Transcript of

Tales From The Crypt

(originally a radio documentary)

Written and produced by
Rosie Cross <rx1@sydgate.apana.org.au> &
Matthew Gream <M.Gream@uts.edu.au> *

Transcripted by Rosie Cross

July 1994

Foreward

"Tales from the Crypt" originally appeared on the Australian Broadcasting Corporation's (ABC) Radio National (RN) on Sunday June 12th 1994 at 8:30 pm as part of the "Radio Eye" documentary features section. Copies of the show, and many others, are made available by RN for a cost, please contact them for details.

The following contains the dialogue as spoken by the main talent, naturally in this "flat" medium, the special effects and exerpts that were used from other sources (ie. the movie "Sneakers" and "Get Smart") are lost.

Transcript

Phil Zimmermann:[1]
Cryptography is a very political technology Historically it is only used by governments.

Bill Caelli:[2]
Cryptography is defined essentially in the dictionary as the art and science of secret

[1] Phil Zimmermann <prz@acm.org> is a consulting software engineer, specialising in cryptography and data security. He is author of the electronic personal security phenomenan called "Pretty Good Privacy" (PGP).

[2] Bill Caelli <caelli@qut.edu.au> is head of the data communications school at the Queensland University of Technology. He currently chairs the data security workgroup within the International Federation of Information Processing (IFIP).

writing. It's all about scrambling information. It's a very ancient art practised by such people as Julius Caesar some two thousand years ago in ancient Rome and even before that in Mesopotamia and China. It's a whole concept of keeping messages secret between two parties who wish to converse privately.

Professor Dorothy Denning:[3]
Our ability to break codes has had major impact on how wars have proceeded and how well we've done and so on, and so it's not just a game. This is serious business for governments.

Phil Zimmermann:
The forerunners of modern computers were invented mainly to solve cryptographic problems.

Bill Caelli:
During the war, the second World War, in Germany particularly, a particular machine was used called an Enigma machine. The machine itself rather resembled a large portable typewriter. As they typed in each letter of what we call the plain text message - that's the message you want to keep secret - a light would come up under another letter on the keyboard. So the Enigma machine is what we call an encrypting, or scrambling machine which was used to scramble messages in such a way that if letters or groups of letters were the same, appeared many times in the message, then indeed the same type of text or encrypted message would not come out. Indeed, one of the very first computers developed by a famous man in computing, Alan Turing, was used in the early days in a place called Betchley Park to decipher some of these machines.

Rosie Cross *(lead)*:
Cryptography, having been used in wartime, became a powerful weapon for international intelligence agencies. During the Cold War they armed themselves with the means to spy and monitor communications, exclusively holding the key to secret codes. This control became chaotic in the seventies with the birth of Public-key cryptography. New mathematical algorithms enabled a break from One-key cryptography. New systems allowed for two keys, private and public. The Public-key could be widely distributed, while the Private-key was well guarded by the owner. This ability to communicate in unbreakable codes has caused concern and posed a major problem for governments.

Phil Zimmermann:
Today we live in the information age where everyone has a personal computer and a modem and it's just getting more and more like that, so there's a need for people to send data back and forth for ordinary commerce, for private electronic mail, and you can't send electronic mail privately unless you use encryption. Paper mail is sent in envelopes. Generally speaking, most people don't send their paper mail on postcards, but with electronic mail it's like sending it on a postcard. If you don't want people to read your electronic mail then you have to encrypt it, otherwise your electronic mail passes from computer to computer across the internet and can be intercepted and read by anyone along the way, including governments. So for us to protect the health of democracy and innoculate the body politic against possible government abuses in the future, I felt that we should be building a technology infrastructure that has secure electronic mail.

[3] Dorothy Denning `<denning@cs.georgetown.edu>` is chair of Computer Science at Georgetown University, USA. She authored the popular reference book "Cryptography and Data Security' and sits on the Clipper Chip review committee.

Rosie Cross *(script)*:
Phil Zimmermann designs cryptographic software which provides an envelope for electronic mail. PGP, or Pretty Good Privacy is being used extensively here in Australia and has become a worldwide defacto standard. The popularity of Phil Zimmermann's product has him in trouble with the Feds in the USA.

Phil Zimmermann:
Pretty Good Privacy, or PGP as we call it, is a program that runs on a personal computer that encrypts electronic mail, letting you send electronic mail to people that you've never met without the prior exchange of encrypting keys. It uses a technology called Public-key cryptography to do this. It has spread all around the world - it has become a worldwide defacto standard for the encryption of electronic mail. I am currently under criminal investigations because our government here in the US, has laws against the export of encryption software. They regard it as ammunitions. The State Department, sort of like our Foreign Ministry here, has rules about exporting munitions. They have a munitions list. Anything on the munitions list can only be exported with a licence from the State Department, and encryption software is one of the items on the munitions list. They generally don't grant licences for the export of encryption software so much of the exported encryption software is weak, in other words, it can be easily broken by the government. PGP is strong cryptography, so there's not much chance of them granting an export licence for PGP. But because PGP was published as free software, it just spread all over the place and was all over the United States in a very short time. And it didn't take long for it to spread overseas after thousands of people in the US had it and people just started giving it to their friends, and they gave it to their friends, and pretty soon, somehow, it got overseas. Our government is taking the position that the electronic publication of PGP is the same thing as exporting it, so that's why I'm under criminal investigation. Maria Cantwell our national representative from Washington, where Microsoft has its headquarters, has introduced legislation that would lift all the export controls on encryption software, but the NSA is against such a law. They want to keep the export controls in place. The mission of the NSA (National Security Agency) is signals intelligence, and that's something that they still want to preserve as their mission, and if widespread encryption software becomes available then they're afraid that they won't be able to decipher as much traffic. We need stronger encryption methods and PGP is a stronger encryption method, but we need those encryption methods to become more widely available to make people's private business communications safe from major governments. There's more governments than just the US government to be concerned about here. The French government is notorious for using their national technical means to listen in on conversations and supply that information to their own domestic businesses. The Internet has potential for decentralising power to some extent. There are social structures arising on the Internet that are unique to Internet. It's possible to have digital cash that's non-traceable. Transactions could be conducted using cryptography on the Internet. There's all kinds of interesting social experiments that could be unfolding now.

Roger Clarke:[4]
Well, the problem with the Internet is that unlike the telephone, which is extremely hard to analyse automatically – you've got to have people sitting,listening, it's an extraordinarily expensive and difficult exercise - with electronic mail you have stream of ASCII data, and ASCII data is analysable in real time by any machine

[4] Roger Clarke `<Roger.Clarke@anu.edu.au>` is reader in information systems at the Australian National University. He is also speaker for the Australian Computer Society and author of many papers on the impact of information technology to society.

that is plugged in on the network that happens to be owned by the CIA or ASIO or whichever other agency plugs itself in. What that means is that the occurrence of more than three words which are deemed to be seditious or deemed to be indicitive of terrorist activity or drug dealings or whatever, the computer program clicks over and your message goes into a pile, and therefore the name of the sender and the name of the recipient goes into a pile of people we've had reason to monitor in the past. It's that kind of suspicion building which can be automated, through what I call data-veillence, those are the real fears of text messaging as opposed to voice messaging. The idea of these spook agencies is that they need to be more efficient in the same way that every government agency needs to be more efficient in its use of taxpayers money. In order to do that, what they have to do is automate their surveillence. They can at present, on the budget they've got, only subject a relatively small number of people to surveillence because they have to have people physically sitting, listening to telephone calls. By having a computer system that will do that for them, and will throw exceptions out in front of their operational staff, they're able to spread their surveillence net much wider. Now if it were physically possible to write surveillence algorithms such that it only pulled out the crooks and the cheats we'd all be delighted. Unfortunately, there are many conversations which mention nasty words like sedition and drugs and Aunt Sally and brown bags and all those other key words that are fed in – well I've just mentioned them so I'm sorry but our conversation, if we were doing it in text, is now in that data base. You're in that data base and I'm in that data base under suspicion because of the usages of words in a message.

Phil Zimmermann:
Well, I just got some electronic mail last week from a reporter in Bangkok who is in contact with some political opposition groups in Burma using PGP, and they're being taught to use it in jungle traing camps in portable computers, and they're taking that knowledge and training others in other jungle training camps and it's helping morale over there. Major governments have cryptography, but now it's possible for disempowered groups to have cryptography as good as that used by major governments. Someone in Latvia sent me this e-mail on the day Boris Yeltsin was showing his parliament building in October; "Phil, I wish you to know what it never be, but if dictatorship takes over Russia, your PGP is widespread from Baltic to Far East now and will help democratic people if necessary.Thanks." Singapore, for example, I can easily imagine embracing the Clipper Chip, with the kind of society that Singapore has where they're already a surveillence society with video cameras and electronic monitoring devices and financial transaction monitoring everywhere, putting Clipper into that kind of society would be easy to do. If in those countries they don't have enough citizen opposition, then there is the danger that Clipper could spread horizontally around the world and would thus become entrenched as an international standard.

Professor Dorothy Denning:
Public-key cryptography has two great advantages. One is that it's provided in with the mechanism for digital signatures, which are extremely valuable, especially as we're going to use networks more for electronic commerce and the other thing is that it's given us a way of exchanging secret keys which are the keys used for encryption. So it provides a way of disseminating those and exchanging those so that you can then carry on your secure communications.

Rosie Cross *(question)*:
Are you opposed to people like Phil Zimmermann releasing something like PGP. Do you think that's a good standard that most people should adopt?

Professor Dorothy Denning:
Oh, no, that's not, I don't think it's a standard that most people should adopt. First of all it dosen't solve my criteria for user friendliness. The average people are not going to use any kind of encryption unless they can basically get it with the push of a button and that's all they have to do. Right now using this system is considerably more complicated than that.

Rosie Cross *(script)***:**
Professor Dorothy Denning, is a world leading cryptographer. She's also a reveiwer of the Clipper system, a system designed by the US government's National Security Agency – the NSA. Intended to increase it's surveillence potential now and for future communications, the Clipper Chip has received great opposition from business and civil liberties groups, although Professor Denning defends the governments position to control the keys.

Professor Dorothy Denning:
We need Clipper Chip because, first of all, what we'd all like to have is a secure way of communicating, and so this will provide that secure way of communicating on the telephone, which is what it's really designed for, and doesn't require a lot of effort on the part of people to use it. So in doing all that, as a society I think we want to do it in a way so that what we won't do is end up creating a safe haven for criminals to conspire and undertake criminal activity in a way that shuts out law enforcement. Clipper is used to secure your telephone communications and the *chip* would be embedded in a device, and you'd basically just, you know, push a button on the device saying phone secure and the person on the other end would do the same and then the communications would get encrypted. And what it will do is scramble up all the communication so if somebody is listening in they won't be able to understand what you're saying. At the same time the chip will put out some information, such that if the government has a court order to do a wire tap of the communications, they're able to get access to encryption keys that will allow them to get access also to the communication. Each device has a secret key and when the device is manufactured the key is split into two parts, and then when the government has their court order, those two parts are loaded into a device which will then combine them and then decrypt the communications on the channel. And so the Clipper chip will ensure that if people are using this encryption scheme, they won't be able to use it counter to the interests of society.

Rosie Cross *(script)***:**
Opposing Dorothy Denning and the Clinton Administration's struggle to sell Clipper to the people, groups like Computer Professionals for Social Responsibility actively campaign to inform the public on issues of privacy. Policy analyst, David Banisar explains the impact that proposed surveillence technology is having in America.

David Banisar:[5]
CPSR is a membership group mostly made up of computer scientists and others in the computer industry. We started originally looking at the social implications of using computers for military purposes. Star Wars was one notable example of stuff we worked on back in the early eighties. Since then we've moved on and are now looking at how generally the technology affects society. In this particular office in Washington DC, we look at civil liberties issues - how technology affects privacy and how technology affects free speech. There's a lot of people out there opposing

[5] David Banisar `<banisar@cpsr.org>` is policy analyst for the Electronic Privacy Information Centre (EPIC), he was with CPSR at the time of this documentary.

Clipper. In fact with exception of your previous interviewee, nobody is supporting Clipper out there. American industry is almost universally against it. The civil liberties groups all oppose it, even the international industry has been strongly opposed to it. The international chamber of commerce came out against it fairly recently.

Rosie Cross *(question)***:**
Do you think Dorothy has a point at all? And if she doesn't, why doesn't she?

David Banisar:
Well, I think the difference between Dorothy's position and ours is the basic difference in how we feel the relationship between a government and its people is. She is willing to trust the government to act within its lawful behaviours and to always act in the best interest. Whereas we take a slightly more sceptical view of the world. There's a couple of problems depending on which perspective- from a privacy perspective it's that the government is asking us to give them the equivalent of us giving them our house keys and then trusting them not to break in and drink our liquor when we're not there. From a technological standpoint it's a real nightmare for companies or anybody who wants to do real security to have to implement this chip into all their products. The other from a purely technical standpoint is that most companies nowadays, whether they're hardware companies or software companies, are writing things in software. They write a program and if they screw up the program they can just start over again, they can replace the software with new software. If you build something into your system with hardware, it's going to cost a lot more because you have to build all the necessary circuits that go into it. But in addition, if it's bad, if it goes wrong somehow, if it gets compromised, you're going to have to throw the whole thing out and start over again with a new piece of hardware rather than just simply reprogramming. In reality Clipper has been around for at least four years. It was started under the Bush Administration and they were probably thinking about it under the Reagan Administration. Under the Reagan Administration there was some pretty widespread domestic surveillence here. People that opposed his plans in Central America were constantly being spied on, and also regular library users. The FBI was going to lots of libraries and saying , if you have a foriegn name then we want to know if you're reading anything we don't think you should be.

Professor Dorothy Denning:
I think that's just nonsense and it comes from a lack of understanding of the people who say that about what kind of threats are really out there, and it's true that the threats have changed over time but that doesn't mean that they're not there. The threat of international organised crime, for example, is becoming more a serious problem globally, and to the extent that we can't effectively deal with it in our country, it's going to become a more serious problem here as well. Wire taps have been one of the key tools that have been used to deal with organised crime. Wire taps and other methods of electronic surveillence as I understand it have been used in all the major organised crime cases here, and so if we lose that capability, potentially we could suffer some really devastating consequences, I think, in our effectiveness in dealing with international organised crime, which is going to create a situation worldwide. Another area is terrorism, and there again I believe wire taps, I heard were used in over 90% of those cases.

David Banisar:
Terrorists won't use it in the first place. If they're smart enough to use an encryption device, they're going to be smart enough not to use that one. So basically it's only

going to be the people who can't afford anything better who are going to use Clipper.

Rosie Cross *(script)*:
Also sceptical of the government and Dorothy Denning's position on Clipper is John Perry Barlow from the Electronic Frontier Foundation. He believes the technology is open to abuse.

John Perry Barlow:[6]
Government is by its nature inclined to invade all the possible spaces of control that it can get its hands on.

Professor Dorothy Denning:
Based on everything I've seen so far, I think that the control will be extremely good, and I consider that that risk is going to be acceptably low. I think it will be very hard for somebody either in or outside the government to conduct an illegal wire tap with Clipper. There's a lot of auditing features so that also what you'll be able to do is trace back from the release of a key all the way back to whose line was actually tapped with that.

John Perry Barlow:
Dorothy has a lot more faith in the morality of government with unlimited power than I do. She seems to think that existing legal restraints on the spook houses and the FBI are going to be sufficient to hold them from unehtical behaviour, even after they've reached the ability to automatically monitor the transactions of just about everybody who uses communications. The National Security apparatus in the USA grew up during the course of the Cold War to be one of the fundamental elements of the economy. There are thousands of people who make their car payments on the basis of a threat which somehow no longer exists, so in the absence of that threat they've had no choice but to ferment new ones.

Ted Nelson:
I have probably as many conspiracy theories as most people, but conspiracies do exist after all. Clipper chip, yes indeed. The Clipper chip is a complete phony because in fact it would be very easy to defeat the Clipper chip so that even if it is in the equipment the government can't read it, simply by encrypting the message a couple of times beforehand, creating a scramble that the government cannot read by the same method. The ostensible purpose to make it possible for the Feds to read everyone's transmissions is total bullshit since they would not be able to read the transmissions of anyone who cared. The genuine purpose has to be and can only be to create a situation where they can search and seize on suspicion of conspiracy to encrypt. And it will give them the right to sieze the computers and possessions of anyone who is under suspicion of encrypting.

John Perry Barlow:
Well, I don't believe in conspiracies. I believe that what is generally regarded to be conspiracy is simply the automatically united endeavours of various forms of self interest. I mean you don't require a conspiracy to see that there are people that want to enhance governmental control for their own institutional purposes. These large agencies are like organisms and they want to survive and they want to have as much control as they can possibly get.

[6] John Perry Barlow `<barlow@eff.org>` is co-founder of the Electronic Frontier Foundation (EFF) and sometimes lyricist for the Grateful Dead. He spends most of his time lobbying and working on electronic issues.

Rosie Cross *(question)*:
How do we know the cypherpunks can't be accused of the same thing? ;)

John Perry Barlow:
Well the cypherpunks seem to be trying to create a situation where control is simply not possible to anybody.

Rosie Cross *(question)*:
David Banisar, I'm wondering if you're a good person to ask this . What is a cypherpunk and what do they do?

David Banisar:
They tend to believe that cryptography is the solution to all of our problems. I'm a little scepitical of that particular scenario myself, but they are very active in discussing among themselves technical solutions for various problems such as Clipper. I mean, cryptography is the tool that can be used to solve some privacy problems, but it doesn't solve all of them. It can certainly be used to make communications secure, but it doesn't secure us from government bureaucracies ordering us to give information to them and them matching that information among themselves or passing it on, or doesn't keep businesses from doing the same. Just as right now you can use a fifty dollar bill when you go out to a restaurant, and there's no transaction data which can be collected and looked at, cryptography can be used to create a digital cash which can do the same. The same will also work for intelligence vehicle highway systems – it can be used to protect medical records on smart cards a variety of ways, which is being developed by a researcher named David Chaum in Amsterdam.

David Chaum:[7]
DigiCash is a company developing what's called pre-paid smart cards/systems where its value is stored on a card or in your computer and then is used to make low value payments. And if you lose your money you can get it back, you can always prove that you made a certain payment, but no-one can find out who you paid unless you agree. So you retain that ability to withhold who you are making payments to, but still the systems are auditable and thats very unattractive compared to paper money or other means for use in any kind of illicit activity. Just like the pre-paid smart card which is being launched in Sydney - I believe you can use that card to pay for all kinds of incidental things like pay phones, vending machines, purchases at point of sale, still preserving your anonymity - so in a way that allows the entity you're paying to receive the money but without allowing them also to discover your identity.

David Banisar:
There is a lot of different definitions of privacy, but anonymity, clearly the right to not have to identify yourself wherever you go and leave a trail for whatever you have done is a key part of privacy. You know, the right to be left alone, to not always be accountable for everything you did. If you go to a grocery store and buy a six pack, is there a reason for *them* to have that information, and is there a reason for a big data base somewhere to collect that you bought a six pack on Monday and a twelve pack on Tuesday, which maybe you bought for your neighbour anyway.

Bill Caelli:

[7] David Chaum `<chaum@digicash.nl>` owner of DigiCash, a startup selling electronic cash and related systems. He is founder of the International Cryptographic Association for Research (ICAR).

In Australia I suppose we have a whole pile of things happening and I don't see the same as I do in the United States. First of all, one, we've already permitted a form of scrambling between a mobile telephone, the GSM telephone, and the base station. That's called an A5 cypher. Now that is not a crypo-type cypher at all. That is a cypher which doesn't have a back door to it at all. Now that's in operation right now if you're using your GSM telephone, between the handset and your base station - now, note that, not between the base station and say a telephone in an office, but at least between the handset and the base station - the radio part of it is actually scrambled using the A5 cypher. Any form of cable tv which, for example, the ABC may take part in, will use encryption. Otherwise there'll be no way of charging for those programs. In other words, normally what happens in a cable tv service is that the signal coming down from the cable system is scrambled and people pay money per month to get the unscrambling capability. Now, so encryption or scrambling is the only way we know of technically to provide security, privacy, integrity,authenticity, all of those services we need once we move to computer and telecommunications networks. There's no other techniques known. Cryptography is our tool of trade for providing those security services we need in telecommunications, computer systems and the telecommunications network. May I say, for example, the much hyped superhighway of the future will absolutely depend upon cryptography.

Roger Clarke:
I don't think people have a clue what the word cryptography means. Before you rang back I was thinking , how do I popularize the notion of cryptography, and I thought, well there are ways to do it because essentially what the Clipper chip is trying to say is that the government has the right to say that you're allowed to speak any of the following – English, Spanish, Pidgeon, or Tagalog because we've got native speakers of all those languages who monitor your lines. But you're not allowed to speak Slavinian, Hindustani or any of these other ones because we don't have a translator handy, and it's not good if we can't intercept and listen to what you're saying. That's the essence of what the cryptography argument is about – the government dictating what form of communication mechanisms we can use and what kind of garbling we're allowed to impose. Now remember there's a technical issues as well. The Clipper chip is designed to work in the US telephone system, and remeber it's still a telephone chip at this stage. There isn't yet a chip for handling data communication, there is proposed to be one. Now the Australian telephone system , as I understand it, is rather different technically to the US one, therefore I suspect that particular chip might not work, but the design would. All they'd have to do would be to change the interfacing and build a slightly different chip that would interface the Australian system, but the pattern I'm sure would work. The important point about the particular cryptographice scheme that's used is that the spooks agencies have got the ability to crack the cryptography, so they can listen in but nobody else can, so the theory goes, and that's probably going to be the practise as well. It probably will be for practicle purposes, uncrackable. If they were in a position to totally impose that on every telephone in the United States, or from our viewpoint, on every telephone in Australia, then I'd be much more concerned, but at this stage that is not what they're proposing. They're proposing that it is a standard which may be used by government agencies in the United States. So it seems like a reasonably soft argument at the moment.

Professor Jennifer Seberry:[8]

[8] Jennifer Seberry <jennie@osiris.cs.uow.edu.au> founded the Centre for Communication Security Research in 1988 and has been Director ever since. She is coauthor of the reference book

I believe the Clipper chip is taking an atomic bomb to a situation which may need a drop of antiseptic. Another issue that isn't addressed in all of this is the cost issue, that you have to buy the Clipper chip from an American company. You have to buy in American dollars. Say it cost you one thousand American dollars, for example, well there's a lot of little people out there who do not want to spend a thousand dollors or little companies, small businesses for whom buying this one, and then when it's upgraded three years later they have to buy another one, there's no standards and they're always following behind, so it's a financial burden on those smaller users. It's a thing which is going to be easy for big business, big organisations and big brother, but it is counter to the interests of the small people, and I think that we've got to think through these issues a lot more carefully before we accept technology from another government, which is set up for their own situation and which is hotly contested in their own country.

Trudi McIntosh:[9]
My name is Trudi McIntosh . I am a high technology and multi-media writer for the national paper, The Australian. I'm also a contributing editor for the national magazine, MIS. I cover all areas from the latest Hollywood multi-media deals being signed right through to the Clipper chip scenario and data security issues. ... At the moment , unless we start using the information that we're collecting and spreading it across our networks, we face a very strong threat from the thriving Asia-Pacific region countries who are doing very nicely out of this. Countries like Taiwan, Japan, China are certainly very far ahead of Australia, and all indicators seem to suggest that they will stay that way!

Professor Jennifer Seberry:
I will give you an example of how we may be missing the boat. The Japanese developed their own indigenous encryption algorithm which they call FEAL. FEAL was presented at international conferences and it was broken, so they put out a new version, and that was broken, and they put out a new version and it's getting a bit harder to break, but everybody said, aren't the Japanese stupid, you know, they're putting out their algorithms and everybody's breaking them. But lots of us felt, aren't they smart. They just put out their algorithms and they get the best people in the world to find out what what's wrong with them for free. Well, the Japanese, having got a version of FEAL now which is in all of their products, but while we were preoccupied with our own problems, the Japanese have gone and sold it. They've sold it to all of the Middle East, they've sold it to the whole of Africa. They went into new and different markets. Australia could have had that. We've developed encryption in this centre, but we can't get it approved for export in any version at all.

Trudi McIntosh:
Rumours coming out of Canberra indicate that Canberra is very wary of the hostile reaction that the Clipper chip debate has already received in America. The American public is not happy about it one iota. The days of it being introduced are still very far off. In fact, I don't think it will get off the ground. I think it's going to collapse.

Roger Clarke:
Yes, things are done through the back door and there is this phenomenom called function creep. Once you get something useful like the Tax-File Number in, then

"Cryptography: An introduction to computer security".

[9] Trudi McIntosh is a multimedia reporter for the newspaper "The Australian" and contributing editor for the "MIS" magazine.

you'd want to use it for something else wouldn't you. It would be very easy to justify. So, yes, there are fears like that, but I think we've got to avoid painting the government as a bunch of devils from beginning to end. There are some things the government needs to do. Let's look at it from another perspective. On behalf of Australian patients, let's say, I'm concerned to ensure that as the Health Communications network in Australia develops that there be suitable privacy protection embodied in it which means encrypting data travelling along telephone lines. So I'm quite pleased if governements are thinking seriously about getting encryption working in places where encryption should work. The idea that governments should actually establish an encryption scheme for themselves isn't of itself a bad thing, it's how they do it. It's how much they impose on the populace with it and it's the extent to which they create the scope for a future totalitarian government to repress individual's thinking and speaking. They're the real issues.