SCIENCE • www.sciencemag.org

EDITORIAL

Cryptography in America

In 1516, almost 20 years before his beheading for political and religious obstreperousness, Sir Thomas More wrote in "Utopia": "... and it will fall out as in a complication of diseases, that by applying a remedy to one sore, you will provoke another; and that which removes the one ill symptom produces others. ..." More was talking about the stratification of society as a result of privilege based on a landed economy. But his injunction applies equally well in the debate over cryptography and the Internet. Simply put, the future prosperity, academic freedoms, and civil liberties of U.S. citizens are being pitted against the interests of society to protect itself against the intrusions of criminals, terrorists, and unfriendly states. Some in government seek to protect society by barring international traffic in expert information and by providing law enforcement and security agencies with unlimited access to all encrypted traffic. However, many information scientists contend that such policies will impede research and teaching, isolate the U.S. expert community, and retard the development of the "information economy."

Proposals advocating domestic controls over cryptography would give government the authority to superintend the transactions of citizens and deprive the human rights community of the tools needed to monitor the fates of those who suffer repressions worldwide. The U.S. government has applied existing laws in questionable ways to stem the spread of this technology. Phil Zimmerman, author of the public domain encryption system PGP (Pretty Good Privacy) was threatened with prosecution for illegally exporting munitions after someone posted the software on the Internet. Ultimately the government dropped its dubious pursuit of a criminal indictment. Recently, a U.S. academic had to go to federal court to be allowed to speak about his research to audiences that might include non–U.S. citizens. A AAAS program to provide training in encryption to human rights groups abroad is hampered by government restrictions.

If the United States unilaterally mediates the intellectual exchange of its information scientists, it will be an unprecedented assault on academic freedom in peacetime. And since U.S. information scientists do not constitute a monopoly of innovation, it would not achieve the intended result of impeding the diffusion of cryptography technology. If the government succeeds in gaining immediate access to the secret keys of companies and individuals, many innocent users in the information chain could be held criminally liable. In response, U.S. service providers and carriers would be forced to downgrade or deny encryption altogether. This could destroy the Internet as a tool of commerce.

In September, despite the rejection by the House Commerce Committee of an amendment that would have prohibited the manufacture, sale, distribution, and export or import of encryption systems,* the House National Security and Intelligence committees had already approved equivalent amendments. The arena has now shifted to the House Rules Committee and to the Senate, which is considering similar restrictive legislation.†

The science and technology communities have tried to inform the Administration and Congress of the critical issues shaping this debate, but they have not been widely heard. These efforts include a 1994 Office of Technology Assessment report,‡ a 1996 National Research Council report,§ and a spring 1997 report of an ad hoc group of senior cryptographers and computer scientists. ‖

It is now time for scientists and technologists to confront the nation's legitimate security and criminal issues and to work in concert with Congress and the Administration to address these confounding puzzles. It will require all of our intelligence and rigor if we are to avoid Sir Thomas More's presentiment that by applying a remedy to one problem we may inflict a suppurating wound elsewhere on the body politic.

Irving Lerch and Mary Gray

Irving Lerch is director of international affairs at the American Physical Society and Mary Gray is professor of mathematics at American University in Washington, DC. They are co-chairs of the AAAS Committee on Scientific Freedom and Responsibility.

*H.R. 695, 105th Cong., 1st Sess. (1997). †S. 909, 105th Cong., 1st Sess. (1997). ‡U.S. Congress, OTA, OTA-TCT-606, Washington, DC, Government Printing Office, September 1994. §K. W. Dam and H. S. Lin, Eds., *Report of the Committee to Study National Cryptology Policy*, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, DC, 1996. ‖Final Report, 27 May 1997. Available at http://www.crypto.com/key_study/