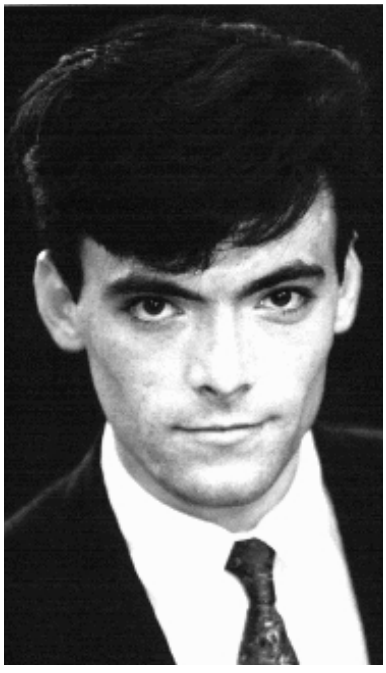
AGAINST THE CENSORSHIP OF ELECTRONIC COMMUNICATION:

A LIBERTARIAN ARGUMENT AGAINST ALL STATE INTERFERENCE IN THE PROVISION AND TRANSMISSION OF PORNOGRAPHIC IMAGERY ON DATA NETWORKS, COMPUTER BULLETIN BOARD SYSTEMS AND INFORMATION SERVICES, AND PUBLIC SWITCHED TELEPHONE SERVICES



RUSSELL WHITAKER

INTRODUCTION

We have been told that we, the inhabitants of Great Britain, are under the shadow of a massive peril: the threat of the corruption of our Youth and our Civic Order from sources outside our Isles, and now from within. Further, it is supposed that this threat flows like a miasma down our telephone lines, seeps into our nation's computers, and insinuates itself into the minds of our dearest little children, who would never otherwise have heard of sex. This threat is, of course, "pornography", the visual depiction of lewd acts that are never engaged in by right-thinking people such as ourselves.

However, I am opposed to this scaremongering. My argument rests on two principles: state control of the free flow of information is (a) immoral, and (b) impractical.

CONTROL OF THE FLOW OF INFORMATION IS IMMORAL

A favourite tool of the would-be controllers of the free flow of information is the moral panic. Raising their flags and proclaiming themselves the guardians of civic virtue, these self-elected arbiters of public morals have deemed that certain classes of information representation are sinful, and, furthermore, that Britons — themselves excluded, of course

Political Notes No. 91

ISSN 0267-7059 ISBN 1 85637 236 7

An occasional publication of the Libertarian Alliance, 25 Chapter Chambers, Esterbrooke Street, London SW1P 4NN
www.libertarian.co.uk email: admin@libertarian.co.uk

This publication was submitted in evidence to the Home Affairs Committee Inquiry on Computer Pornography, on behalf of the Libertarian Alliance, in October 1993.

As well as being the communications editor of *Extropy: The Journal of Transhumanist Thought*, and a director of the Extropy Institute, Russell Earl Whitaker was co-organizer of the First European Conference on Computers, Freedom and Privacy, held in London in November 1993.

— are not fully capable moral agents, and thus must be protected from themselves. Citing "crimes" of dubious existence, the controllers, through the blunt instrument of State edict, have classed certain textual and visual representations of information as intrinsically evil, and therefore illegal.

The libertarian position on this matter is unambiguous: the State is not entitled to hinder the free flow of data on any network, nor, for that matter, control within the borders of its proclaimed jurisdiction any image or representation, regardless of the medium employed.

This is an uncompromising position. The reasons for it are simple.

There exist no valid arguments to support the assertion of inherent criminality in the existence of an object, nor, for that matter, for the mere possession of that object. Crime inheres in positive actions, i.e. the imposition of force and the employment of objects as means to the attainment of criminal ends, where such objects enable the crime to take place.

A recent favourite statist tool of moral panic is the assertion of the existence of elusive consortia of child pornographers, who, in secret dens reminiscent of legends of white slavery, film ghastly sexual encounters of minors with adults, and market videotapes of these encounters to an equally elusive and mysterious black market of paedophiles.

While the author of this submission personally considers the depiction of adult sex with unconsenting children to be repugnant, he categorically rejects the proposition that the very existence of such images itself constitutes crime.

The terms of reference of the Home Affairs Committee Inquiry into Computer Pornography assume that pornography *per se* is some sort of evil. We see no reason why a non-coercive activity such as the enjoyment of sexually stimulating words or pictures should be considered a crime. Even if certain personal moral or religious codes should deem such enjoyment a sin or an evil, the enforcement of such forms of personal morality should not, in a liberal society, be the function of law.

The argument that pornography causes crimes or assaults is bogus, and has not been demonstrated by scientific evidence (See Thompson). Indeed, since human beings have free will, no evidence *could* exist which would demonstrate that individuals are "determined" by any such external force.

Since the moral and political arguments have been dealt with at greater length in the Submission by Feminists Against Censorship (See Carol) we have instead chosen to concentrate on those issues concerning the practicality of censorship of computer and electronic communications.

CONTROL OF THE FLOW OF INFORMATION IS IMPRACTICAL

In the most extreme case, given the supposition that sex with minor children is to be treated as an actionable offence under the law, it does not follow that the generation of images of such sexual acts is itself to be considered a criminal or civil offence. At worst, such images can only rightly be considered as *evidence* of criminality.

The mistake of assigning criminality to the image, rather than to the act, is made more evident by the fact that technology has now made it possible to generate photo-realistic renderings of events that have never taken place in this world. That is, there now exist a large and increasing number of computer software packages — once the province of Hollywood mainframes but now in the domain of the individual artist – that can produce images so breathtakingly realistic as to be utterly, seamlessly indistinguishable from real life. (This is used as a plot device in the recently released film *Rising Sun*).

These programs range from simple pixel-editing programs, which allow the user to create images from aggregations of small, coloured dots, to highly sophisticated "morphing" technology, in which an object — *any* object — can be made to look like any other object. With a morphing program, a motivated user could, for example turn an image of a pillar of salt into that of a full-grown woman. Or two lumps of coal into that woman's breasts. Or, for that matter, the image of a full-grown and full-bodied woman can very easily be made into that of a sylphlike and pre-pubescent schoolgirl — complete with strategically missing bits of school uniform. And, furthermore, she could be engaged in distinctly un-childlike action with a male Cabinet member who, in real life, never passed within two miles of the woman of the image's original provenance.

This "girl" never existed. The man never met the woman. Yet not only has a software representation of the hapless couple been generated but, in an interesting turn of events, someone has printed a colour negative of the image at very high resolution, and sent copies of prints of this image to New Scotland Yard by anonymous post, with an attached message that a ring of kiddie pornographers is operating in Britain.

This could happen. It may have already happened. Now, law enforcement is in an interesting position. Either it treats the image as the useful depiction of an actual event, as has been the case historically, or it questions the nature of the photograph. If the photograph is deemed possible evidence of sexual misconduct on the part of the Cabinet member, the police are put in the unenviable position of trying to identify the schoolgirl in question, before making moves to attempt a public prosecution.

Where to start? In a hypothetical near-future, an inspector turns to his computer console and, scanning the photograph into the police database, unwittingly attempts a photofit of the schoolgirl's face to images of schoolgirls from a National Identity Database recently mandated by a law and order Home Secretary. Unbeknown to the inspector, the face of the schoolgirl, originally that of the buxom woman, has also been altered: like the compromising event itself, which never in real life occurred, the face of the schoolgirl is a lie: in this case, a statistical composite of a very large number of images of different women ... and even a few effeminate men, from images earlier scanned from popular fashion magazines, for algorithmic variety.

The face is a fiction. There's probably not one like it anywhere around. Or, to make matters interesting, it's probably very much like any number of Essex schoolgirls around. A photofit might occur on a number of these schoolgirls. Arrests might be made, promising political careers may be destroyed, and utterly bewildered and inno-

cent schoolgirls may find themselves the victims of jarring state intrusions into their privacy and, furthermore, may become the unwilling wards of the state's "protective custody". This is not to mention the disposition of the parents in the matter. A strange tragedy, born of ignorance. And avoidable.

The days of conventional views on crime-fighting are over. And, for that matter, are those of conventional views on crime itself.

There are four categories of pornography in the UK:

1) Legal for adults to own and distribute;

2) Legal for adults to own but illegal to distribute;

3) Illegal to either own or distribute;

4) Legal for adults to both own and distribute but, crucially, illegal to distribute over the lines of public switched telephone networks, such as British Telecom and Mercury Communications.

This last category, of images classed fully legal to place on the top shelf of a newsagent's shop, or in a government licensed "sex shop", but illegal to send over a common carrier, is of particular interest here.

Modern telephone lines allow the passage of voice, fax, and data signals. Anyone who wishes to do so can buy a computer and a modem, connect the two to a telephone line, and call electronic computer bulletin boards anywhere in the world. Once logged on, a user can retrieve picture files which are not only "Legal for adults to own and distribute", as in category 1, above, but, quite frankly, are sometimes in categories 2 and 3, above. And never mind category 4: short of an electronic surveillance regime so intense as to make the former Iron Curtain police states look like the Land of the Free and Home of the Brave, there is simply no way of stopping it.

This is an absolute certainty. Short of physically quarantining the British Isles, and forbidding travel, trade, and communications — utterly — there is simply no way of stopping the flow of electronic images into Britain.

CHEAP AND SECURE ENCRYPTION

Even if every international telephone call were diverted through an electronic Customs Office, and screened for content — an outrageous breach of privacy, in any event — it's unlikely that even the most clever customs agent would be able to find anything criminal. This may sound an odd statement. However, in a series of interesting developments unforeseen by Establishment theorisers, the once closed domain of strong mathematical cryptography has been opened, with the publication and distribution of free "public key cryptography" computer programs, which allow for extremely secure communications over data networks and common carriers. Computers themselves were until not too many years ago the exclusive province of multi-million pound defence research establishments. They then spread throughout the world market. At today's best estimate there are approximately 150 million personal computers of far greater power than the old mainframes. The same sort of revolution is now occurring with computer networks. And with such networks we are also seeing the emergence of the phenomenon of widespread strong personal cryptography, allowing once and for all utterly secure communications. As mathematician Chuck Hammill has written:

> Updating now to the present [arguing from the analogy of the man-portable crossbow — REW], the public-key cipher (with a personal computer to run it) represents an equivalent quantum leap — in a defensive weapon [the crossbow used by a put-upon peasant versus an officious government knight: a tax collector — REW]. Not only can such a technique be used to protect sensitive data in one's own possession, but it can also permit two strangers to exchange information over an insecure communications channel — a wiretapped phone line, for example, or skywriting, for that matter) — without ever having previously met to exchange cipher keys. With a thousand-dollar computer, you can create a cipher that a multi-megabuck CRAY X-MP can't crack in a year. Within a few years, it should be economically feasible to similarly encrypt voice communications; soon after that, full-colour digitised video images. Technology will not only have made wiretapping obsolete, it will have totally demolished government's control over information transfer. (See Hammill)

These comments were made about 6 years ago. A crucial prediction therein has already come to pass: secure voice-grade commercial encryption is now commercially available. The most well-known standards, such as the GSM standard recently partially crippled by the security services (see Burroughes), are not the only ones. There exist stronger standards for encryption, which are being rapidly adopted for the manufacture of "homebrew" telephone kits, with none of the restrictions suffered by the commercial kit. And, in East Asian countries whose governments see the obvious advantages of secure business communications in such areas as banking data exchange these technologies are fast becoming commercial realities.

And with good reason, too. Software engineer and personal privacy advocate Phil Zimmermann, the author of the now-famous public key encryption program PGP ("Pretty Good Privacy"), has this to say about personal data security:

> Perhaps you think your E-mail is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? You must be a subversive or a drug dealer if you hide your mail inside envelopes. Or maybe a paranoid nut. Do law-abiding citizens have any need to encrypt their E-mail?
>
> What if everyone believed that law-abiding citizens should use postcards for their mail? If some brave soul tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world, because everyone protects most of their mail with envelopes. So no one draws suspicion by asserting their privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their E-mail, innocent or not, so that no one drew suspicion by asserting their E-mail

privacy with encryption. Think of it as a form of solidarity. (See Zimmerman)

This view runs counter to the popular — and wrong — public intuition that people who hide things "have something to hide". I, for one, wouldn't trust a public carrier which wouldn't allow me to say whatever I wanted secure from its paternalistic "good intentions". And clearly, if I have this capability, there's nothing to keep me — or anyone else with a computer and a modem — from sending encrypted representations of any image I care to transmit, anywhere, to anyone.

BACK TO THE THIRD WORLD?

And I certainly would not trust my banking details to a banking network that was security-crippled, and prevented from acting in the best interests of its clients by providing them with truly secure data links. The British government has no monopoly on computing power: if GCHQ, or for that matter, the American NSA (National Security Agency), can read sensitive data transmitted by relatively insecure DES (the US government's recommended commercial encryption standard), then so can anyone else with sufficient financial and computing resources, and with enough determination. This would be the effective result of Government attempts to impose a police state on communications. And this is just the beginning. There exists a worldwide, sprawling computer network known as the Internet, which comprises, according to several recent estimates, almost 2 million host computers, and somewhere between 18 and 25 million users. These figures are very rough approximations. According to Internet chronicler Paul Gilster, the current growth rate of the Internet is around 15 percent per month. This is a conservative estimate, based on figures given by the National Science Foundation Network Information Centre (NIC) in America. Other estimates put it higher. (See Gilster).

Internet is a network which started a mere decade ago. Economist George Gilder, in the recent 150th anniversary issue of *The Economist*, predicts that digital, multimedia computer networks will utterly replace today's telephony and centralised, state-controlled model of broadcast television within 10 years. Today's regulatory structures simply cannot cope with these changes, other than to attempt more interference, and thus cripple Britain in its future trade relations with other countries.

After all, when almost all business is conducted over extremely high-speed data links, and trade depends on unconditional security, what sane businessman would do business in a backwater country with crippled communications? Singapore, which is in many ways ahead of the U.K. in the employment of information technology, is finding itself in a similar situation: free up or be bypassed (see Gibson and Sandfort).

In an even more recent *Economist*, of 16 October 1993, it is noted that:

> Fibre-optic cables are producing a vast increase in the amount of bandwidth available. Made of glass so pure that a sheet of it 70 miles (110km) thick would be as clear as a window-pane, a solitary strand of optical fibre the width of a human hair can carry as much information as all radio frequencies put together. (See References)

This, by the way, is using today's technology. It probably comes as no great surprise that tomorrow's will be even more phenomenal. When gigabit data transmission networks become commonplace, information flow will become ever more intense, as information expands to fill the channels available to it. More information will be generated and transmitted in a typical business day than in all previous human history. A centralised government trying to monitor all of it will find itself in the position of a child trying to dam up a fire hose with a piece of tissue paper.

Attempts to crack down on the relatively minuscule portions of this bandwidth used for transmission of dirty pictures will be largely doomed to failure. Repeated attempts will lose Britain further international credibility. And desperate, last-ditch attempts, typical of governments whose efforts meet with failure, will knock Britain totally out of the running in the world market. Why should we be marched down another road to Third World status, anyway? We've already been down that road already, in the years preceding 1979.

REFERENCES

Anon., "Computer porn 'hurts female staff'", *The Independent*, 6 September 1993.

Anon., "No Hiding Place", *The Economist*, 7 August 1993, pp. 16-17.

Anon., "The tangled webs they weave", *The Economist*, 16 October 1993 Multimedia section, pp. 21-22, 26.

Tom Burroughes, "Snoop-proof phones' code stays secure, BT insists", *East Anglian Daily Times* (Business Scene section), p 3, 9 June 1993.

Tom Burroughes, "Spymasters pull plug on snoop-proof telephones", *The Times*, p. 5, 29 May 1993.

Avedon Carol, *Submission to the Home Affairs Inquiry into Computer Pornography*, Feminists Against Censorship, London, 1993.

William Gibson, "Disneyland With The Death Penalty", pp. 51-55, and Sandy Sandfort, "The Intelligent Island?", pp. 52-55, 116, *Wired*, September/October 1993.

Paul Gilster, *The Internet Navigator*, John Wiley, London, 1993, Chapter 2, "The Internet Defined".

Chuck Hammill, *From Crossbows to Cryptography: Thwarting the State Via Technology*, text of a speech given at the 1987 Future of Freedom conference in Culver City, California. Reprinted under the same title by the Libertarian Alliance, Scientific Notes No. 9, London, 1993.

Mitch Kapor, "Civil Liberties in Cyberspace", *Scientific American*, September 1991 (Special Issue) pp. 158-164.

William Thompson et al, *Soft-Core: A Content Analysis of Legally Available Pornography in Great Britain 1968-90 and the Implications of Aggression Research*, Department of Sociology, University of Reading, September, 1990.

Phil Zimmermann, *User's Manual*, PGP public key encryption program, latest versions of 1993.