Philip R. Zimmermann

Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation.

26 June 1996

Mr. Chairman and members of the committee, my name is Philip Zimmermann, and I'm Chairman and Chief Technology Officer for PGP Inc., a newly-formed company that provides cryptographic products. I'm here to talk to you today about S.1726 and the need to change US export control policy for cryptographic software. I want to thank you for the opportunity to be here to speak in favor of this bill.

I'm the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of E-mail, winning numerous industry awards along the way. For three years I was the target of a criminal investigation by the US Customs Service, who assumed that laws were broken when PGP spread outside the US. That investigation was closed without indictment in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers, because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and mirrors the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

In addition to the limited availability of computers, another problem with cryptography in those days was that cryptographic keys had to be distributed over secure channels so that both parties could send encrypted traffic over insecure channels. Governments solved that problem by dispatching key couriers with satchels handcuffed to their wrists. Governments could afford to send guys like these to their embassies overseas. But the great masses of ordinary people would never have access to practical cryptography if keys had to be distributed this way. No matter how cheap and powerful personal computers might someday become, you just can't send the keys electronically without the risk of interception. This widened the feasibility gap between government and personal access to cryptography.

Today, we live in a new world that has had two major breakthroughs that have an impact on this state of affairs. The first is the coming of the personal computer and the information age. The second breakthrough is public-key cryptography.

With the first breakthrough comes cheap ubiquitous personal computers, modems, FAX machines, the Internet, E-mail, the World- Wide Web, digital cellular phones, personal digital assistants (PDAs), wireless digital networks, ISDN, cable TV, and the data superhighway. This information revolution is catalyzing the emergence of a global economy.

But this renaissance in electronic digital communication brings with it a disturbing erosion of our privacy. In the past, if the government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This is analogous to catching fish with a hook and a line, one fish at a time. Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale.

Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm for everyone, not the novelty it is today. Unlike paper mail, E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing -- making a quantitative and qualitative Orwellian difference to the health of democracy.

The second breakthrough came in the late 1970s, with the mathematics of public key cryptography. This allows people to communicate securely and conveniently with people they've never met, with no prior exchange of keys over secure channels. No more special key couriers with black bags. This, coupled with the trappings of the information age, means the great masses of people can at last use cryptography. This new technology also provides digital signatures to authenticate transactions and messages, and allows for digital money, with all the implications that has for an electronic digital economy.

This convergence of technology -- cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera -- is all part of the information revolution. Encryption is just simple arithmetic to all this digital hardware. All these devices will be using encryption. The rest of the world uses it, and they laugh at the US because we are railing against nature, trying to stop it. Trying to stop this is like trying to legislate the tides and the weather. It's like the buggy whip manufacturers trying to stop the cars -- even with the NSA and the FBI on their side, it's still impossible. The information revolution is good for democracy -- good for a free market and trade. It contributed to the fall of the Soviet empire. They couldn't stop it either.

Today, every off-the-shelf multimedia PC can become a secure voice telephone, through the use of freely available software such as PGPfone. When you combine that with the strong political will that exists in the American people to have their privacy, it's going to require extreme measures to control this technology. What does this mean for the government's Clipper chip and key escrow

systems?

Like every new technology, this comes at some cost. Cars pollute the air and cause traffic jams. Cryptography can help criminals hide their activities. People in the law enforcement and intelligence communities are going to look at this only in their own terms. But even with these costs, we still can't stop this from happening in a free market global economy. Most people I talk to outside of government feel that the net result of providing privacy will be positive.

Law enforcement and intelligence interests in the government have attempted many times to suppress the availability of strong domestic encryption technology.

In 1991, Senate Bill 266 included a non-binding resolution, which if it had become real law, would have forced manufacturers of secure communications equipment to insert special "trap doors" in their products, so that the government could read anyone's encrypted messages. Before that measure was defeated, I wrote and released Pretty Good Privacy. I did it because I wanted cryptography to be made available to the American public before it became illegal to use it. I gave it away for free so that it would achieve wide dispersal, to inoculate the body politic.

The 1994 Digital Telephony bill mandated that phone companies install remote wiretapping ports into their central office digital switches, creating a new technology infrastructure for "point-and-click" wiretapping, so that federal agents no longer have to go out and attach alligator clips to phone lines. Now they'll be able to sit in their headquarters in Washington and listen in to your phone calls. Of course, the law still requires a court order for a wiretap. But while technology infrastructures tend to persist for generations, laws and policies can change overnight. Once a communications infrastructure optimized for surveillance becomes entrenched, a shift in political conditions may lead to abuse of this new-found power. Political conditions may shift with the election of a new government, or perhaps more abruptly from the bombing of a Federal building.

A year after the 1994 Digital Telephony bill passed, the FBI disclosed plans to require the phone companies to build into their infrastructure the capacity to simultaneously wiretap one percent of all phone calls in all major US cities. This would represent more than a thousandfold increase over previous levels in the number of phones that could be wiretapped. In previous years, there were only about 1000 court-ordered wiretaps in the US per year, at the federal, state, and local levels combined. It's hard to see how the government could even employ enough judges to sign enough wiretap orders to wiretap 1% of all our phone calls, much less hire enough federal agents to sit and listen to all that traffic in real time. The only plausible way of processing that amount of traffic is a massive Orwellian application of automated voice recognition technology to sift through it all, searching for interesting keywords or searching for a particular speaker's voice. If the government doesn't find the target in the first 1% sample, the wiretaps can be shifted over to a different 1% until the target is found, or until everyone's phone line has been checked for subversive traffic. The FBI says they need this capacity to plan for the future. This plan sparked such outrage that it was defeated in Congress, at least this time around, in 1995. But the mere fact that the FBI even asked

for these broad powers is revealing of their agenda. And the defeat of this plan isn't so reassuring when you consider that the 1994 Digital Telephony bill was also defeated the first time it was introduced, in 1993.

Advances in technology will not permit the maintenance of the status quo, as far as privacy is concerned. The status quo is unstable. If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of. The only way to hold the line on privacy in the information age is strong cryptography. Cryptography strong enough to keep out major governments.

The government has a track record that does not inspire confidence that they will never abuse our civil liberties. The FBI's COINTELPRO program targeted groups that opposed government policies. They spied on the anti-war movement and the civil rights movement. They wiretapped Martin Luther King's phone. Nixon had his enemies list. And then there was the Watergate mess. The War on Drugs has given America the world's largest per- capita incarceration rate in the world, a distinction formerly held by South Africa, before we surpassed them during the eighties even when apartheid was in full swing. Recently, we've seen the images and sounds of the Rodney King beatings, Detective Mark Fuhrman's tapes boasting of police abuses, and the disturbing events of the Ruby Ridge case. And now Congress and the Clinton administration seem intent on passing laws curtailing our civil liberties on the Internet. At no time in the past century has public distrust of the government been so broadly distributed across the political spectrum, as it is today.

The Clinton Administration seems to be attempting to deploy and entrench a communications infrastructure that would deny the citizenry the ability to protect its privacy. This is unsettling because in a democracy, it is possible for bad people to occasionally get elected-- sometimes very bad people. Normally, a well-functioning democracy has ways to remove these people from power. But the wrong technology infrastructure could allow such a future government to watch every move anyone makes to oppose it. It could very well be the last government we ever elect.

When making public policy decisions about new technologies for the government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the government to deploy those technologies. This is simply a matter of good civic hygiene.

In addition to the human rights arguments, there are technological reasons why the current export control regime makes no sense anymore.

There has been considerable debate about allowing the export of implementations of the full 56-bit Data Encryption Standard (DES). At an academic cryptography conference in 1993, Michael Wiener of Northern Telecom in Ottawa presented a paper on how to crack the DES with a special machine. He has fully designed and tested a chip that guesses DES keys at high speed until it finds the right one. Although he has refrained from building the real chips so far, he can get these chips manufactured for $10.50 each, and can build 57000 of them into a special machine for $1 million

that can try every DES key in 7 hours, averaging a solution in 3.5 hours. $1 million can be hidden in the budget of many companies. For $10 million, it takes 21 minutes to crack, and for $100 million, just two minutes. That's full 56-bit DES, cracked in just two minutes. I'm sure the NSA can do it in seconds, with their budget. This means that DES is now effectively dead for purposes of serious data security applications. If Congress acts now to enable the export of full DES products, it will be a day late and a dollar short.

Knowledge of cryptography is becoming so widespread, that export controls are no longer effective at controlling the spread of this technology. People everywhere can and do write good cryptographic software, and we import it here but cannot export it, to the detriment of our indigenous software industry.

I wrote PGP from information in the open literature, putting it into a convenient package that everyone can use in a desktop or palmtop computer. Then I gave it away for free, for the good of democracy. This could have popped up anywhere, and spread. Other people could have and would have done it. And are doing it. Again and again. All over the planet. This technology belongs to everybody.

PGP has spread like a prairie fire, fanned by countless people who fervently want their privacy restored in the information age.

Today, human rights organizations are using PGP to protect their people overseas. Amnesty International uses it. The human rights group in the American Association for the Advancement of Science uses it. It is used to protect witnesses who report human rights abuses in the Balkans, in Burma, in Guatemala, in Tibet.

Some Americans don't understand why I should be this concerned about the power of government. But talking to people in Eastern Europe, you don't have to explain it to them. They already get it-- and they don't understand why we don't.

I want to read you a quote from some E-mail I got in October 1993 from someone in Latvia, on the day that Boris Yeltsin was shelling his own Parliament building:

"Phil I wish you to know: let 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."