish the D-Notice Committee? Of course we could, but my own view is that this would lead to more injunctions. I can think of a couple of cases where had I not been involved the ministers concerned would have gone straight to court, and I don't think that's healthy. The revised notices offer a starting block for a definition of national security, and I still think a voluntary system is better than litigation.

Glenmore Trenear-Harvey: I have very simple suggestions before the FOI Bill is enacted: firstly, greater publicity given to the understanding of what is embraced by national security. I would also like to see Legoland [nickname for the newly built MI6 headquarters] across the water at Vauxhall Cross set up its own Web site and just put the information that is already in the public domain on it. I particularly like Stephen [Dorril]'s suggestion that we get greater interest from MPs on security issues. It does seem that very little attention is paid to these issues.

Stephen Dorril: Somebody mentioned complicity. There is complicity, but on a small level — little things like journalists who won't mention that their main source is an MI5 officer. Baroness Park, BBC governor, was often called a diplomat when she was in fact an MI6 officer. Somebody mentioned the Cold War: Yes, it is over, so why do we still need the OSA? To say a good word for journalists, they can't name agents because it can put lives at risk. The fact is that no MI5 or MI6 officer has lost his life in the past 50 years. They have a pretty easy existence. And finally, if there had been a proper complaints procedure we'd probably never have heard of Richard Tomlinson or David Shayler, and that's my recommendation: a proper complaints procedure that really works.

Panel 2:

British state security in Northern Ireland

Moderator:

Gary Gibbon (*Channel 4*)

Panel:

Tony Geraghty

(*author and Northern Ireland analyst*),

Andrew Puddephatt

(*Executive Director, Article 19*),

Alistair Brett

(*Sunday Times lawyer*),

Ruth Dudley Edwards

(*historian and author*)



Tony Geraghty
*AUTHOR AND NORTHERN
IRELAND ANALYST*

It's good to be here and at liberty.
Everybody here knows the recent

background — the knock on the door after my refusal to allow the D-Notice Committee access to my then-unpublished book about Ireland; the six Ministry of Defence [MoD] detectives, one of whom was a woman to look after my wife. Unfortunately she was wearing high heels and was somewhat disconcerted when my wife said she had to go out in the mud to look after the horse.

This was the beginning of a hallucinatory, Kafkaesque experience, one in which I had to direct the MoD police to the local police station, as they didn't know where it was. When we got there, the officer in charge of the station was unsure how to log me in. He said, "Tony, we don't get too many OSA cases in Leinster." So I said, "Try miscellaneous." And he replied that that was fine, and then they locked me up for a while and interrogated me.

It soon became apparent that I had caused embarrassment in my book. I had caused — in an exquisite phrase (the man who wrote it should have been an advertising copywriter) — "unquantified awkwardness," but no damage to military capability and no lives were at risk. It was clear from the outset that no crime had been committed.

After two years of investigation, expert testimony provided by Duncan Campbell and Brian Gladman essentially confirmed what the MoD had found during the first two days. What happened during those two years was constant pressure, intimidation, bullying not only of myself but also my publisher Harper Collins, whose offices were also raided. The book remained in the public domain on

BRITISH STATE SECURITY IN NORTHERN IRELAND



ALISTAIR BRETT, ANDREW PUDDEPHATT, GARY GIBBON, TONY GERAGHTY, RUTH DUDLEY EDWARDS

sale and yet, after some 12 months, a letter came from a Mr T Taylor, Special Secretariat Home and Special Forces, to my publishers, saying we strongly urge you not to print the paperback edition because it endangers national security. An additional incentive was an invitation to the head of the legal department at the publishers to go to Hammersmith police station and be questioned for four hours by the MoD police.

“In my view, Northern Ireland has polluted the body politic of the British mainland. It has done so as an unhappy conjunction of three historical factors. One was the guerrilla war against terrorism, the second was the evolution of computers as a means of surveillance, and the third was the lack of any constitutional safeguard to protect the civil liberties of the honest citizens of either the mainland or Northern Ireland.”

So here you get one part of the act with your arm twisted up your back and the other half saying we strongly urge you not to publish. I think the message is pretty clear. The intimidation succeeded in holding up publication of the paperback.

I first encountered that Kafkaesque strangeness while in Belfast in July 1970, while I was a Sunday Times correspondent during an illegal curfew imposed by the British army. I remember hearing a voice from a helicopter saying there was a curfew in force, so get off the streets, and a whole district was put under curfew. Those of us unwise enough to ignore this were put in handcuffs and nasty things followed. I shall never forget the corpse being dumped in the rain beside me and the soldiers making a joke about it. That experience was followed the next Monday morning by the announcement in Parliament that there had been no curfew, only a restriction of movement. It was this change of perception of reality that led me to report that the IRA were back in business because there was a “no go” area on the Lower Falls Road. This led me to be called back to London by the Sunday Times and court-martialled by the director of public relations for the army, who said it was nonsense to say there were “no go” areas in the UK.

So how do we arrive here? First, you should understand that the British army has, or had, a manual of deception. The manual is classified, of course. A further joy is that we must

BRITISH STATE SECURITY IN NORTHERN IRELAND

not show this plan telling you how to lie convincingly to female members of the army or members of the Royal Corps of Padres. The deception plan is often necessary in certain situations to save lives, but that is one element in the military mind that we don't understand. Diplomacy has been defined as lying for one's country and getting an OBE for it.

For the other element, we have to go back to the Second World War and Malaya. The strategy that evolved to fight that sort of campaign was to remove people from the villages and bring them under control in fortified settlements to contain them. Then you declared the settlement a free-fire zone, and you could go out and kill the guerrillas. The US tried the same process in Vietnam, with the fortified hamlet idea that did not work. Clearly with the onset of insurgency in Northern Ireland in 1969, that sort of physical control of hundreds of thousands of people was not an option even in spite of Bloody Sunday and the Amritsar approach of some generals.

The alternative emerged after a period of time, and it's what I call the electronic cage: tight surveillance of suspects, their extended families, neighbourhoods and supporters. It meant evolving a system using computers, cameras and covert human surveillance. It meant the targets could go nowhere without being contained. That was a necessary process in the war against terrorism — witness Omagh. However, like the war the French army fought in Algeria, the military were left to get on with their thing and the politicians averted their gaze. Then when it went wrong, they tried to scapegoat the soldiers. There has been a similar evolution in Northern Ireland.

In my view, Northern Ireland has polluted the body politic of the British mainland. It has done so as an unhappy conjunction of three historical factors. One was the guerrilla war against terrorism, the second was the evolution of computers as a means of surveillance, and the third was the lack of any constitutional safeguard to protect the civil liberties of the honest citizens of either the mainland or Northern Ireland. Those three came together with the military mindset, with the relinquishing of political control over how the war was fought. Those three things have produced a poison that has damaged us all. That is why our civil liberties are now under threat in this country, for example, through the RIP [Regulation of Investigatory Powers] Act.



Andrew Puddephatt
EXECUTIVE DIRECTOR,
ARTICLE 19

One of the most difficult things for a journalist to do is to cover conflict.

Wars these days aren't usually the outright things we saw in Kuwait or the Gulf. They're internal conflicts over disputed territory or jurisdictions where sovereignty is being challenged by a substantial minority or proportion of the population. Just think of Spain, Sri Lanka, Sierra Leone: This is the face of modern conflict and it's often intermittent, vicious and extremely confused. That describes the conflict that raged in Northern Ireland for around 30 years. In those kinds of conflicts, there's rarely, if ever, a military solution. The role of the state forces is to fight the insurgents to a standstill or some kind of stalemate, within which some constitutional settlement can be developed that embraces the sufficient interest of all parties to ensure a lasting peace. Again, that's more or less the situation in Northern Ireland.

“The hearts and minds of the population — who are usually the target of both state and insurgent forces — are won or lost depending on the media. Control of the media is essential to both sides. One of the characteristics of the conflict in the former Yugoslavia was that the fight for the media agenda was an integral part of the strategy of all combatants. That's partly why they conducted their operations to secure the right kind of international media coverage.”

The role of the media in covering that conflict is not that of a neutral vessel that conveys information in a free and open way about the issues and the nature of the conflict. The media are part of the conflict. The hearts and minds of the

population — who are usually the target of both state and insurgent forces — are won or lost depending on the media. Control of the media is essential to both sides. One of the characteristics of the conflict in the former Yugoslavia was that the fight for the media agenda was an integral part of the strategy of all combatants. That's partly why they conducted their operations to secure the right kind of international media coverage.

This was also true of the conflict in Northern Ireland, both in the operation of the army's press office and the Royal Ulster Constabulary [RUC] press office and also the Provisional IRA. Anyone who ever visited West Belfast in the 1980s was taken on what the Provos liked to call the scenic railway trip, where they took journalists and visitors to their highspots, from Bombay Street to Anderson's Town. Everybody's seeking to control the flow of information so members of the public see what people want us to see. There are two main reasons for this. One is the legitimate one of protecting the nature of the operations you're undertaking and the identity of the people you're working with. Often if you're in the state forces, you don't want people to know how far you've infiltrated paramilitary groups — these are highly sensitive pieces of information.

The second more problematic desire to control information comes because any revelations may compromise the image of the conflict you see as essential to your strategy to control. That's a wholly different problem for journalists to deal with and raises three problems. The first is the problem of truth. One of the characteristics of successful political conflicts worldwide is some kind of truth process or commission, where there isn't any justice as immunity is usually given to the combatants on all sides. So people who've been the victims of that conflict want to know the truth almost by way of compensation. The British government has recognised this need in the establishment of the Bloody Sunday inquiry, which is an important development as it was a very significant moment in the history of that conflict. We've also seen them demand of the IRA to know where the bodies of the people they murdered are secretly buried. That desire for openness is part of the same desire for truth.

But truth is not just the story of certain deaths. It's also about the nature of the conflict and its causes and management. That's why I think Tony's book doesn't just deal with the tactics; it also deals with the history of the Northern Ireland conflict. Here one of the key questions about Northern

Ireland was about the role of the state. Was the state, as is often portrayed in Britain, an impartial referee between two recalcitrant communities, where Britain was holding the ring without any strategic interest? Or was the state a participant in the conflict on one side with a very shadowy relationship with the combatants of one particular side, the loyalist paramilitaries? Answering that question seems as important as the understandable need to explain particular deaths. It's the attempt to control that second debate that is the reason Tony's book was so controversial, and why Liam Clarke is facing prosecution now.

“The second problem is the double standards of justice in the UK. The legal regime in Ireland and Britain began to separate some time in the 19th century. In Ireland there has always been a history of far more repressive legislation with regard to popular rights than there has been in Britain. That was understandably a feature of Northern Ireland.”

The second problem is the double standards of justice in the UK. The legal regime in Ireland and Britain began to separate some time in the 19th century. In Ireland there has always been a history of far more repressive legislation with regard to popular rights than there has been in Britain. That was understandably a feature of Northern Ireland. When it was partitioned, a substantial part of the population were there against their will and did not accept the legitimacy of that state. So there has always been emergency legislation in place of some kind or another.

An acceptance has grown up at official levels that you can run Northern Ireland in a way you would not dream of running anywhere else in the UK. You wouldn't dream of carrying out the same level of surveillance on the people of Britain that is routine in Northern Ireland. A senior policeman once showed me a map of Portadown, with the religious affiliations of every household indicated by green and/or orange. That's not a secret in Northern Ireland. I don't think

BRITISH STATE SECURITY IN NORTHERN IRELAND

there's anybody in Northern Ireland who doesn't know that's how the province is managed. But that is regarded by our masters as too shocking for the British population as a whole to be told. So we're not allowed to know that there's been this distinct police and military regime within Northern Ireland. As a citizen of the United Kingdom, I have a right to know how the UK as a whole is being covered, and no one should take that right away from me.

Thirdly, there's the problem of what Tony called pollution, which I would call contamination. Running a secret war requires some extraordinary things to be done, and there have been some extraordinary acts of heroism in that war. But equally if you look at the treatment of the Stevens inquiry, there's also been some unsavoury things conducted, in that case by agents of the state against other agents of the state carrying out a legitimate inquiry. The problem with draconian secrecy laws is they don't just cover up the necessary heroism, they cover up corruption, mismanagement and the breaking of laws and principles those agents are there to protect.

A thorough airing of the truth of what's going on in Northern Ireland is not only necessary for democracy as a whole in the UK, but also vital for the resumption of democracy in Northern Ireland itself. If we want to see a viable democratic culture developing in Northern Ireland, there has to be the basis that the truth can be told and talked about. This does not just apply to the state forces — truth isn't a one-way street — but also to what the paramilitaries did, particularly those that are represented in the current government of Northern Ireland. This is obviously why the truth is hard to get at, because none of the combatants ever wants the truth to be told afterwards. Whether that's the case in Northern Ireland — whether we allow that to happen or whether we say notwithstanding the interests of the new political government of Northern Ireland, the truth should be told — is an important question. Whether that can actually happen depends on a radical reform of the official secrecy regime of the United Kingdom, and until we change it fundamentally we will never be allowed to learn the truth of anything that's happened in such a sensitive area as Northern Ireland.



Alistair Brett
SUNDAY TIMES LAWYER

Liam Clarke has been writing about the Forces Research Unit [FRU — secret army intelligence squad]

over the past year, and we have had huge difficulties in getting into the public domain information the public has a right to know. For instance, should the public not be allowed to know that the FRU sent a team to burgle and then set on fire John Stevens' police office in Northern Ireland, because Stevens was about to find out about [FRU agent] Brian Nelson and what had been going on in collusion with the paramilitaries? We had huge difficulties getting that in the public domain, but luckily we got there.

But immediately what happens after that is that the Secretary of State for Defence goes to court to get an injunction under the laws of confidence, which is wheeled out time and time again in this country to silence the press. The government knows that after [Clive] Ponting¹, it daren't take anybody to court because with a good defence team you can get the charges dropped and the government can't afford a huge fiasco again. So what they're doing now is using the laws of confidence and silencing the press. Judges are establishment figures and they're prepared to err on the side of safety because of some bland general affidavit from some security man in the MoD.

We can't even name the people who've sworn affidavits in Liam's case. There is no danger of damage to national security because at the Sunday Times we are so careful not to put people's lives at risk. Liam was actually approached by "Martin Ingrams," his source, who said, "You're not being fair to the FRU. Northern Ireland is an incredibly dangerous place and you can't make an omelette without breaking eggs." He said not only do we need to protect and give information to the security services to try and police things in Northern Ireland. But equally, the military intelligence branch is breaking the law and that's how we got to publish what we had to publish.

¹ Clive Ponting was a senior Ministry of Defence official who passed documents to MPs on the sinking during the Falklands War of the Argentine ship, the General Belgrano, in which 323 Argentine sailors died. He was charged in 1985 under the Official Secrets Act, but acquitted by an Old Bailey jury.

BRITISH STATE SECURITY IN NORTHERN IRELAND

People need to bite the bullet on just how dangerous journalists' positions are in Northern Ireland. Liam's predecessor, Chris Ryder, had huge difficulties with the paramilitaries, IRA or UDA [Ulster Defence Association, the largest Protestant paramilitary group]. Very often they have to have personal protection weapons. Liam sent me a memo yesterday saying that when he was first talking to "Martin Ingrams," they had to buy pay-as-you-go phones, and that secondly he didn't want to know too much about agents acting for FRU. If he knew too much, he could be picked up.

"The government knows that after [Clive] Ponting¹, it daren't take anybody to court because with a good defence team you can get the charges dropped and the government can't afford a huge fiasco again. So what they're doing now is using the laws of confidence and silencing the press."

It's my job to help protect journalists and photographers. After the Trafalgar Square riots, the police hit us with a PACE [Police and Criminal Evidence Act] injunction to provide every single photograph our photographers had taken. I went to see [then editor of The Times] Simon Jenkins, who said the one thing the world's got to know is that my journalists are not coppers' narks. If they want photographs of all the people in the square, they've got to go through all the right hoops to get them because we don't want our journalists to be put at risk in the future by letting it be thought they work hand-in-glove with the police.

It is desperately important for papers to be a proper element in the whole equation of the executive. Our job is to seek after the truth and it really hurts when [Defence Secretary] Geoff Hoon wheels out these confidence injunctions all the time. I sincerely hope that one day he wheels out one too many and he'll be taken all the way because there is an issue here: Can the state honestly wheel out the OSA or the law of confidence to close down the exposure of iniquity and criminality by elements of the state, in this case the FRU?



Ruth Dudley Edwards
HISTORIAN AND AUTHOR

I am here under duress because nobody would come from the security forces and because it was

thought that I was slightly less hostile to them than most people here would be. I have absolutely no affiliations whatsoever. I have occasionally been accused of being MI5 or MI6 but that is the usual IRA tactic to discredit you because they don't like what you're saying and because they want to set you up as target. I have to be careful about what I say about the civil liberties and human-rights industry, because I see in the audience Gareth Pierce, who took £10,000 off the Sunday Times because of something I wrote about him several years back. I would have fought the case myself but the Sunday Times thinks that £10,000 is neither here nor there.

I find myself eternally torn on the rights and wrongs in this. I am at the moment caught between my belief in freedom of expression and the matter of protection of reputation, which is why I've just threatened to sue another journalist for malicious defamation. I don't like doing it. I do care about free speech but there are two sides to it. I worked for the government and I realise the government can be an ass, just as much as the law can be an ass. I also think that a democratic government has its own legitimacy. When John Wadham talks about New Labour being tainted by being in control of the levers of power, maybe he should consider that maybe they've acquired a little wisdom because they control the levers of power. Sometimes in opposition things are very straightforward. Sometimes in power they're not and everything is rather more difficult.

Freedom of information cuts two ways for historians. As an ex-civil servant I was very unhappy about the 50-year rule becoming a 30-year rule because I thought that if you're a civil servant of 24, you know that in 30 years the memos you're writing now will be available freely. With a freedom of information act, I don't think there will be enough information on the record; people will circumvent it. So don't be too sure; always remember the law of unintended consequences.

I would have been strongly opposed to any restriction of freedom of expression for representatives of terrorists. I was opposed to the Irish Section 31 [broadcasting ban on Sinn

BRITISH STATE SECURITY IN NORTHERN IRELAND

Fein], but I changed my mind. My mind was changed by the research I was doing into [19th-century British journalist] Walter Bagehot in the late 1980s. I came to the conclusion that he was right when, as a result of his experiences in the 1848 revolution in France, he said that order should come before liberty. In the end he said that the most important thing is that the fig seller can sell figs. That doesn't mean liberty isn't important, but it may not be the most important issue.

“You can argue that any decent solicitor in Northern Ireland doing their job is a human-rights lawyer. Just think about accepting propaganda — I'm saying this directly to the human rights/civil liberties lobby — don't be too gullible. Terrorists are smarter than you think.”

I am ferociously anti-terrorist in Northern Ireland or the United Kingdom because I don't think anybody has the right to kill because they're not getting their own way — and that goes for Republican terrorists or Loyalists. I am very uneasy about the way terrorists have used the law against two liberal governments. I am concerned about the victims of terrorism who, if they're at all aware of the human-rights industry, see it slanted against them. They believe nobody cares about the RUC man who was shot seven times in the back of the head; they're far more concerned with helping terrorists disband the RUC. That is how they see it. The RUC had 302 of its members murdered by terrorists and shot 50 people, and I think that's a pretty good record. The record of the security forces, with all their stupidities and occasional barbarities, is pretty good by the standards of any country.

When the victims look at the human-rights lawyers, I think they feel they are not running to back up ordinary law-abiding Northern Ireland citizens. I might be entirely wrong, and I apologise if I am, but did Liberty campaign for the right of the Orangemen to march their traditional route? I don't think they did, but they did rush to support [Sinn Féin leader] Gerry Adams because he was being forced to swear allegiance to the Queen. They do seem

keen to support terrorists or supporters of terrorists. There was a huge outcry when Michael Mansfield began to cross-examine traumatised RUC officers in a manner that caused deep offence to the victims because it seemed there was more concern in that corner of the world with the forces of law and order than with the perpetrators of the atrocity.

What's a human-rights lawyer? Was Pat Finucane a human-rights lawyer? Pat Finucane was an IRA member — does that make him a human-rights lawyer? Rosemary Nelson was a human-rights lawyer — why? Why was Edgar Graham, who was murdered by the IRA at Queen's University, not a human-rights lawyer? Who dictates what a human-rights lawyer is? Somebody who's on the side of Republicans. You can argue that any decent solicitor in Northern Ireland doing their job is a human-rights lawyer. Just think about accepting propaganda — I'm saying this directly to the human rights/civil liberties lobby — don't be too gullible. Terrorists are smarter than you think. It was terribly easy when Rosemary Nelson was foully murdered for HQ to announce collusion. They did within about an hour of the attack. You say collusion/human-rights lawyer, and the industry rushes to you.

Let's take Ken Livingstone. He is much loved in the activist part of the Irish community because he has always been an opponent of the Prevention of Terrorism Act. I was at an event during his mayoral campaign when he said that while he'd always been against that because it discriminated against the Irish, he couldn't say he was against the new broader act because he was aware of the international conspiracy of the KKK, European neo-Nazis, Italian Freemasons and retired army officers and police who are putting all our lives possibly at risk, and therefore there had to be wider terrorist legislation. So there are two sides to every story: One man's freedom fighter is another man's terrorist. The civil rights/human rights industry can be an ass.

² Pat Finucane was a nationalist lawyer shot dead in 1989 by Protestant paramilitaries. Rosemary Nelson was another prominent nationalist solicitor in Northern Ireland, shot and killed in 1999. Edgar Graham was a leading light in the Ulster Unionists and law lecturer at Queen's University in Belfast who was killed by the IRA in 1983.

Discussion

Gary Gibbon: Thanks Ruth for that wide-ranging and no doubt blood-boiling survey of the scene for some people here. I'd like to throw up another issue: Should the Labour government be posed as such a bogey? Isn't it throwing the door open with the HRA and the albeit limited FOI Act?



Nigel Wylde: I was one of the few people identified publicly because the BBC made a documentary about my tour. I watched the Protestants trying to kill each other and then trying to kill Catholics — ethnic cleansing, as we would know it today. I saw Catholics — and I'm not

hinting at any particular organisation — try to kill me. There are an awful lot of brave people who have been working in Northern Ireland and we are fed up with all the bad eggs. The people in the FRU who are my former colleagues had been in eastern Germany observing when they went back to Northern Ireland. They were horrified at what was going on, and the story that Liam brought out must be heard. I don't hold out hope that Lord Williams is the man to do this. He wrote to me saying he saw no purpose in a truth and reconciliation committee for Northern Ireland. Nothing over there is black and white, but the middle course is a very difficult way indeed.



Duncan Campbell: What struck me most when I became involved in Northern Ireland through Nigel's case was the ignorance among many journalists and army officers as to boundaries of secrecy — no realisation of what is and isn't secret and what is and isn't known.

Perhaps the most startling thing I found out from this case, not a secret at all, was about a little spot in South Armagh straddling the border, where the chief of staff for the IRA lives. On the two hills to the northeast and northwest are two enormous British army surveillance towers. Everybody knows they're there; it was no secret to anyone. Within the army one of the most extraordinary things was to see documents, classified confidential, that didn't even refer to MI5, because at the level of confidential MI5 was an organisation that didn't dare speak its name. But we have grown up: You can go to an MI5 Web site and get a complete report on divisional structure.

Glenmore Trenear-Harvey: There's a culture of senior military staff who are totally unaware of the capability of the Internet. There is a piece of surveillance equipment called Glutton that monitors vehicular movement, and there is detailed information about it on the Sinn Féin Web site, stuff that the Sunday Times couldn't publish. I have wry amusement at the concerns people have about information getting out, when it's already there.

“What struck me most when I became involved in Northern Ireland through Nigel's case was the ignorance among many journalists and army officers as to boundaries of secrecy — no realisation of what is and isn't secret and what is and isn't known.”

— Duncan Campbell

Tony Geraghty: I'm struck by the extent to which there is a dislocation between the apparent knowledge of the MoD and the knowledge that is already out there. This dislocation is illustrated by the lady using the nom de guerre “Susan George” who was given clearance to write about her time in 14 Company. The book was published, and two months later MoD sought an injunction to stop publication. The capriciousness of military censorship is growing exponentially. It has to do with nervousness and a style of information control set by this government. It has to do with the military habit of turning jobs over every couple of years. Such is the nature of the military mind that each new generation that takes over the regiment or office adopts a Pol Pot approach: This is Year Zero, nothing else matters. The result is total chaos and no consistency. The powers-that-be in Whitehall like it that way because we don't know where the rules are — which leads to self-censorship, which is exactly what is intended.

Tim Gopsill: I have slight sympathy with what Ruth said with the regard to the human-rights lobby because the industry did not take up the case of the Sunday People, which was trying to publish stories about collusion between military intelligence and the UDA in the killing of Catholics.

BRITISH STATE SECURITY IN NORTHERN IRELAND

They were subjected to the most extraordinary injunctions. The Northern Ireland editor of the Sunday People had written these stories and the injunctions prevented any mention of the security services or their agents in Northern Ireland. Anything they wanted to publish on the subject had to go to Mr Hoon first, three working days before publication. There was a series of hearings to try and get the injunctions lifted. The Sunday People did succeed in getting nearly all the injunctions lifted. The lesson is that the paper resisted and made a great song and dance about it, and the glare of publicity made the government back down. The point is that if the media defies the government, it will win. If it complies, it won't.

"...the military habit of turning jobs over every couple of years. Such is the nature of the military mind that each new generation that takes over the regiment or office adopts a Pol Pot approach: This is Year Zero, nothing else matters. The result is total chaos and no consistency."

— Tony Geraghty

Gary Gibbon: Tony, is there any sense that the Labour government is trying to curry favour with the intelligence establishment because there is a sense that they are outsiders?

Tony Geraghty: This government more than any other is keen to control the flow of information as a political asset. That goes along with the natural tendency of the military community to keep secret those things that don't necessarily need to be kept secret, and there is obviously a coalition of interests. What is different now is that because of the desire of this government to spin information, it has encouraged some in the military community to go one step further than they have done before. It seems we have a state within a state and a ministry that is out of control. I'm not in favour of the collective punishment of communities by the military without restraint of government. I'm not in favour of the

reckless use of firearms to murder people whose only offence is to demonstrate their political abhorrence. I do recognise that the security forces have a difficult job, but the problem is that the citizen has no redress, as we have no written constitution.

Ruth Dudley Edwards: I'm not in favour of collusion. I also don't think the security forces' record is impeccable. What I said was that I couldn't think of any security forces in any other country that would have done as restrained a job, and I can certainly say that as a citizen of the Republic of Ireland, where the Gardai would have taken such a rough approach if they could. But in Northern Ireland the system is inclined toward one direction — the Human Rights Commission, on which I have yet to find one person with a vague Unionist sympathy. It consistently shows no interest in paramilitary human-rights abuses, and that is wrong.

John Wadham: It's important that human-rights organisations make decisions that are neutral. We did represent Gerry Adams because it was a free-expression issue. Under the Prevention of Terrorism Act, he had been banned from attending a meeting in Parliament to speak about his concerns. We have also given advice to Loyalists who have been the subject of exclusion orders. Inevitably the state chooses who it wishes to victimise and charges them under the OSA, and so far the people that have come forward have been critical of the state. It's crucial that lawyers are available to represent people from both sides. I'm not saying everybody always gets it right.

Lawrence Lustgarten: I'm always amazed at the faith put in written constitutions. The Republic of Ireland has had one since 1937. I don't recognise Ruth's picture of the RUC, but I do accept that the Gardai are worse and having the constitution there hasn't made a difference. As long as we treat Northern Ireland as something "over there," we're never going to deal with this.

Andrew Puddephatt: I remember flying back from Belfast and sitting next to the Chairman of the Northern Ireland Confederation of British Industry. He asked me what I did, and I said I worked in human rights. And he said, "Oh, you're a Republican then." It wasn't said with any antagonism, he just regarded it as a given fact. I thought that said as much about the mindset of the political establishment in Northern Ireland as it did about the human-rights community. As it happened, I was flying back from a meeting with Ian Paisley Jr., and I was going back to London to attend a victims' rights group. There is a defensive

mindset in Northern Ireland, especially in the Protestant community, toward human rights and what it can offer, which is one of the obstacles to producing an integrated community.

Tony Geraghty: This has been a productive, interesting discussion of a situation for which there is no clear solution, except time. One of the seminal points turns on the degree of sympathy accorded both the security forces and the terrorists. I'm certainly no friend of terrorism. The kernel of this is whether we should expect the same level of amorality from the security services. We don't expect them to be angels, but they should be answerable to the rule of law.

“Somebody said that there is plenty of information around on Northern Ireland and that it's very easy to get, and that's true. But while there's plenty of information, there's very little free expression and that's the key problem.”

— Andrew Puddlephatt

Andrew Puddlephatt: Somebody said that there is plenty of information around on Northern Ireland and that it's very easy to get, and that's true. But while there's plenty of information, there's very little free expression and that's the key problem. That's why I would favour a truth process, but I don't think the combatants would want it.

Alistair Brett: It appears that Liam Clarke can't win — either he's exposing military intelligence for colluding with paramilitaries or he's accused of working too closely with MI5. Not only do the authorities bring confidence suits, they insist on all the documents staying under wraps. This isn't open justice. This is the beginnings of a totalitarian state, and we have to fight this kind of secrecy. As regards human rights, I think Article 10 [on freedom of expression] will help journalists get a fair and open trial under the HRA.

Ruth Dudley Edwards: I'd like to make a couple of corrections. The gentleman at the back talked about the taxpayer paying for state-sponsored terrorism. Well, they've been paying for Republican and Loyalist terrorism because they were all on the dole; maybe the Real IRA still are. I do not see it as balance to say, “Okay, I stuck up for Republican terrorists here and Loyalists here.” The balance I'm concerned about in Northern Ireland is the balance between democrats and terrorists, and I don't think there's been enough concern from the Islington armchair brigade for the law-abiding people of Northern Ireland. When Michael Stone³ got out of prison, it affected more law-abiding Protestants than the IRA getting out because they felt he had dishonoured them. I do not condone amorality by the state. I do not want to see any moral equivalence between the state and terrorists, but it's also wrong to handcuff the state against the danger of a terrorist threat. I agree with Andrew [Puddlephatt] in wanting a truth and reconciliation commission, but he's right that it's unlikely to happen.

³ Michael Stone, a member of the Ulster Freedom Fighters, killed three people at the 1988 Belfast funeral for three IRA members who had been shot by the security services in Gibraltar. He was released in July 2000 under the terms of the Good Friday Agreement.

Panel 3:

The Internet: circumvention of censorship?

Moderator:

Sheena McDonald (*Channel 4*)

Panel:

John Young

(*www.cryptome.org*),

Rohan Jayasekera

(*Web managing editor,*

Index on Censorship),

Phillip Virgo (*EURIM*),

Richard Norton-Taylor

(*The Guardian*),

Roger Darlington

(*Internet Watch Foundation*)



John Young

CRYPTOME

Cryptome was set up to publish what no one else will publish. It started off with cryptography

issues and spread to other things that are called dual-use technologies that are coming out of the intelligence field into the public domain. It is a public-education site with about 6,000 documents, designed to help people understand this technology. Some of it is known, some misunderstood, but it's coming on the market very fast, and the law is well behind the technology. Most people don't know what is used against them right now but they have a rough idea because once it was used against their enemies.

There are two developments taking place: One is commercialisation, the other is the use of it by domestic law-enforcement agencies. It's being fed to them from the national security people, and so more and more of it is being directed toward internal enemies. It's certainly happening in the United States, and that is not well known. We put up a document a couple of weeks ago of a speech by the Department of Justice, which said that we've got a window of opportunity to use this technology to develop an international police information-collection and sharing system before a law is passed against it. We will get this by the public because we'll spin the story our way; we need a PR campaign.

An interesting thing about the act Clinton recently vetoed was that they were the ones that sponsored the act, and the story of why he vetoed it is not yet known. The story

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?



ROHAN JAYASEKERA, JOHN YOUNG, SHEENA MCDONALD, RICHARD NORTON-TAYLOR, PHILLIP VIRGO, ROGER DARLINGTON

is that there's a covert version in effect that hasn't yet been publicised, and this might have been a stalking horse to see if they could get it through. If not, they'll do it another way. One of the ways is through technology, and the technology is not well understood because there's a fair amount of misinformation about its capabilities. We're publishing everything we can get our hands on because we're learning about it from people who work in the industry, who design and sell this technology to the law-enforcement agencies and to commercial organisations.

"We're not engineers, we just make this stuff available. That's all we do. We don't evaluate it. We get death threats and we get chastised for going too far — we are happy to go too far. We are disreputable on purpose. We know how this technology works, and the mainstream media are way behind us on this one."

One of the first things we realised when we got on the Internet was that it's one of the most fabulous surveillance systems ever invented, and right now it's far beyond the telephone or radio for tracking what people are doing. The capacity to store what people are doing on the Internet is slightly known, but there are a number of private individuals who are doing this as well as military intelligence people. And so one of the stories that has not yet been written is: Was it invented for this purpose? Was the commercial spin on the Internet merely to induce people to trust it and buy into it, to use it for private communication? This has happened very fast — in fact, some people think it has happened too fast.

Back to this question of technology leading the law in all nations right now. Most people in senior levels of government do not understand the technology and they're repeatedly misinformed about this. I can cite two or three new technologies that are just coming on to the market, one dealing with the gathering of electromagnetic radiation. Official agencies are putting out stories that this stuff really doesn't work, but in fact it does work very effectively, and it's one of the more interesting stories.

Who's going to leak this stuff? It's going to be people that are actually using it and who see it in action, not the official spokespeople of these agencies, who don't know what it's capable of. We're told that they are deliberately kept in the dark so they can tell the truth as far as they know it. We think

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

those people [who do know what they're talking about] will come out now, too, if they have a place they can send information anonymously. One of the best things about technology right now is that there are technologies where they can communicate with us in total anonymity. We had to learn all this ourselves. We're not engineers, we just make this stuff available. That's all we do. We don't evaluate it. We get death threats and we get chastised for going too far — we are happy to go too far. We are disreputable on purpose. We know how this technology works, and the mainstream media are way behind us on this one.

"We do expect to get false documents but it's not our job to sort that out. ...We like the really anarchistic approach to information: We get it, you decide."

Sheena McDonald: Without naming names, can you give me examples of the sort of people who share otherwise classified information with you?

John Young: Some folks are willing to be named, like the former Japanese security agent who leaked CIA documents. He was recently arrested, and released a few days ago. We don't know where some of the more controversial material came from.

Sheena McDonald: In May 1999, you published a list of MI6 agents. What have been the most embarrassing scoops for the American state?

John Young: That was the document that came from the Japanese fellow. Not being chauvinistic, but most Americans couldn't care less about British secrets. We watched the hits build up but then we found that it wasn't really secret. A lot of this stuff is out there; it's just not well known.

Sheena McDonald: Surely you're in danger of being sent viruses or infiltrated?

John Young: Perhaps. But don't forget we get a lot of people coming to us who have worked in the industry, ex-intelligence staff looking for work. There are a lot of people that either don't like what's going on or want to raise hell or they're in competition with someone else. We do expect to get false documents but it's not our job to sort that out — somebody else will do that. We like the really anarchistic approach to information: We get it, you decide.



Rohan Jayasekera
INDEX ON CENSORSHIP

When we first started looking seriously at the Internet all those Web centuries ago, we at Index on

Censorship quickly concluded it wasn't true to say — as a lot of people did — that the Web was impossible to censor. It was equally untrue that the Internet was anonymous, despite the great New Yorker line, "in cyberspace nobody knows you're a dog." Nevertheless, it was at least theoretically possible to make it both censor-proof and anonymous, and that there were plenty of people out there who were making it their business to have a go at it.

So we've been out there tracking the rolling war between the authorities and the anoraks. We're pleased to report that at the moment the anoraks have the edge. It's been a lucky thing for freedom of expression that cyberspace inherited its own iconoclastic culture of independence and free speech from its progenitors. It gave it a head start.

"So we've been out there tracking the rolling war between the authorities and the anoraks. We're pleased to report that at the moment the anoraks have the edge."

Where are the front lines? First, the Web site itself. In its basic form, it comes with a unique IP [Internet Protocol] address, a physical home in a real computer server — the computers that store and distribute information on the World Wide Web — in a real building owned by a real person, using a domain name registered by a person with a home address on public record. Plenty there for a secret policeman to start with. These numbers give the file data carried over the Internet a give-away identity that can be blocked at a gateway — if the gateways are controlled by a state, as in China or Kazakhstan, for example. Kazakhstan bars access to the international news service on www.eurasia.org, for example. It has blocked the site since Sept. 15 by sealing up access via the country's two state-run joint-stock telecom firms.

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

If you can't stop people dialling over the border for their connection — if international calls are allowed — then you can find out from one of the servers on the way who has been accessing what. Or you can just call round the surfer's home and check his browser history cache, then take a baseball bat to the computer itself. It's not only an issue in China or Syria. The Church of Scientology uses lawyers just as effectively to shut down critical sites that use church documents to underpin their charges, citing copyrighted property. Corporations are using the same techniques to silence employees, ex- or otherwise, who criticise their works online.

The same problems apply to the people posting the Web sites themselves. Plenty of rebel groups on the losing end of a government counteroffensive have found places to regroup in the virtual safety of cyberspace, but generally they have to do the html coding and uploading in physical security from Geneva or London. Yet still, for the specialist, there are several ways to track the path of the surfer back through the ether and to a real-world address. Internet activist John Gilmore's famous statement that "the Net treats censorship as damage and routes around it" is generally true, but the new routes taken are no less traceable. It's what computers do.

So, objective one: make the Web site and the route to it unidentifiable and anonymous. Index is one of two score groups and individuals who have offered up server space to a project set up by researchers at AT&T Labs called Publius, a new system that could go a long way toward eliminating online censorship. ("Publius," incidentally, was one of the pen names used by Alexander Hamilton and James Madison to anonymously publish the Federalist Papers [newspaper essays urging support for the proposed constitution] in revolutionary America.) It's not new — essentially it's a way of hiding the evidence that a particular server holds a certain file by splitting it up. Publius works by encrypting files — text, pictures or audiovisual files — and dividing them into fragments. Someone wanting to receive materials from the Publius network would look through a directory on a Publius-affiliated Web site; the network itself does the reassembling of the requested file.

The next bit of track-covering is hiding the path to the Publius-affiliated Web site, which will of course have its address logged by the forces of darkness. There are several sites that will do that for you. The current star is silentsurf.com, which disguises the site you are after, a system much beloved by people who spend time at the

office scanning Playboy online instead of working. Naturally, that address can be logged as well, which is why they offer up alternatives like banking2020.com.

Then there's the problem of covering your way in. Not much help in Syria, of course, but Web users on AOL and other major Internet service providers [ISPs] grant access via servers with dynamically assigned — i.e., random — IP addresses. Setting up new Internet accounts and e-mail addresses to use for a few days takes seconds to do, yet can slow down the investigators for days. You could always dial in from a Web café or via a mobile phone if you needed to be on the move.

But the best method out there at the moment is a system called Freedom, developed by the Canadian-based Zero Knowledge company. It uses multiple encrypted links to the desired servers and includes a secure connection to a local ISP running a Freedom server. Several are now operating in Britain. Similar to the Publius system, the message — re-encrypted each time it travels — is shared around several Freedom servers before being slipped into the Internet somewhere far away from the originator. The system used means that no one, including Zero Knowledge itself or your ISP, knows what messages are being sent or who is sending them.

The key to this is encryption. Present encryption on the Net is based on the fact that multiplication is easier than division. It uses two large prime numbers multiplied together to produce a "public key." One of the numbers becomes a "private key" — and only a person with that number will be able to decode the message. Thus, if you want to send something securely to one person, you use their public key to encrypt the message, and they use their private key to decrypt it.

Making a public key is simple, but cracking it to find the private key from it — that is, working out the divisors of a huge number that is the product of two roughly equal primes — defeats most computers. The larger the number, the longer it takes to search for the divisors. Hence, the "public padlock/private key" set-up is widely used on the Net, at least among those who use encryption. The system's main defence is the size of the prime numbers used to encode messages — basically, the bigger the prime, the longer it takes the computer to do the sums. This is also its main weakness: Computers follow "Moore's Law," i.e., double in computing power every 18 months. Keys that were uncrackable in a lifetime of computing five years ago can now be cracked, eventually, by the bigger and faster computers of today.

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

The British government is spending millions on arrays of supercomputers that can do the math to unravel these numbers — with the RIP Act in Jack Straw's pocket if the sums are too hard. But already there's a team up at De Montfort University that is working on an encryption system that will probably defeat the biggest and best computers for some years — a system that uses random permutations within multiple formulas called, appropriately enough, "chaotic encryption."

All these systems are easily found, if not always easily used. You have to have your anorak wrapped pretty tight to make full use of them. A note to passing venture capitalists: Index is toying with the idea of a service, accessible online, that would do all the preceding for those in need of protection from enemies of free speech, but in a more user-friendly manner. Call it a PSP — a privacy service provider — instead of an ISP.

That said, in all these exchanges there are humans at each end. Before you can encrypt a message to send to someone you have to get his or her public key. Likewise with chaotic encryption — sender and receiver have to "meet" online at some stage to synchronise their respective places in the coding and decoding algorithm. And when they meet, that's when the secret policemen will jump on them.

In any case, no matter how tight the system, if you get the encryption code, you are in. You can use lawyers, like the Church of Scientology and Jack Straw, or you can use other means. Which brings us back to the men with baseball bats and a more fundamental analysis of freedom of speech. I'm not unaware of the possibility that this well-meaning system could be abused. The Publius developers envisage that host-server managers like myself will take action to weed out child pornographers and supposed terrorists, but I'd like to wait and gauge the scale of the problem before I set up the Index IT department's censorship section. The project originators see its ideal user as a person in China observing abuses, on a day-to-day basis, of human rights. In nations where freedom of speech is severely limited and people might suffer great hardship for speaking out, Publius could be an instrument of social change. That's why Index is on board.

Secondly, there is the role of private business in all this. An entire industry has grown up to develop public-private key infrastructure for ordinary commerce. When you next go to the Index site to buy a subscription by credit card, you will

see the padlock icon in the bottom left-hand corner of your browser, and you will be using encryption. In the UK alone, the electronic-security trade is forecast to be worth the best part of £1 billion within three years.

Some people's eyebrows have been raised by the role of AT&T in the Publius project. Some skeptics have theorised that they might be the Trojan horse that will let the security services into the Publius fortress. I don't want to malign AT&T without evidence, but Duncan Campbell will testify to the close links between the telecoms industry and the secret services. All I can say is, let's look it over.

This is a war of sorts. Chinese journalist Qi Yanchen was sentenced to four years in prison on Sept. 19 in Hebei province. He was arrested in 1999 on charges of subversion relating to articles published in Hong Kong and on the Internet. But his May trial and sentencing were delayed, apparently to avoid coinciding with a US congressional vote on granting permanent normal trading relations with China. He was sentenced hours after Congress granted China that status.

But if you exclude the very many people jailed and/or tortured for pro-democracy activities on the Web, the casualties are virtual, like the war itself. Anoraks and secret policemen fight it out in cyberspace using ever more advanced technology, until a kind of stalemate sinks in and the war spills over into theatres — dangerous theatres — that it was never originally intended to reach. For the anoraks this means cover for pervers; for the secret policemen, it leads down the path to perversion of democracy and human rights in the form of vague law.

New regulations covering the Internet in China ban vaguely defined "state secrets" and any content deemed likely to "threaten social stability, Communist Party authority or harm ethnic unity." ISPs are expected to block any illegal or subversive content, and are required to keep a log of their subscribers' reading habits on the Internet — details to which the police can gain instant access. Only in China? The overall effect is not unlike the combination of Britain's own RIP Act and the precedent of the Demon Internet case, which makes the ISP liable for the actions of its clients. If you want to take the nuclear stand-off analogy to extremes, perhaps now is the time for Strategic Privacy Limitation Talks. Both sides could learn to live with a little more openness if the reward was a little more security of a more peaceful, democratic kind.



Phillip Virgo
EURIM

We need to put the whole of the Internet into context. Electronic commerce is around 100 years old.

The first legal case pertaining to whether a cable authorisation is a legal signature is more than 100 years old. The first encrypted signal was sent by [19th-century] General Henry Havelock in a telegram and it makes the point that PKI [Internet security software] is only one of a vast range of technologies. The Internet is only 10 per cent of the traffic being carried by electronic networks. One of the big problems in the RIP bill was that you had a whole raft of stuff driven by people who believed in PKI. It doesn't work very well — lots of people trying to flog lots of equipment to use it and then sell governments even more technology to try and read it. Most of this stuff isn't necessary, but there are a lot of people whose jobs and reputations would go if the technology worked well.

Back in 1997 it looked like everyone agreed there should be industry self-regulation that was properly organised and funded, and the application of the existing laws to the Internet should be clarified. A key part of the analysis then was the belief that only a small proportion of that content was either illegal or harmful. That may well still be true about the content. But when we're looking at the transactions, there are some interesting questions. One of the issues in recent years is that ordinary people use them and they don't want to get ripped off. When we launched our most recent exercise in July we were told that cybervandalism and fraud was costing even the best-run e-commerce operations about 4 per cent of turnover. Those less well run were losing about 40 per cent. One of the descriptions of the Internet is the Wild West without six guns, and that cybervandalism — like the "love bug" — is costing billions. It is a common situation for a bank to spend more on electronic security than it does on physical security. Visa said last year that the Internet accounted for 1 per cent of sales but 47 per cent of chargebacks.

Meanwhile, the enthusiasts say that your card details are far more at risk when you hand them over at a garage or restaurant. One of the big problems is that the focus of law enforcement is on attaining covert information about conventional criminals. But business is actually concerned about cybercrime, the crimes over the Internet itself. One of

the reasons for that split is that business has no particular reason to tell the police or the public what they're doing. They don't want to tell the public because they want people to have faith in the Internet. They don't tell the police because they don't know how to report this and the police don't know how to deal with this kind of thing anyway. The UK end of the G8 response force on international crime has fewer officers in post than would man the firewall of an average high-street bank. Any one of the UK's big financial institutions probably has more people looking after their electronic security than all the computer-crime units of all the civilian law-enforcement agencies in the country. Even in the US, with the love bug the FBI teams were dwarfed by the teams from industry.

"E-impersonation is soon going to be the most feared crime in the e-world and the punishment is global credit blacklisting - you could call it e-death."

Law and order — how's it coming to the Web? Just like it came to the Wild West, with little or no help from the government. The various telcos and ISPs that declined to help in a recent spamming attack were disconnected by their peers until they did help. Few of the big ISPs held out for more than a couple of hours. Meanwhile, you've got telcos and ISPs spending billions to try and upgrade their networks to provide prioritised, secure, authenticated communications, not just bandwidth. At the same time you've got banks and credit-card companies spending billions on authentication linked to some kind of guaranteed payment or delivery. Anonymity on the Web, even if you can achieve it, means you are an e-zombie, you have no credit, you can't actually buy anything. That's fine if all you want is confidential communication, but those who underwrite your payment not only know who you are but the biometrics that measure who you are. E-impersonation is soon going to be the most feared crime in the e-world and the punishment is global credit blacklisting — you could call it e-death.

One of the strands of debate on the RIP act was criticism from industry about giving priority to covert surveillance at almost any cost. Business is far more concerned about cybercrime, from the love bug through to very sophisticated imitations of the Web sites of well-known banks. You go into

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

this Web site all innocent, your transaction is forwarded but on the way all your details are stripped for future use. One of the most telling e-commerce campaigns earlier this year was the one on the London buses by BSkyB: "You can trust us. We're not the Internet."

The big issue is not whether the Internet is going to be controlled or not, because it already is. There certainly appears to be consensus across most of the business and political world that the same laws should be applied online as offline. How on Earth do you do that in a cross-border environment? There is no consensus among politicians, so it's up to the business community to get its solutions. There are two on offer. Will that handful of players — Cisco, IBM, et cetera, who effectively run the Internet — be promoting secure walled gardens governed by contract for the "moral majority." Are the forensic arms of the big accountancy firms and the investigation arms that control risks going to be paid by the banks to do a Wild West lawman job? Are we going to have networks of self-regulators working across frontiers to do what government can't do? Are the various agencies that have got the skills and resources going to make the transition to democratically accountable law enforcement or is the Internet going to polarise between regulated walled gardens with a cyber jungle outside that for predators and free thinkers alike?

In fact, all that will happen but the real question is when some of these are abused, as they will be, how do you get democratic accountability? And there it all depends what you're more concerned about. Freedom is freedom from what? Is it freedom from abuse by criminals, businesses or government agencies? And what are the priorities? And when we're dealing with geographical boundaries, one of the problems is that the priorities are different from country to country, and that's why governments can't find the solution themselves but end up rubber-stamping something provided for them. A lot of what's being touted at the moment doesn't actually work.

Sheena McDonald: Richard Norton-Taylor, you're one of our guides to democratic accountability. You live by paper — how do you use the Internet?



Richard Norton Taylor
THE GUARDIAN

Certainly for professional purposes to get information, but definitely not for anything in my personal life or finances. I'm going to be really brief and talk about RIP. When the government first introduced the bill it did so with breathtaking arrogance. It said it was merely bringing the Interception of Communications Act up to date with the technology, and that it will all be compatible with the HRA. Richard Shepherd MP says that the key proposal, whereby people hand over information, is like handing over to the police the keys to your home.

Now I'm pretty bad at technology, as I understand are most ministers and MPs. That ignorance is the point, in that the bill was very complicated and one is left being asked to trust the government and the ministers and security services to be sensible — an argument they've used in many other bills recently, including the PTA. So what does RIPA stand for? Certainly R.I.P. for privacy and another attempt to potentially control the free flow of information. Until now, GCHQ has been authorised to intercept domestic communication only if there is a suspicion of terrorist activity. Under RIP, they can trawl through domestic e-mails almost at will. Home Office Minister Steve Bassam admitted as much in a letter recently. Individuals and companies could be forced to hand over information and their keys in the interests of national security or to prevent or detect serious crime or in the interests of the UK's "economic well-being."

But this is not all. Keys would have to be disclosed if the information was necessary for the effective performance of any public authority in carrying out their duty or functions. The law never keeps up with technology and who does that benefit really — who gets round the law? The government says it's aimed primarily at pedophiles and drug dealers but aren't these the sort of people that will get round the law, not innocent and half-ignorant members of the public who will be caught in the net. There are a lot of uncertainties about this, too. Some people, maybe Admiral Wilkinson, would say that something on the Internet is not necessarily in the public domain, which is what a lot of government lawyers insist.

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?



Roger Darlington
*INTERNET WATCH
FOUNDATION*

I address you as chair of the Internet Watch Foundation, which was set up in 1996 by UK ISPs to combat criminal content on the UK Internet. By criminal content I mean, overwhelmingly, child pornography. If I had to put a single proposition to this very interesting conference, it would be that the Internet — of which I am both an intensive personal and business user — is nothing magical or mystical. Essentially it's a deliberate mechanism for news and views and related materials and to that extent conceptually is the same as newspapers, books, radio, TV, films. And therefore the laws that apply to those other mechanisms ought, as far as possible, to apply to the Internet.

Phillip Virgo has been talking about some of the civil issues that arise. As far as the Internet Watch Foundation is concerned, our concentration is exclusively in the criminal field and, most especially, in the field of child pornography. In this country that is a criminal offence and so technically any ISP that hosts such material is guilty of a criminal offence. Understandably, ISPs will say they can't possibly control that. And if they don't know, then they would argue they can't be prosecuted. The police have not really bought that argument and have put a lot of pressure on ISPs. In response the ISPs have set up IWF, which has a hotline where people can report material they believe to be criminal. If in our view that is the case, we advise ISPs to remove the material. In the time we've been in operation, more than 23,000 images of child pornography have been removed.

There are those who argue that the Internet is different and there ought not to be laws. That's not our view, and it's not the view of the government that supports us, and it's not the overwhelming view of citizens and Internet users. From every survey I've seen, they don't believe child porn should be freely traded within our national boundaries or across them. The creation of a child-pornographic image usually involves the abuse of a child, and I think society is right to act.

The model we've chosen to adopt is a self- or co-regulatory model, and that has been criticised from opposite sides of the spectrum. Children's groups and others say that we are not effective enough. Civil libertarians ask, who are we to be exercising quasi-judicial judgment without the need to go to court? Both would argue it would be better if we had a statutory body.

Firstly, you've just heard from Richard Norton-Taylor about the experiences of politicians legislating on the Internet. I put it to you that politicians have not shown themselves to be particularly familiar with the complexities of the technology and the sensitivities of the issues and therefore there is a lot to be said for a non-statutory model. Secondly, the Internet is an incredibly fast-moving area with many different dimensions. Our focus is very much on newsgroups, but there is concern about chat rooms, and the World Wide Web throws up its own problems, and I don't think any statutory model would be able to keep up.

Thirdly, we have a lot of co- or self-regulatory models in the British tradition, and I would argue that over the past three or four years IWF has done a good job. Having said that, if we argue for having to have co- or self-regulatory models or statutory controls, there is a serious obligation on such bodies to be as transparent as possible in the way in which they operate. When I was appointed as independent chair a year ago, the first thing I did was to put to the board that all the board papers should be published on our Web site immediately they are cleared and that has been the case for the past year.

Equally, I think our policies should be the subject of consultation and the widest possible support. Yesterday we published our first policy paper, which is on the central issue we have to address, that of child-pornography newsgroups. [It looked at] whether we continue with our present policy of asking for the removal of specific images we judge to be clearly illegal, or whether we adopt the policy of closing down newsgroups that regularly display offensive images, even if the majority of the content is legal. We have a responsibility to be open and discuss the issues, and that is why I'm here today.

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

Discussion

Sheena McDonald: It has been all too possible to intercept communications sent by e-mail. Julie-Ann Davies, would you like to tell us what happened to you?

Julie-Ann Davies: I'm not too sure what happened to me because Special Branch has never told me what I was supposed to have done. I was a mature student at Kingston University and a supporter of David Shayler's campaign, and I was in some kind of communication with David on the mailing list but nothing further. On March 6 [2000], Special Branch came into my lecture and I was arrested under Section 5 of the OSA. They said I'd been in receipt of information from David and circulated it, but I never had anything that wasn't already in the public domain. That's all the information I was given. They were intending to hold me incommunicado, but word got out of my arrest. I was held on police bail for six months, and my police bail was dropped the day David came back to the country. I was lucky because a friend of mine got in touch with a few people, and I did get a civil liberties lawyer. Otherwise I wouldn't have known where to start. My lawyer now is Gareth Pierce, and I'm taking legal action against the police.

Sheena McDonald: So you would fall into the category that Richard would call innocent and half-ignorant, which is what I would say most citizens are?

Julie-Ann Davies: There was a lot of belief in the media that it was because I'd originally leaked the document to a Web site. If they had bothered to look through the archive of the mailing list I'm on, they'd realise just how little I know about things like that. At that stage, I had no idea how to put up a Web page.

Sheena McDonald: Had you ever been in trouble with the police before?

Julie-Ann Davies: No, never.

David Shayler: This is a great example of how the law-enforcement agencies don't understand the Internet and how they've gone for Julie-Ann Davies for no good reason. I do happen to know how that document did get on the Internet, but I'm not at liberty to say. I can say that it was put on the Internet because people could not get a proper inquiry into the Gadhafi plot. If we had a proper system of open government, somebody could have taken

that document to an independent body and got the matter investigated. And from that, of course, there could have been criminal charges against two MI6 officers. I have to say I wasn't unhappy to see that document go on the Internet, because as far as I was concerned the general details were already known as I'd already talked about them. And the person that did [put it up on the Web] was obviously responsible because they blacked the names out so nobody in Libya would have any comeback.

I have to say I had a problem with the other document, dealing with Khalifa Bazelya, who was a member of Libyan intelligence and was let into the country by MI6 and subsequently expelled. I had a problem with that because it did name potential sources and some of them had families in Libya and they would have been open to reprisals. We have to be careful with the Internet. I realise it can do enormous damage to national security, but at the same time it does put the onus on the security forces to behave more responsibly.

Sheena McDonald: You said that if there were an independent body — is there such an organisation?

David Shayler: No. OSA is quite clear, in Section 1, that any disclosure by a former agent is illegal.

Sheena McDonald: What do you think of Cryptome?

David Shayler: They actually put the Bazelya document on the Internet. It was good because it confirmed that the security forces do at times let terrorists into the country in order to recruit them, and nobody ever gets to know about them when they get it wrong. So from that point of view, it was good. But I can't agree with the detail that was in it.

Duncan Campbell: I don't think you gave John [Young] enough credit. He started out as an architect with a social conscience, and his site is now regarded as one of the safest places in the world for safe leaking. Ten years ago we had the Spycatcher row, and to get the book in the public domain we had to go through this absurd process in the courts. If anything like that happens now, you can be sure it will be immediately available on John's site.

To take something else that was leaked, the list of names allegedly from Richard Tomlinson. I'm pretty clear how that got on the Internet — it's Tomlinson's list all right, but he

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

didn't put it there. We don't know whether Richard gave him the list or if he nicked it. But suppose it wasn't a list of names; suppose it was a recipe for making nerve gas in your back garden?

“Ten years ago we had the Spycatcher row, and to get the book in the public domain we had to go through this absurd process in the courts. If anything like that happens now, you can be sure it will be immediately available on John's site [www.cryptome.org].”

— Duncan Campbell

There was a chap at the Department of Trade and Industry, Nigel Hickson, who would come to all sorts of gatherings. This was in the time we were supposed to hand over all the keys we used for encryption. You could see through him that they were waiting for a great public outcry in which encryption had been used. They weren't interested in public interest; they were waiting for this disaster that never came. The Internet is a safe place for the ethical leaker who wants to go to John Young, now and in the future.

Sheena McDonald: John, do you heed copyright rules?

John Young: Usually not, as you well know.

Sheena McDonald: Well, exactly. Just one negative point: You're willing to publish other people's work.

John Young: We're always interested in what's going to happen to us. We always report phone calls and threats, but apart from temporary losses of service, we've not been shut down. We've taken measures. We bought a new server, split the site in two machines. One of the things about this is helping people to learn as we're learning on the fly.

Yes, the copyright issue does come up a lot. We don't consider ourselves to be bandits. The copyright issue is pretty big in the US, and we're right in the thick of it. It's about protection and ownership of information in a digital

world. It's a global issue that's being driven by technology. While I respect the work of anyone, I used to copyright my work as an architect and it never used to stop anyone using it. Right now the huge corporations are trying to control the Internet, but most of us who are interested in it couldn't care less about commerce. The US is one of the huge inventors and exporters, and thinks that copyright is one of the greatest tools of control and they learn to do this through the military. The criminalisation of information and the great concern with commerce misses the point that the Internet is about person-to-person communication.

Commerce is just a small piece of the Internet — one that's getting a large amount of attention — and law enforcement couldn't be happier. The Internet is not about commerce. The military has its own Internet, and they're using the public Internet as a cover for theirs — it's called Intel link and other things. They're using this superficial technology to develop a much more pervasive one. It's not secret, it's just not well known. If you follow the hacker links, you'll find all this. Our site has just become a portal for information. What happened to your site, David?

David Shayler: To give you an idea of how naive our law-enforcement agencies are at the moment: I offered all my information to the government and they didn't take it. I got so fed up lobbying that I threatened to post it on the Internet, and that was my idiocy. I warned them and they hacked into my site and I couldn't put up my information. I was subsequently arrested and put into prison for three months, but when I got out I managed to put my site up. Because people realised it was under threat, it was mirrored and the information was put on many other sites, and they still didn't take the information. I am now covered by the First Amendment, even though I'm not a US citizen. When I offered the information again they again acted repressively and wrote to American lawyers asking them to get the site taken down. But because of the constitution, we were made to look ridiculous. People are increasingly going to use the Internet to get stuff in the public domain, and once it's in the public domain it can appear in the British press.

John Wadham: I think the difficulty here is this dual approach to the state, because although most of us here are concerned about the activities of the state, the state isn't all bad. There are issues, such as privacy — things relating to one's private life should be private. International human rights isn't only about Article 10, it's also about Article 8 — the right to privacy. This is an important human right that needs to be respected, not just by governments with regard

THE INTERNET: CIRCUMVENTION OF CENSORSHIP?

to e-mails, phone calls and the like, but also by individuals. Imagine communications between myself and David Shayler and the tactics we're going to use in court: that information is very important to us, and if somebody gets hold of it and puts it on John's site, that seems to me to have little to do with freedom of expression. Not all publication is good. There needs to be balance.

"Imagine communication between myself and David Shayler and the tactics we're going to use in court: that information is very important to us, and if someone gets hold of it and puts it on John's site, that seems to me to have little to do with freedom of expression."

The problem with the Internet, it seems, is the problem of what the Internet is about. The government spins it to concentrate on criminals and pornographers. The problem — and we've had this discussion with IWF — is that we should be concerned with anything that harms children, but that's not what the law criminalises in this country. It criminalises images. If I draw a picture of a child and I possess that picture or I put it on the Internet for sexual purposes, then my possession of that image is a criminal offence and IWF is about controlling that as well. We need to distinguish between the images, pornography, and the issue of harm. Liberty has seen cases of people being arrested for possessing pictures of children on the beach. Some of those people had those images for sexual purposes, but the children were not harmed.

Richard Darlington: I'm afraid the images I've seen are not rough drawings or pictures of children on a beach, and I

don't really want to spend a lot of time investigating whether [the sexual acts depicted] were consensual or not. The issue is whether we treat the Internet as fundamentally different from other media, and our proposition is that we shouldn't. We need a more consistent approach from the media. The enforcement mechanisms have to be different because we're dealing with a global problem — 90 per cent of the material reported to us originates outside the UK. Regulating the Internet is not easy but it has to be done. Some people may exaggerate the dangers of the Internet. I believe that, overwhelmingly, it is a power for good. But we cannot deny that it is used for criminal purposes. And on the civil side, issues such as defamatory libel and breach of copyright are as real on the Internet as they are offline, and we have to address that.

Richard Norton-Taylor: I want to ask Nick Wilkinson what is in the public domain and what isn't, because there's a lot of confusion about that in some corners of Whitehall. They say that if stuff is put on the Internet, it isn't necessarily in the public domain.

Nick Wilkinson: If something is on the Internet, then it is obviously in the public domain. The only questions that then remain are: to what extent and for how long?

Phillip Virgo: Everybody talks about the digital world. In fact now, with optical cable, we're moving back into the analogue world. In that world, the volume of data that may or may not be information is growing at a rate of knots. The problem with it is that you're stuck with a 56-kps modem at best, with no prospect of anything better to come.

John Young: On copyright, because we respect artists, if we put something up that is copyrighted and a publisher contacts us and asks us to remove it, then we do so immediately.

Sheena McDonald: This is not a very tidy ending, because it's not a tidy subject.

What Price National Security was edited by Kelly Haggart, with photographs by Matthew Issep.
Designed by Lylaani Dixon and co-ordinated by Duncan Furey and Hilda Hatz.