Panel Discussion

Below is a slightly edited transcription of hand-scribbled notes taken by one observer (the editor) during the panel discussion. No guarantee of accuracy can be made. Individual statements cannot be reliably attributed to any particular panelist.

We are rapidly heading into the era of the Information Marketplace. We can already see the extent of intra-organization machines hooked to one another. This is the first stage of a three stage process. The second stage will be inter-organization communications in the business sector. The third will involve interpersonal communication between home and private office machines. Hundreds or thousands of computers will be talking to each other. The purchase and sale of information is central to the free enterprise system. Information will be a commodity like potatoes, you know its there and you can pay for it.

Consequences: Sortware protection is needed. Legal issues, copyright, liability if software fails, laws for governing ownership, transfer, acquisition, and protection of information. People are in the business or selling information. The need for protection is simply putting a door on the merchant's warehouse. The difference is that with information it is not only possible to steal the goods, but it can also be done without leaving any traces, unlike the physical theft of goods.

These thoughts led MIT to form a committee "On the Changing Nature ot Information" recognizing the growing importance of the field oi cryptography and the need to work in this field. They also recognize the importance ot U.S. national security and not to proceed irresponsibly. The result is that they decided to send all papers to NSA at the same time as they are sent to a close circle or a few technical colleagues.

The burden of deciding what is clasified should not fall entirely on the researcher. A second and more important factor is the relationship between university research and government. By sending papers to NSA we do not ask permission to publish. This gives the right checks and balances. Nobody wants to hurt the U.S. or to hurt free inquiry.

We will not have built in procedures where traditions of free inquiry are subordinated. There is no equivalent of NSA for the civilian sector. We need new laws to take into account the changing nature or information as computer networking develops.

Compare cryptography researchers with physicists and their atomic bomb. Whether they wanted it or not they were in it. The effects there are dramatic and visible, but unlike crypto the cost of entry into the field is high. Here in the mathematical world the problem is dramatically different with computer power readily available for cryptographic research. People don't readily see the magnitude or the effect or cryptography. In the commercial world, it has major implications. Two extremes are to have no secrets at all or to have total security for all communications. What one does in this area tends to have an effect one way or another.

Suppose a university preprint goes to a hundred people and to NSA at the same time then NSA says if you publish this it will destabilize the middle east. What do you do? A hundred copies are too many to retrieve. Broad distribution before seeking advice may not be a good idea Progress in this field may have serious consequences not only in military area but also in the economic arena. There is some concern about NSA's advice when a paper is sent in. They may focus on military and diplomatic concerns but ay they may not be aware of what goes on in the financial area.

The ACE report is inadequate since there is no consideration of NSA broadening its focus to include knowledge of commercial communications security.

NSA is in a poor position to defend its views in this debate. It can't say why publishing a certain paper will do damage to national security. Those who want to know can be cleared.

Until two years ago there was no output at all from NSA. Inman's speech startled people in NSA. He did recognize the need for crypto in the private sector but wanted more awareness of the potential for damage to national security. There are cases of 'inadvertent espionage'. Should the crypto market be regulated? Some degree or certification is needed. But then a liability question arises. NSA may not be willing to take on this task. An algorithm does not make a secure system. Publishing crypto papers may harm U.S. foreign intelligence efforts but it may also hurt commercial security also.

NSA's grant program (Project OCREAE) now offers an opportunity for unclassified research in crypto. It will help provide a source or future NSA employees as well as basic tools they will need for developing future crypto sturf.

NSA is interested in hearing from prospective nonauthors.

NSA is a fantastic organization and has done a great deal of good for this country.

This meeting is a remarkable phenomenon. Most of the researchers in this field in the western world have shown up. Previously we as a group had neither power nor responsibility.

Subordination or our will to NSA is not really an issue. MIT is older than NSA and is as great a pillar of American security.

Serious diplomatic consequences must be weighed against serious economic consequences.

It is very important to recognize that open naked confrontation with NSA is not in our interest. We had a tendency in that direction in the past.

Forums like this provide a potential for cooperation and mutual understanding.