TALES FROM THE CRYPT

by Rosie Cross and Matthew Gream ■ Illustration by Ian Haig

PRIVACY ON THE NET IS UNDER ATTACK, AND THE INTELLIGENCE COMMUNITY – WORRIED ABOUT NET USAGE BY TERRORISTS AND ORGANISED CRIME – IS LEADING THE CHARGE, SEEKING TO EAVESDROP ON ALL ELECTRONIC MAIL. BUT WILL THE TECHNOLOGY FOR ELECTRONIC WIRETAPPING BE USED TO 'PRESERVE AND PROTECT' SOCIETY OR THREATEN THE WIDE OPEN DEMOCRATIC SPACES OF CYBERSPACE?

PHIL ZIMMERMANN

PHIL ZIMMERMANN IS IN HOT WATER WITH THE FBI. HE IS ACCUSED OF DELIBERATELY EXPORTING SOFTWARE THE FEDS CONSIDER DANGEROUS TO THE NATIONAL INTEREST AND, IF CONVICTED, FACES FOUR YEARS JAIL FOR HIS TROUBLE.

Zimmermann's PGP (Pretty Good Privacy) software flies in the face of the Clinton Administration's plans to introduce key escrow encryption – known as the Clipper Chip – a proposed 'public key' encryption system designed by the U.S. government's National Security Agency to be implanted in every American phone, fax and modem.

In effect, Clipper is a hardware system which would act as a listening device, allowing federal agencies authorised by the attorney general to effectively wire tap most forms of electronic information. Purportedly 16 million times stronger than the existing federal standard, DES, the Clipper Chip has become the centre of a furious debate between government officials and civil liberty organisations. The alternative to the government's eavesdropping is 'private key' cryptography, such as PGP, disguising messages in ways that evade the prying eyes of the State and spook agencies.

Cryptography, the science of secret writing, dates back some 2,000 years to Caesar's Rome and before that, Mesopotamia and China. The relatively simple concept of keeping messages secret between two parties became more complex in wartime. And this is the government's main defence for using cryptography: the ability to break codes has had major impact on how wars have proceeded and been won.

Indeed, the forerunners of modern computers were invented largely in order to solve cryptographic problems. During the Second World War, the Germans developed the encrypting machine known as Enigma. The Enigma machine scrambled messages in such a way that if letters, or groups of letters, were the same and appeared many times in the message, then the same type of text or encrypted message would not come out. One of the very first computers, developed by Alan Turing, was used to decipher some of these machines.

During the Cold War, governments armed themselves with the means to spy and monitor communications, exclusively holding the key to secret codes. But this control became chaotic in the 1970s with the birth of public key cryptography. New mathematical algorithms enabled a break from one-key cryptography. These 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. It is this ability to communicate in unbreakable codes which has caused concern and posed a major problem for governments.

Today the U.S. government is retaliating against Zimmermann and his ilk, and the battle is heating up. On one side are such government policy supporters as Professor Dorothy Denning, a world leading cryptographer and a reviewer of the Clipper system. Despite the great opposition from business and civil liberties groups, Denning vigorously defends the government's position to control the keys.

Opposing Denning and the Clinton Administration's struggle to sell Clipper to the people, are groups like Computer Professionals for Social Responsibility who actively campaign to inform the public on issues of privacy. Policy analyst David Banisar deplores the impact that proposed surveillance technology is having in the United States. Also sceptical of the government's position on Clipper is John Perry Barlow of the Electronic Frontier Foundation who believes the technology is open to abuse. Contemplating the prospect of being put on a government databank for actually discussing these issues, these key players debate one of the many evolving dilemmas on Netopia.

Phil Zimmermann: Today we live in the information age where almost everyone has a personal computer and a modem, but with electronic mail it's like sending messages on a postcard, 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 inoculate the body politic against possible government abuses in the future, I feel we should be building a technology infrastructure that has secure electronic mail.

PGP is a program that encrypts electronic mail and runs on a personal computer, letting you send e-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. This defacto standard for the encryption of electronic mail has spread all over the world. I am currently under criminal investigation because the U.S. government has laws against the export of encryption software. They regard it as ammunition. The State Department has rules about exporting munitions – in the form of a munitions list. Anything on this list can only be exported with a licence from the State Department. PGP is strong cryptography, it can't be easily broken by the government, so there's not much chance of them granting an export licence for it. But because PGP was published as free software it has spread all over the place in a very short time. And the U.S. government is taking the position that the electronic publication of PGP is the same thing as exporting it. Maria Cantwell, our national representative from Washington, where Microsoft has its headquarters, has proposed legislation that would lift all the export controls on encryption software, but the National Security Agency (NSA) is against such a law, they want to keep the export controls in place. The mission of the NSA is signals intelligence, and that's something that they still want to preserve. If widespread encryption software becomes available, then they're afraid that they won't be able to decipher as much traffic.

THE U.S. GOVERNMENT HAS LAWS AGAINST THE EXPORT OF ENCRYPTION SOFTWARE. THEY REGARD IT AS AMMUNITION

We need stronger encryption like PGP, but we need those encryption methods to become more widely available to make people's private business communications safe from major governments. 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: The problem with the Internet is that, unlike the telephone which is extremely hard to analyse automatically (you've got to have people sitting and listening), with electronic mail you have a stream of ASCII data which is analysable by any machine that is plugged into the network.

ZIMMERMAN: I CAN EASILY IMAGINE THE SINGAPORE GOVERNMENT EMBRACING THE CLIPPER CHIP, FOR EXAMPLE. SINGAPORE IS ALREADY A SURVEILLANCE SOCIETY WITH VIDEO CAMERAS AND ELECTRONIC MONITORING DEVICES AND FINANCIAL-TRANSACTION MONITORING EVERYWHERE.

What that means is that on the occurrence of more than three words which are deemed to be seditious or indicative of terrorist activity or drug dealings or whatever, the computer program clicks over and the message goes into a pile; therefore the name of the sender and the name of the recipient go into a pile of people the agency had reason to monitor in the past. It's that kind of suspicion building which can be automated through what I call data-veillance, which are the real fears of text messaging as opposed to voice messaging.

These spook agencies need to be more efficient, in the same way that every government agency needs to be more efficient in its monitoring of tax evasion. In order to do that, they have to automate their surveillance. At present, on the budget they've got, they can only subject a relatively small number of people to surveillance because they have to have people physically sitting, listening to telephone calls. By having a computer system that will do that for them, they're able to spread their surveillance net much wider. Unfortunately, there are many conversations which mention nasty words like sedition and drugs and all those other key words that are fed in – well I've just mentioned them so if we were having this conversation in text, our names would now be in that database.

Zimmermann: I received 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 training camps on 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.

I can easily imagine the Singapore government embracing the Clipper Chip, for example. Singapore is already a surveillance 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 there is not enough citizen opposition, there is the danger that Clipper could spread horizontally around the world and become entrenched as an international standard.

Professor Dorothy Denning: Public key cryptography has two great advantages. One is that it's provided with the mechanism for digital signatures. These are extremely valuable, especially as networks will be used more for electronic commerce. The other 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 and exchanging those keys so that they can be carried on secure communications.

Rosie Cross: Are you opposed to people like Phil Zimmermann releasing something like PGP?

Denning: I don't think it's a standard that most people should adopt. First of all it doesn't solve my criteria for user-friendliness. The average people are not going to use encryption unless they can basically get it with the push of a button. Right now using this system is considerably more complicated than that.

We need Clipper Chip because we'd all like to have a secure way of communicating, and this will provide it on the telephone, which is what it's designed for, and it doesn't require a lot of effort to use it. As a society I think we want Clipper Chip so we won't 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. The chip would be embedded in a device so you'd basically 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. 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 to the communication. Each device has a secret key and when the device is manufactured the key is split into two parts, then when the government has their court order, those two parts are loaded into a device which will then combine them and decrypt the communications on the channel. 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.

Jennifer Seberry (jennie@osiris.cs.uow.edu.au) was founder of the Centre for Communication Security Research in 1988 and has been director ever since. She co-authored the reference 'Cryptography: An introduction to computer security.'

Dorothy Denning (denning@cs.georgetown.edu) is chair of computer science at Georgetown University, USA. She is author of the popular 'Cryptography and Data Security' and sits on the Clipper Chip Review Committee.

Phil Zimmermann (prz@acm.org) is a consulting software engineer, specialising in cryptography and data security. He is author of Pretty Good Privacy (PGP), an electronic personal security phenomenon.

David Chaum (chaum@digicash.nl) is the owner of Digicash, a start-up company selling electronic cash and related systems. He is founder of the International Cryptographic Association for Research.

John Perry Barlow (barlow@eff.org) is co-founder of the Electronic Frontier Foundation and is an occasional lyricist for The Grateful Dead. He spends most of his time lobbying on electronic issues.

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.

Roger Clarke (roger.clarke@anu.edu.au) is a reader in information systems at the Australian National University in Canberra.

David Banisar (banisar@cpsr.org) is policy analyst for the Electronic Privacy Information Centre.

Trudi McIntosh is the multimedia reporter for 'The Australian' newspaper.

David Banisar: Computer Professionals for Social Responsibility 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 [a planned space-borne nuclear defence shield] was one notable example of stuff we worked on back in the early '80s.

Since then we've moved on and are now looking at how the technology affects society generally. In this particular office in Washington D.C., we look at civil liberties issues – how technology affects privacy and free speech. There's a lot of people out there opposing Clipper. American industry is almost universally against it. The civil liberties groups all oppose it, even international industry is strongly opposed to it. The International Chamber of Commerce came out against it fairly recently.

Cross: Do you think Dorothy Denning has a point at all?

Banisar: I think the difference between Dorothy's position and ours is in how we see the relationship between a government and its people. 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.

CLARKE: THE IMPORTANT POINT ABOUT THE CRYPTOGRAPHIC SCHEME IS THAT THE SPOOK AGENCIES HAVE GOT THE ABILITY TO CRACK THE CRYPTOGRAPHY, SO THEY CAN LISTEN IN BUT NOBODY ELSE CAN AND THAT'S PROBABLY GOING TO BE THE PRACTICE.

There's a couple of problems, depending on which perspective you are viewing from. From a privacy perspective it seems the government is asking us to give them the equivalent of our house keys and then expecting us to trust them not to break in and drink our liquor when we're not there. From a technological standpoint, it's a real nightmare for anybody who wants real security to have to implement this chip into their products. From a purely technical standpoint, most hardware or software companies are writing things into 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 and 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 simply reprogramming.

Clipper has been around for at least four years. It started under the Bush Administration and was probably being thought about under Reagan. Under the Reagan Administration there was some pretty widespread domestic surveillance. People that opposed his plans in Central America were constantly spied on, as were regular library users. The FBI was going to libraries and saying, if a user has a foreign name then we want to know if they're reading anything we think they shouldn't be.

Denning: That's just nonsense. 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 a more serious problem globally, to the extent that we can't effectively deal with it in our country and 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. So if we lose that capability, potentially we could suffer some really devastating consequences. Another area is terrorism, and there again wire taps are used in over 90 per cent of cases.

Banisar: Terrorists wouldn'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 the only people who are going to use Clipper are those who can't afford anything better.

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

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.

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 unethical 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 U.S. 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 no longer exists, so in the absence of that threat the government had no choice but to foment new ones.

Ted Nelson: I have probably heard as many conspiracy theories as most people, but conspiracies do exist after all. The Clipper Chip is a complete phoney because it would, in fact, 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 and creating a scramble means that the government cannot read by the same method. The ostensible purpose which makes 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 seize the computers and possessions of anyone who is under suspicion of encrrypting.

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 possibly can.

Cross: How do we know the cypherpunks can't be accused of the same thing?

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

Banisar: They tend to believe that cryptography is the solution to all of our problems. I'm a little sceptical of that particular scenario myself, but they are very active in discussing among themselves technical solutions for various problems such as Clipper. 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, and it doesn't keep businesses from doing the same. Just as you can use a $50 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 intelligent vehicle highway systems – cryptography can be used to protect medical records on smart cards in a variety of ways.

There are a lot of different definitions of privacy. The right to be left alone is the key part of privacy, to not always be accountable for everything you do. If you go to a grocery store and buy a six-pack, is there a reason for them to have that information? Is there a reason for a big database somewhere to collect that you bought a six-pack on Monday and a 12-pack on Tuesday, which maybe you bought for your neighbour anyway?

Caelli: 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. For example, the much-hyped superhighway of the future will absolutely depend upon cryptography.

Clarke: The essence of what the cryptography argument is about is that the government is attempting to dictate what form of communication mechanisms we can use and what kind of garbling we're allowed to impose. Now remember there's technical issues as well. The Clipper Chip is designed to work in the U.S. telephone system, and it's still a telephone chip at this stage. There isn't a chip yet for handling data communication, although one is proposed. The Australian telephone system is rather different technically to the U.S. one, therefore I suspect that that particular chip might not work, but the design would. All they'd have to do would be to build a slightly different chip that would interface the Australian system. The important point about the cryptographic scheme that's used is that the spook agencies have got the ability to crack the cryptography, so they can listen in but nobody else can, and that's probably going to be the practice. It will probably be, for practical purposes, uncrackable. If they were in a position to totally impose that on every telephone in the U.S., or Australia, then I'd be much more concerned, but at this stage that is not what they're proposing.

CLARKE: THE ESSENCE OF THE CRYPTOGRAPHY ARGUMENT IS THAT THE GOVERNMENT IS ATTEMPTING TO DICTATE WHAT FORM OF COMMUNICATION MECHANISMS WE CAN USE AND WHAT KIND OF GARBLING WE'RE ALLOWED TO IMPOSE.

Professor Jennifer Seberry: The Japanese developed their own indigenous encryption algorithm which they call FEEL. FEEL was presented at international conferences and was broken, so they put out a new version, and that was broken, and so they put out a new version and it was 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 many of us felt, aren't they smart. They put out their algorithms and get the best people in the world to find out what's wrong with them for free. Well, the Japanese, having got a version of FEEL now which is in all of their products, have gone and sold it, while we continue to be preoccupied with our own problems. 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 has developed encryption, but we can't get it approved for export in any version at all.

Trudi McIntosh: Rumours indicate that Canberra is very wary of the hostile reaction that the Clipper Chip 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.

Clarke: Yes, things are done through the back door and there is this phenomenon called 'function creep'. Once you get something useful like the tax-file number in, then you'd want to use it for something else. 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. 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 it imposes on the populace and the extent to which they create a scope for a future totalitarian government to repress the individual's thinking and speaking. They're the real issues. ■