Seminar Surveys Electronic Frontier

Until quite recently, computers and telecommunications have mainly been seen as the tools of specialists, whether in science, business, or the mysterious community of "computer geeks." That is changing, very quickly. The explosive proliferation of access to the Internet and other online net-

Roland Rakotonirainy and Simona Nass

work services, as well as the political debate over the future of the "information superhighway" have placed the brave new questions of our newly hyper-connected society right in our faces. A seminar at the New York HGS on March 5th, entitled "Privacy and Community on the Electronic Frontier," dealt provocatively with many of those questions and raised a few more.

Simona Nass, President of the Society for Electronic Access, a New York-based nonprofit organization devoted to research and dialogue on legal issues surrounding telecommunications, explained that the nature of the new electronic media has given rise to distinctly new civil-rights questions. We have long been accustomed to various agencies keeping records on us, she noted; such things as motor vehicle and hospital records are useful and necessary. But, when merchandisers of, say, baby products learn from your medical records that you are expecting, and start barraging you with advertising, you might feel that your privacy has been compromised. The ease - and sheer volume - of information exchange simply overwhelms traditional methods of ensuring confidentiality. We are hard-pressed to determine who knows what about our business.

The biggest area of contention at present is that of digital telephony and encryption. In the *(continued on back page)*

Electronic Frontier

(continued from front page)

(not very) distant past, the tapping of telephones by law enforcers (or by criminals) was a process that left physical evidence. But digital telephone technology thwarts traditional wiretapping methods; tapping must be enabled through a "trap door" in the equipment. Senate Bill 266 in 1992, which ended up being scuttled in committee, tried to mandate "tappability" for all phone systems in the US, so that conversations could be tapped without any traces whatever. The feature of untraceability, argued Simona Nass, has ominous implications for our right to privacy. The analogy of a search warrant no longer holds. Because wiretaps would become untraceable, laws prohibiting their misuse would be unenforceable.

The second danger, she said, is that if an opening were built into phone systems that allowed coded signals to be tapped, it is possible - likely, in fact - that unauthorized listeners would tune in as well.

These dangers are at the heart of the debate over the "Clipper Chip," an encryption device that scrambles your digital data according to its own internal code. No one can listen in - except the government, because the two keys to your Clipper-chip codes are to be held by two separate agencies in the Executive Branch. If a warrant is issued to tap your wire, these codes are brought into play - and their use is undetectable. Vice President Gore, the Clinton Administration's technological point man, supported the plan initially, but popular opposition to it is mounting.

Roland Rakotonirainy, an aerospace engineer who researches the trends of the day for his own edification (and ours) rounded out the program with a presentation on the impact that computers and telecommunications have had on banking. He reminded the audience that far more of the world's money circulates in the financial economy than in the "real economy," where consumers buy and sell goods. Information-processing technology is making such trading more efficient and profitable all the time. In rapidly changing markets, the faster one can complete a transaction, the more profit one can make, and modern systems have cut that time dramatically.

The danger of all this processing efficiency, Rakotonirainy noted, is that it creates incentives for more and more money to be devoted to financial speculation - draining resources from production, and further concentrating economic power in the hands of the wealthiest players with the best technology. The potential for tightening control, he warned, is ominous.

Both speakers stressed how very important it is for more people to consider the implications of these issues concerning the online world - because rules and procedures set up now will become important precedents. Among the people who know about the Clipper Chip, for example, the overwhelming majority are against it. The law enforcement community is the only group that enthusiastically supports it. The problem is that most people are not aware of the issues. The online world, Simona Nass concluded, is a brand new medium. We are in a process of learning which laws can be extended to these new forms of communication, and which ones must be rethought. Thus it is vital, just now, that people become informed about how to ensure both security and privacy in the electronic realm.

You can contact the Society for Electronic Access at 595 West End Ave., #9D, NYC 10024. (or Email them at sea@panix.com)