WIRED 2.04

Electrosphere

****

Jackboots on the Infobahn

Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace.

By John Perry Barlow

[Note: The following article will appear in the April 1994 issue of WIRED. We, the editors of WIRED, are net-casting it now in its pre-published form as a public service. Because of the vital and urgent nature of its message, we believe readers on the Net should hear and take action now. You are free to pass this article on electronically; in fact we urge you to replicate it throughout the net with our blessings. If you do, please keep the copyright statements and this note intact. For a complete listing of Clipper-related resources available through WIRED Online, send email to <infobot@wired.com> with the following message: “send clipper.index”. - The Editors of WIRED]

On January 11, I managed to schmooze myself aboard Air Force 2. It was flying out of LA, where its principal passenger had just outlined his vision of the information superhighway to a suited mob of television, show- biz, and cable types who fervently hoped to own it one day - if they could ever figure out what the hell it was.

From the standpoint of the Electronic Frontier Foundation the speech had been wildly encouraging. The administration’s program, as announced by Vice President Al Gore, incorporated many of the concepts of open competition, universal access, and deregulated common carriage that we’d been pushing for the previous year.

But he had said nothing about the future of privacy, except to cite among the bounties of the NII its ability to “help law enforcement agencies thwart criminals and terrorists who might use advanced telecommunications to commit crimes.”

On the plane I asked Gore what this implied about administration policy on cryptography. He became as noncommittal as a cigar-store Indian. “We’ll be making some announcements .... I can’t tell you anything more.” He hurried to the front of the plane, leaving me to troubled speculation.

Despite its fundamental role in assuring privacy, transaction security, and reliable identity within the NII, the Clinton administration has not demonstrated an enlightenment about cryptography up to par with the rest of its digital vision.

The Clipper Chip - which threatens to be either the goofiest waste of federal dollars since President Gerald Ford’s great Swine Flu program or, if actually deployed, a surveillance technology of profound malignancy - seemed at first an ugly legacy of the Reagan-Bush modus operandi. “This is going to be our Bay of Pigs,” one Clinton White House official told me at the time Clipper was introduced, referring to the disastrous plan to invade Cuba that Kennedy inherited from Eisenhower.

(Clipper, in case you’re just tuning in, is an encryption chip that the National Security Agency and FBI hope will someday be in every phone and computer in America. It scrambles your communications, making them unintelligible to all but their intended recipients. All, that is, but the government, which would hold the "key" to your chip. The key would separated into two pieces, held in escrow, and joined with the appropriate "legal authority.")

Of course, trusting the government with your privacy is like having a Peeping Tom install your window blinds. And, since the folks I've met in this White House seem like extremely smart, conscious freedom-lovers - hell, a lot of them are Deadheads - I was sure that after they were fully moved in, they'd face down the National Security Agency and the FBI, let Clipper die a natural death, and lower the export embargo on reliable encryption products.

Furthermore, the National Institutes of Standards and Technology and the National Security Council have been studying both Clipper and export embargoes since April. Given that the volumes of expert testimony they had collected overwhelmingly opposed both, I expected the final report would give the administration all the support it needed to do the right thing.

I was wrong. Instead, there would be no report. Apparently, they couldn't draft one that supported, on the evidence, what they had decided to do instead.

THE OTHER SHOE DROPS

On Friday, February 4, the other jackboot dropped. A series of announcements from the administration made it clear that cryptography would become their very own "Bosnia of telecommunications" (as one staffer put it). It wasn't just that the old Serbs in the National Security Agency and the FBI were still making the calls. The alarming new reality was that the invertebrates in the White House were only too happy to abide by them. Anything to avoid appearing soft on drugs or terrorism.

So, rather than ditching Clipper, they declared it a Federal Data Processing Standard, backing that up with an immediate government order for 50,000 Clipper devices. They appointed the National Institutes of Standards and Technology and the Department of Treasury as the "trusted" third parties that would hold the Clipper key pairs. (Treasury, by the way, is also home to such trustworthy agencies as the Secret Service and the Bureau of Alcohol, Tobacco, and Firearms.)

They reaffirmed the export embargo on robust encryption products, admitting for the first time that its purpose was to stifle competition to Clipper. And they outlined a very porous set of requirements under which the cops might get the keys to your chip. (They would not go into the procedure by which the National Security Agency could get them, though they assured us it was sufficient.)

They even signaled the impending return of the dread Digital Telephony, an FBI legislative initiative requiring fundamental reengineering of the information infrastructure; providing wiretapping ability to the FBI would then become the paramount design priority.

INVASION OF THE BODY SNATCHERS

Actually, by the time the announcements thudded down, I wasn't surprised by them. I had spent several days the previous week in and around the White House.

I felt like I was in another remake of The Invasion of the Body Snatchers. My friends in the administration had been transformed. They'd been subsumed by the vast mindfield on the other side of the security clearance membrane, where dwell the monstrous bureaucratic organisms that feed on fear. They'd been infected by the institutionally paranoid National Security Agency's Weltanschauung.

They used all the telltale phrases. Mike Nelson, the White House point man on the NII, told me, “If only I could tell you what I know, you’d feel the same way I do” I told him I’d been inoculated against that argument during Vietnam. (And it does seem to me that if you’re going to initiate a process that might end freedom in America, you probably need an argument that isn’t classified.)

Besides, how does he know what he knows? Where does he get his information? Why, the National Security Agency, of course. Which, given its strong interest in the outcome, seems hardly an unimpeachable source.

However they reached it, Clinton and Gore have an astonishingly simple bottom line, to which even the future of American liberty and prosperity is secondary: They believe that it is their responsibility to eliminate, by whatever means, the possibility that some terrorist might get a nuke and use it on, say, the World Trade Center. They have been convinced that such plots are more likely to ripen to hideous fruition behind a shield of encryption.

The staffers I talked to were unmoved by the argument that anyone smart enough to steal a nuclear device is probably smart enough to use PGP or some other uncompromised crypto standard. And never mind that the last people who popped a hooter in the World Trade Center were able to get it there without using any cryptography and while under FBI surveillance.

We are dealing with religion here. Though only ten American lives have been lost to terrorism in the last two years, the primacy of this threat has become as much an article of faith with these guys as the Catholic conviction that human life begins at conception or the Mormon belief that the Lost Tribe of Israel crossed the Atlantic in submarines.

In the spirit of openness and compromise, they invited the Electronic Frontier Foundation to submit other solutions to the “problem” of the nuclear-enabled terrorist than key escrow devices, but they would not admit into discussion the argument that such a threat might, in fact, be some kind of phantasm created by the spooks to ensure their lavish budgets into the post-Cold War era.

As to the possibility that good old-fashioned investigative techniques might be more valuable in preventing their show-case catastrophe (as it was after the fact in finding the alleged perpetrators of the last attack on the World Trade Center), they just hunkered down and said that when wiretaps were necessary, they were damned well necessary.

When I asked about the business that American companies lose because of their inability to export good encryption products, one staffer essentially dismissed the market, saying that total world trade in crypto goods was still less than a billion dollars. (Well, right. Thanks more to the diligent efforts of the National Security Agency than to dim sales potential.)

I suggested that a more immediate and costly real-world effect of their policies would be to reduce national security by isolating American commerce, owing to a lack of international confidence in the security of our data lines. I said that Bruce Sterling’s fictional data-enclaves in places like the Turks and Caicos Islands were starting to look real-world inevitable.

They had a couple of answers to this, one unsatisfying and the other scary. The unsatisfying answer was that the international banking community could just go on using DES, which still seemed robust enough to them. (DES is the old federal Data

Encryption Standard, thought by most cryptologists to be nearing the end of its credibility.)

More frightening was their willingness to counter the data-enclave future with one in which no data channels anywhere would be secure from examination by one government or another. Pointing to unnamed other countries that were developing their own mandatory standards and restrictions regarding cryptography, they said words to the effect of, “Hey, it’s not like you can’t outlaw the stuff. Look at France.”

Of course, they have also said repeatedly - and for now I believe them - that they have absolutely no plans to outlaw non-Clipper crypto in the US. But that doesn’t mean that such plans wouldn’t develop in the presence of some pending “emergency.” Then there is that White House briefing document, issued at the time Clipper was first announced, which asserts that no US citizen “as a matter of right, is entitled to an unbreakable commercial encryption product.”

Now why, if it’s an ability they have no intention of contesting, do they feel compelled to declare that it’s not a right? Could it be that they are preparing us for the laws they’ll pass after some bearded fanatic has gotten himself a surplus nuke and used something besides Clipper to conceal his plans for it?

If they are thinking about such an eventuality, we should be doing so as well. How will we respond? I believe there is a strong, though currently untested, argument that outlawing unregulated crypto would violate the First Amendment, which surely protects the manner of our speech as clearly as it protects the content.

But of course the First Amendment is, like the rest of the Constitution, only as good as the government’s willingness to uphold it. And they are, as I say, in the mood to protect our safety over our liberty.

This is not a mind-frame against which any argument is going to be very effective. And it appeared that they had already heard and rejected every argument I could possibly offer.

In fact, when I drew what I thought was an original comparison between their stand against naturally proliferating crypto and the folly of King Canute (who placed his throne on the beach and commanded the tide to leave him dry), my government opposition looked pained and said he had heard that one almost as often as jokes about roadkill on the information superhighway.

I hate to go to war with them. War is always nastier among friends. Furthermore, unless they’ve decided to let the National Security Agency design the rest of the National Information Infrastructure as well, we need to go on working closely with them on the whole range of issues like access, competition, workplace privacy, common carriage, intellectual property, and such. Besides, the proliferation of strong crypto will probably happen eventually no matter what they do.

But then again, it might not. In which case we could shortly find ourselves under a government that would have the automated ability to log the time, origin and recipient of every call we made, could track our physical whereabouts continuously, could keep better account of our financial transactions than we do, and all without a warrant. Talk about crime prevention!

Worse, under some vaguely defined and surely mutable “legal authority,” they also would be able to listen to our calls and read our e-mail without having to do any backyard rewiring. They wouldn’t need any permission at all to monitor overseas calls.

If there's going to be a fight, I'd rather it be with this government than the one we'd likely face on that hard day.

Hey, I've never been a paranoid before. It's always seemed to me that most governments are too incompetent to keep a good plot strung together all the way from coffee break to quitting time. But I am now very nervous about the government of the United States of America.

Because Bill 'n' Al, whatever their other new-paradigm virtues, have allowed the very old-paradigm trogs of the Guardian Class to define as their highest duty the defense of America against an enemy that exists primarily in the imagination - and is therefore capable of anything.

To assure absolute safety against such an enemy, there is no limit to the liberties we will eventually be asked to sacrifice. And, with a Clipper Chip in every phone, there will certainly be no technical limit on their ability to enforce those sacrifices.

WHAT YOU CAN DO

GET CONGRESS TO LIFT THE CRYPTO EMBARGO

The administration is trying to impose Clipper on us by manipulating market forces. By purchasing massive numbers of Clipper devices, they intend to induce an economy of scale which will make them cheap while the export embargo renders all competition either expensive or nonexistent. We have to use the market to fight back. While it's unlikely that they'll back down on Clipper deployment, the Electronic Frontier Foundation believes that with sufficient public involvement, we can get Congress to eliminate the export embargo.

Rep. Maria Cantwell, D-Washington, has a bill (H.R. 3627) before the Economic Policy, Trade, and Environment Subcommittee of the House Committee on Foreign Affairs that would do exactly that. She will need a lot of help from the public. They may not care much about your privacy in DC, but they still care about your vote.

Please signal your support of H.R. 3627, either by writing her directly or e-mailing her at cantwell@eff.org. Messages sent to that address will be printed out and delivered to her office. In the subject header of your message, please include the words "support HR 3627." In the body of your message, express your reasons for supporting the bill. You may also express your sentiments to Rep. Lee Hamilton, D-Indiana, the House Committee on Foreign Affairs chair, by e-mailing hamilton@eff.org.

Furthermore, since there is nothing quite as powerful as a letter from a constituent, you should check the following list of subcommittee and committee members to see if your congressional representative is among them. If so, please copy them your letter to Rep. Cantwell.

Economic Policy, Trade, and Environment Subcommittee:

Democrats: Sam Gejdenson (Chair), D-Connecticut; James Oberstar, D-Minnesota; Cynthia McKinney, D-Georgia; Maria Cantwell, D-Washington; Eric Fingerhut, D-Ohio; Albert R. Wynn, D-Maryland; Harry Johnston, D-Florida; Eliot Engel, D-New York; Charles Schumer, D-New York.

Republicans: Toby Roth (ranking), R-Wisconsin; Donald Manzullo, R-Illinois; Doug Bereuter, R-Nebraska; Jan Meyers, R-Kansas; Cass Ballenger, R-North Carolina; Dana Rohrabacher, R-California.

> House Committee on Foreign Affairs:

Democrats: Lee Hamilton (Chair), D-Indiana; Tom Lantos, D-California; Robert Torricelli, D-New Jersey; Howard Berman, D-California; Gary Ackerman, D-New York; Eni Faleomavaega, D-Somoa; Matthew Martinez, D- California; Robert Borski, D-Pennsylvania; Donal Payne, D-New Jersey; Robert Andrews, D-New Jersey; Robert Menendez, D-New Jersey; Sherrod Brown, D-Ohio; Alcee Hastings, D-Florida; Peter Deutsch, D-Florida; Don Edwards, D-California; Frank McCloskey, D-Indiana; Thomas Sawyer, D-Ohio; Luis Gutierrez, D-Illinois.

Republicans: Benjamin Gilman (ranking), R-New York; William Goodling, R- Pennsylvania; Jim Leach, R-Iowa; Olympia Snowe, R-Maine; Henry Hyde, R- Illinois; Christopher Smith, R-New Jersey; Dan Burton, R-Indiana; Elton Gallegly, R-California; Ileana Ros-Lehtinen, R-Florida; David Levy, R-New York; Lincoln Diaz-Balart, R-Florida; Ed Royce, R-California.

BOYCOTT CLIPPER DEVICES AND THE COMPANIES WHICH MAKE THEM.

Don’t buy anything with a Clipper Chip in it. Don’t buy any product from a company that manufactures devices with Big Brother inside. It is likely that the government will ask you to use Clipper for communications with the IRS or when doing business with federal agencies. They cannot, as yet, require you to do so. Just say no.

LEARN ABOUT ENCRYPTION AND EXPLAIN THE ISSUES TO YOUR UNWIRED FRIENDS

The administration is banking on the likelihood that this stuff is too technically obscure to agitate anyone but nerds like us. Prove them wrong by patiently explaining what’s going on to all the people you know who have never touched a computer and glaze over at the mention of words like “cryptography.”

Maybe you glaze over yourself. Don’t. It’s not that hard. For some hands-on experience, download a copy of PGP - Pretty Good Privacy - a shareware encryption engine which uses the robust RSA encryption algorithm. And learn to use it.

GET YOUR COMPANY TO THINK ABOUT EMBEDDING REAL CRYPTOGRAPHY IN ITS PRODUCTS

If you work for a company that makes software, computer hardware, or any kind of communications device, work from within to get them to incorporate RSA or some other strong encryption scheme into their products. If they say that they are afraid to violate the export embargo, ask them to consider manufacturing such products overseas and importing them back into the United States. There appears to be no law against that. Yet.

You might also lobby your company to join the Digital Privacy and Security Working Group, a coalition of companies and public interest groups - including IBM, Apple, Sun, Microsoft, and, interestingly, Clipper phone manufacturer AT&T - that is working to get the embargo lifted.

ENLIST!

Self-serving as it sounds coming from me, you can do a lot to help by becoming a member of one of these organizations. In addition to giving you access to the latest information on this subject, every additional member strengthens our credibility with Congress.

Join the Electronic Frontier Foundation by writing membership@eff.org.

Join Computer Professionals for Social Responsibility by e-mailing cpsr.info@cpsr.org.

CPSR is also organizing a protest, to which you can lend your support by sending e-mail to clipper.petition@cpsr.org with "I oppose Clipper" in the message body. Ftp/gopher/WAIS to cpsr.org /cpsr/privacy/ crypto/clipper for more info.

In his LA speech, Gore called the development of the NII "a revolution." And it is a revolutionary war we are engaged in here. Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace. If they win, the most liberating development in the history of humankind could become, instead, the surveillance system which will monitor our grandchildren's morality. We can be better ancestors than that.

San Francisco, California

Wednesday, February 9, 1994

***

John Perry Barlow (barlow@eff.org) is co-founder and Vice-Chairman of the Electronic Frontier Foundation, a group which defends liberty, both in Cyberspace and the Physical World. He has three daughters.