

**Testimony Of**

**THOMAS PARENTY  
DIRECTOR, DATA AND COMMUNICATIONS  
SECURITY  
SYBASE, INC.**

**On Behalf Of**

**AMERICANS FOR COMPUTER PRIVACY**

**including the  
BUSINESS SOFTWARE ALLIANCE**

**WHY ENCRYPTION PROTECTS PRIVACY,  
PREVENTS CRIME & PROMOTES  
NATIONAL SECURITY**

**Before The  
CONSTITUTION, FEDERALISM AND  
PROPERTY RIGHTS SUBCOMMITTEE OF  
THE COMMITTEE ON THE JUDICIARY  
U.S. SENATE  
Washington, D.C.**

**March 17, 1998**

**Introduction**

Good morning. I am Thomas Parenty, the Director of Data and Communications Security for Sybase, Inc., and responsible for all security-related product development for the sixth largest software company in the world.

I want to take this opportunity, Mr. Chairman, to thank you for taking the time to analyze this complex, difficult issue and for your leadership in helping to bring it to the attention of the public. I also

would like to thank the others on this Subcommittee, and on the full Committee -- especially Senator Leahy who has worked tirelessly on the subject -- who have expressed their desire to address the concerns of American citizens about privacy in the Information Age.

I also, at this time, would like to acknowledge the recent overtures of the Administration and their desire to pursue a dialogue with the private sector to arrive at "cooperative solutions". We certainly are always open to discussion - as we have been for six years. But we need policies now that work for American computer users and American computing companies. That is why we are strongly supporting legislative efforts this Congress to affirm the rights of Americans to use and sell whatever encryption they want and to end unwise export controls on American encryption products.

I have been active in the cryptography and computer security field for over a decade, starting with my tenure at the National Security Agency (NSA) in the early and mid-eighties. While at NSA, I worked on internal NSA computer security issues and focused on the formal verification of cryptographic protocols and internal computer security controls for global nuclear command and control networks. Since then in the private sector, I have worked on the security design of operating systems, networks, and database management systems for many customers ranging from U.S. companies to government agencies, including the Central Intelligence Agency, the Defense Intelligence Agency, and the Air Force. Most recently, I have served as an advisor to the President's Commission on Critical Infrastructure Protection, specifically addressing the needs of the telecommunications and banking infrastructures.

My company, Sybase, Inc., is headquartered in Emeryville, California, and is a worldwide leader in distributed, open computing solutions. We provide

customers and partners with the software and services to create business solutions for strategic, competitive advantage. These high-performance, end-to-end solutions encompass client/server, Internet and intranet transaction processing, mobile computing, and data mart and data warehousing applications. Sybase's Adaptive Component Architecture(tm) enables rapid design, development and deployment of distributed multi-tier business applications. Our product lines include Sybase high-performance database servers, distributed data access and connectivity products, and Powersoft(r) enterprise development tools.

Today, however, I am not only speaking on behalf of Sybase, but also on behalf of Americans for Computer Privacy (ACP), which includes the Business Software Alliance (BSA)[[1](#)] and Sybase.

ACP is a new coalition of more than 70 companies and 28 associations representing the financial services, manufacturing, telecommunications, high-tech and transportation sectors, and associations and organizations, including the Eagle Forum, Americans for Tax Reform, and Center for Democracy and Technology. ACP's mission is to ensure that the privacy of all Americans' confidential files and communications is preserved and protected in the information age. ACP opposes new federal restrictions on the use of encryption products in the U.S. and supports the sale of strong U.S. encryption products to customers around the world.

But most of all, I am here today to speak on behalf of the tens of millions of users of American software products. The American software industry has succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users

are demanding is the ability to protect their electronic information and to interact securely worldwide. Medical records. Employee evaluations. Information about credit cards, Internet sales, and bank accounts. In short, users are demanding the ability to protect the privacy of confidential and sensitive files and communications.

This morning, I want to make four points:

- Encryption protects privacy rights in the information age;
- Encryption prevents crime and protects national security;
- The Administration's key recovery scheme inherently introduces additional vulnerability and insecurity and will not work; and
- In order to promote American's privacy, Congress should reject proposals which mandate - by law or heavy-handed incentives or conditions - key recovery and liberalize existing U.S. export controls on American products with strong encryption capabilities.

### **Strong Encryption Protects Privacy In the Information Age**

As computer users worldwide become more networked than ever before - through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet - the need for strong encryption to protect their electronic information and confidential business information becomes ever more important. Companies, governments and individuals now realize that they can no longer protect data and communications from others by simply limiting physical access to computers or by maintaining stand-alone centralized mainframes. Yet they understandably do not want to put sensitive information on line without the best assurances that that information will remain private. A recent Business Week poll, "A Look at On-

Liners", found that if privacy were protected, 61 percent of those who currently do not go online would be more likely to start using the Internet, and 78 percent of those who already do go online would be more likely to use the Internet more often.

Consider the New York State Department of Health which is developing the New York State Childhood Immunization Program to track immunization records of children. No matter what clinic, hospital or doctor's office a child visits, a doctor or nurse need only pull up that child's records to determine whether he or she ever got the right shot or is due for booster shots. Because of the highly sensitive nature of the information and because the system will catalogue the names and addresses of the state's children, strong encryption is being used (and no key recovery will be incorporated into the system).

Similarly, doctors have noted that if they have access to even limited clinical information about a patient, especially in an emergency situation (such as pertinent drug information, recent lab tests, or radiology results), they could save billions of dollars by not initiating unnecessary or repetitive procedures.

Encryption provides assurances that the people updating medical records are authorized to make those changes. Encryption also assures that the personal information can neither be viewed or modified by unauthorized parties.

So, too, encryption is becoming vital to the banking and financial services industry. Today, cash is distributed electronically; banks clear and settle their funds electronically, as well. PC/Internet banking is quickly emerging as an alternative to in-person banking or even ATM transaction banking. In fact, one global banking firm recently indicated that 80% of its transactions worth trillions of dollars are

routinely conducted electronically.

The U.S. Government recognizes the threats hackers pose in the new digital world. In fact, FBI Director Freeh testified that "illegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as 'electronic intruders' responsible for penetration of many of America's computer networks. It is estimated that the Pentagon's computers are subject to hackers' attempts 250,000 times a year." Recently, defense sources said approximately 11 Department of Defense sites were attacked -- computers which are used to transmit logistics data as well as pay and personnel information. Deputy Defense Secretary John Hamre has acknowledged that DOD recently has undertaken several exercises that confirmed DOD's vulnerability to computer attack in the future.

Information security is critical to the integrity, stability and health of individuals, corporations, and governments. While cryptography is but one element of security, it is the keystone of secure distributed systems. For these reasons, corporations are now demanding 128-bit encryption.

### **Encryption Is Necessary to Prevent Crime And To Promote America's National and Economic Security**

The interests of computer users, hardware and software companies and privacy groups, therefore, are not opposed to those of law enforcement and national security. As the blue ribbon National Research Council (NRC) Committee found in its May 1996 CRISIS Report ("[Cryptography's Role in Securing the Information Society](#)"), encryption prevents crime by protecting the trade secrets and proprietary information of businesses and correspondingly reducing economic espionage.

Encryption also promotes the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of more widespread use of encryption outweighed the disadvantages and that the U.S. Government has "an important stake in assuring that its important and sensitive . . . information . . . is protected from foreign government or other parties whose interests are hostile to those of the United States."

In 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks. We may see many, many hundreds of millions in losses, and we may possibly see the destabilization of a company, the stock market or perhaps even a whole economy.

To counter these threats, corporations "compartmentalize" their critical business information, and strictly control access to these compartments. Not everyone is trustworthy within a company, and it is this security, this compartmentalization, that prevents crimes such as insider trading, leakage of trade secrets, and corporate espionage. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime through these networks.

Widespread use of encryption is also necessary to protect the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets which are highly vulnerable. Indeed, the U.S. General Accounting Office in its report issued in May of 1996 entitled "*Information Security*:"

*Computer Attacks at Department of Defense Pose Increasing Risks,"* found that:

- Computer attacks are an increasing threat, particularly through connections on the Internet;
- Such attacks are costly and damaging; and
- Such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

Furthermore, U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Thus, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies loose. Continuing down their present path will be more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

### **The Administration's Key Recovery Scheme Does Not Meet Demands for Privacy**

The Administration's key recovery scheme is too complex and inherently too vulnerable. Technologically, it will not work on the scale required, and users do not want it. Let me explain why.

*First, a huge bureaucracy will be necessary to manage the Administration's key recovery scheme.* The Administration's proposal assumes that we can effectively accommodate the needs of dozens of governments, thousands of companies, tens of thousands of law enforcement offices, and millions of users. It also assumes that we can handle tens of millions of public-private key pairs and billions of recoverable session keys across thousands of different products. As the number of people using

computers and the Internet grows, the number of keys that must be managed will explode. By the end of the decade, a key recovery system capable of accommodating all of the potential users around the world would have to be capable of handling many, many billions of keys. This is a very tall order. The bureaucracy to manage this key recovery system is likely to rival that of the Social Security Administration, the Internal Revenue Service, or the U.S. Postal Service.

*Second, the technology does not yet exist to create and smoothly operate a reliable system of this magnitude and complexity.* Furthermore, the Administration's proposed key recovery scheme may actually make consumers more vulnerable. Advocates of a worldwide key recovery system conveniently overlook the tremendous technical barriers posed. It is unclear that such a system can be built at all, much less in the next few years. As Novell's CEO, Dr. Eric Schmidt stated, "Perhaps the technology necessary to create such a system will be available in my lifetime; it is not available today."

Cryptography experts report that "secure cryptographic systems are deceptively hard to design and build properly . . . Very small changes frequently introduce fatal security flaws . . . [A]dding key recovery makes it much more difficult to assure that such systems work as intended. It is possible, even likely, that lurking in any key recovery system are one or more design, implementation, or operational weaknesses that allow recovery of data by unauthorized parties." (See [The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption](#), A Report By An Ad Hoc Group of Cryptographers and Computer Scientists, May 1997.)

*Third, despite widespread claims of international agreements on "key recovery" infrastructures, no such agreements exist today.* Bilateral and/or multilateral agreements must be negotiated and

foreign governments' rights and responsibilities must be defined before the Administration's key recovery system can be realized. Despite years of insisting that these treaties were just around the corner, the Administration has yet to conclude a single bilateral, much less multilateral, agreement with another government on key recovery. Nor has the Administration outlined any rights or responsibilities for foreign governments requesting access to U.S. decryption keys held by key recovery agents. It is not even clear whether these keys are subject to civil discovery in addition to criminal discovery.

Ministers and business leaders from 30 European nations attending an Internet conference in Bonn, Germany, roundly criticized the U.S. key recovery policy that requires guaranteed access for law enforcement. The ministers agreed in the Bonn Declaration that "they will work to achieve international availability and free choice of cryptography products and interoperable services, subject to applicable law, thus effectively contributing to data security. If countries take measures in order to protect legitimate needs of lawful access, they should be proportionate and effective and respect applicable provisions relating to privacy." The German Economics Minister, Guenter Rexrodt, in fact opened the conference by calling for the removal of restrictions on encryption technology. (*See Should Encryption Software Have Limits?*, MSNBC Reuters Report and Jack Breibart, *Europeans Hit U.S. Encryption Policy*, American Reporter Correspondent.)

*Finally, criminals and terrorist groups will avoid using the Administration's key recovery scheme.* The stated purpose of the Administration's key recovery scheme is to strengthen law enforcement and national security. But it is unlikely that criminals and terrorist groups will choose to use a key recovery system that requires them to provide their keys to third-parties

who can, in turn, give them to government officials. At the same time, it is impossible to force criminals to use a key recovery system!

Unfortunately, other similar attempts at forcing key recovery also are fatally flawed. The Secure Public Networks Act, S. 909, as adopted by the Senate Commerce Committee promotes, through the use of heavy handed incentives, the Administration's mandated third party key recovery access. It is a significant step backwards for American consumers. In fact, far from being a compromise, S. 909 is actually worse than the status quo. The bill attempts to set up an extremely complex domestic key recovery system that puts at greater risk the privacy of all Americans. This complex a key recovery scheme will inevitably sacrifice business and consumer's security and unnecessarily drastically increase their costs. At the same time, S. 909 does not ensure easy exportability of stronger encryption or otherwise meaningfully relax export restrictions.

### **Export Controls on American Products with Strong Encryption Must Be Modernized**

The incredibly dynamic U.S. computer software industry is an American success story. Since 1980, the industry has grown seven times faster than the rest of the economy and today is larger than all but five manufacturing industries. Conservative estimates are that more than 1.2 million people are employed in the software, hardware, and semiconductor industries - with more than half a million people in the computer software industry alone. This economic success has fueled research and development for new generations of products and spurred the creation of numerous market-leading products and choices.

The computer software industry is one of our country's most internationally competitive. Presently, U.S. software accounts for over 70% of the world

market, with exports of U.S. software programs constituting half of many software companies' revenues. The incredible growth of the industry and of its exporting success benefits America through the creation of jobs, highly-skilled, well-paid jobs, here in the United States.

But, unless the government's export control policy changes, we will lose our competitive advantage. American software companies are still forced to limit the strength of our encryption to the 40-bit key length level set in 1992 - despite an Administration commitment at that time to increase key lengths regularly to take into account technological and market developments. Recent regulations from the Administration allow, on a limited company-by-company basis, the export of products with 56-bit encryption capabilities in exchange for proof of commitments to build "key recovery" into future products. However, not only do customers demand encryption stronger than 56-bit, but this license exception is set to expire in December, 1998. Furthermore the Administration has defined "key recovery" in its own terms, not in consumer-driven terms, and so promoted the development of features for which there is no demand. Thus, 40-bits remains the effective level for which easy export is still permitted.

The results of these continuing, unilateral U.S. export controls on American computer software and hardware with encryption capabilities has been two-fold.

*First, the U.S. government has succeeded in delaying the widespread deployment of American products with strong encryption within the U.S. as well as abroad. Why? Because American companies manufacturing mass market products for the world market find it extremely inefficient and difficult to develop, market, and support two versions of their product -- one for the U.S. and one abroad. Recently,*

some companies have had to go down this route or risk losing purely domestic sales! But this does not help customers with global operations and interests who demand the ability to securely interact worldwide. American companies can only offer these customers products with 40-bit encryption!

For example, a U.S. design company which builds highways, bridges, and dams in foreign countries would like to design its projects here in the U.S. and transmit those designs to foreign countries. Unfortunately, because of the sensitive nature of the information, they would have to use strong encryption with no key recovery - which is prohibited by the U.S. government. Thus, those design jobs go overseas where plans can be designed and developed in a safer atmosphere.

*Second, the U.S. government has succeeded in giving foreign companies a major market opportunity.* The General Accounting Office concluded in 1995 that sophisticated encryption software was widely available to foreign users on foreign Internet sites. A 1996 Department of Commerce study confirmed the widespread availability of foreign manufactured encryption programs and products. The most widely used encryption program, PGP, with over two million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key. An on-going industry study by Trusted Information Systems (TIS Study) revealed that as of September 1997, there were 653 foreign programs and products available from 29 countries, 275 of which employ DES.

In short, U.S. companies can only sell a product that is inferior to the most popular products already available. It is like being forced to sell a car without bumpers and seat belts in a world which demands safer and safer cars. As a result, American companies face strong competitive disadvantages overseas and are losing product sales every day because of current

encryption export controls.

## **Conclusion**

The time for action is now. Privacy must be assured, crime prevented and national security promoted. U.S. export controls are inhibiting the use of products with strong encryption domestically. They must be immediately updated to reflect technological and international market realities and enable American companies to compete on a level playing field. Domestic controls in any form that have the effect of forcing the inclusion of back doors must be opposed. It is hard enough to do security right when the sole focus is protecting information -- it is incredibly more difficult to do so if one is forced to do so in a key recovery climate. Instead, it will open up our electronic information to unnecessary and potentially harmful vulnerabilities and insecurities, thus posing an even greater risk to our national and economic security.

Thank you.

---

## **Footnotes**

1 The BSA promotes the continued growth of the software industry through its international public policy, education, and enforcement programs in 65 countries throughout North America, Europe, Asia and Latin America. BSA worldwide members include the leading publishers of software for personal computers, including Adobe, Apple Computer, Autodesk, Bentley Systems, Lotus Development, Microsoft, Novell, The Santa Cruz Operation and Symantec. BSA's Policy Council consists of these software publishers and other leading computer technology companies, including Intel, Compaq and my company Sybase. .