POLICING THE INTERNET: *JAKE BAKER* AND BEYOND

March 9, 1995

QUESTION ONE: WHAT IS THE DEPARTMENT OF JUSTICE'S POSITION ON PROSECUTION OF ENCRYPTION?

March 9, 1995

PROFESSOR LOWENSTEIN:

I think because the opening speeches went a little longer than we had anticipated, I sense some restlessness among the natives, and I want to open it up to questions from the audience right away.

AUDIENCE PARTICIPANT:

I'm Matt Pulliam from Ford Motor Company.

I'd like to know what Mr. Charney says for a couple of questions regarding, a couple of years ago in Massachusetts, Phil Zimmermann developed the first widespread public encrypting system for encrypting E-mail communications.

He is in the process of being indicted right now by the Justice Department for exporting this technology as a munitions, which is the equivalency of supporting, say, (inaudible) produce their weapons.

Based on your record and the handling of the (inaudible) case, I believe that as you have a strong interest in protecting people's civil liberties, so I'd like to question, how can the Justice Department go after one of our prime spokespeople for practicing Internet?

SCOTT CHARNEY:

I'm going to answer your question in a little of a roundabout way, and the reason for that is you'll notice in my opening comments, I did not mention the Baker case either. The reason for that, the same reason I can't discuss the particulars of the Zimmermann case, is because they're pending cases, and I am prohibited from discussing them.

The issue of cryptography generally, however, is a fairly complex one.

On one hand, we do want people to have strong cryptography so that they can protect their own privacy, not only for their own purposes, but because hackers have been known to wiretap phone switches, intercept other people's communications and steal their data.

So you're back to wanting strong cryptography on one hand.

On the other hand, just like the anonymity problem, there are people who will use cryptography for bad things.

In this context, in the encryption context, the U.S. has two distinct but significant interests. One is that law enforcement not be thwarted in doing their investigations because data's encrypted, but the U.S. also has a broader national security interest.

If you look, for example, historically at World War II, our ability to break the German ciphers and the Japanese code was critical to our successes in the war. And if you don't believe me, you can read Body Guard At Large by Anthony K. Brown, which is probably the best book on intelligence in World War II.

So we have this problem that on one hand you want the proliferation of strong encryption, but on the other hand, if strong encryption gets in the wrong hands, you shoot yourself in the foot.

It's a very difficult issue to resolve, because the values on both sides of the equation are legitimate.

I mean, you can take something like murder and say, that's obviously bad, so people who are against it are good, people who are for it, are bad. That's easy. But cryptography is much harder.

The people who support cryptography, the use of cryptography, includes not just civil libertarians and privacy advocates, but the government. We encrypt a lot of our data for the very reason that we're protecting the sanctity, integrity and confidentiality of government information.

On the other hand, we had the problem that if cryptography is misused or used by people doing bad things, we end up in trouble.