

NLWJC- Kagan

Counsel - Box 006 - Folder 005

Encryption bill

## ON THE NET The F.B.I. sting operation on child pornography raises questions about encryption.

**F**EDERAL agents swooped down on more than 125 homes and offices across the United States on Sept. 13, seizing computers and diskettes from people suspected of trafficking in child pornography over the America Online network. But to date, the number of arrests in the sting operation remains at 15.

More arrests are expected, but why haven't more occurred?

Last week, Louis J. Freeh, the director of the F.B.I., offered an oblique explanation for the seemingly low initial success rate.

At least some of the suspected child pornographers had used data encryption software, Mr. Freeh said Thursday in remarks at an International Cryptography Institute conference in Washington. In other words, they had scrambled their computer files so that only someone with the password — or with proper code-breaking skills — could view the contents.

Mr. Freeh wisely did not say whether the F.B.I. agents were able to decipher the encrypted files seized in the investigation. It would be foolhardy, from a law-enforcement perspective, to tip one's hand.

If the head of the F.B.I. acknowledged that his agency was powerless to crack a cryptography program like Pretty Good Privacy, the stampede for that software on the Internet would make the run on Windows 95 look puny.

From a political perspective, Mr. Freeh's coyness is shrewd as well. By making even a subtle suggestion that some child pornographers may walk free because of unbreakable cryptography, he gains more leverage in seeking Government-mandated controls over the use of encryption technology.

Mr. Freeh said that encryption was a "public safety" issue, and he said law-enforcement agencies around the world "will not tolerate" the use of private data encryption to impede investigations. He said encryption had also been encountered in the Philippines in a plot to blow up an American jet and to assassinate Pope John Paul II. (In that case, at least, one can presume the code was cracked.)

It seems worthwhile to point out that even if the suspects in the child pornography sting, called Operation Innocent Images, used cryptography, that did not provide evidence that they were doing something illegal. Our legal system is predicated on the belief that one is innocent unless proved guilty, and there is no exception clause for technology.

"Fortunately we are not yet at the point where the mere use of encryption overcomes the presumption of innocence," said David Sobel, staff counsel for the Electronic Privacy Information Center in Washington.

Another point to remember is that the F.B.I. identified more than 100 suspects, and gathered sufficient information to warrant raids, using existing laws and enforcement techniques. On the other hand, there is no denying that child pornographers use data encryption to keep co-workers, family members and police from discovering their secrets.

"We are involved in a couple of jobs every week resolving some kind of a child pornography investigation," said Eric K. Thompson, president of Access Data Inc. of Orem,

Utah, a private company that specializes in cracking encrypted files for corporations and Government agencies.

The Government's elite code-breakers at the National Security Administration are prohibited by law from using their talents against American citizens. The F.B.I. has its own code-cracking experts, but it routinely calls on independent experts like Access Data to help on some cases.

After eight years of breaking into encrypted files, ranging from situations involving secretaries who simply forgot their passwords for important memos to cases involving corporate computer systems that were encrypted by disgruntled employees, Mr. Thompson has concluded: "Basically, the criminal element is becoming more computer literate, and they are discovering encryption. Files are becoming more difficult to break."

Dorothy Denning, an expert in cryptography and a professor of computer science at Georgetown University in Washington, said she recognized the importance of encryption for businesses seeking to protect information. At the same time, she said, she also recognized the problems that law-enforcement agencies face because of cryptography.

"So many people had been saying people in law enforcement weren't having this problem, and I didn't believe that," Dr. Denning said. So in May, she said, she spent two days calling sources at law-enforcement organizations. "I came up with over 20 cases — child pornography, terrorism, murder, embezzlement, fraud, tax protesters, export violations — and, in some cases, they were able to crack it, and others they couldn't," she said.

What can be done? The Administration's plan is to seek voluntary compliance with a "key escrow" plan, which would enable citizens to use strong, private cryptography as long as a copy of the software "key" were made available to law enforcement officials.

Last week, Mr. Freeh stressed that he preferred a voluntary approach. But "if consensus is impossible" on the encryption issue, he said, the F.B.I. might consider other approaches.

The debate is certain to heat up as more information about Operation Innocent Images becomes known. There are no comforting answers, only an echo of advice from a time predating the Internet: There is no solution. Seek it wisely.

# Congressman Heads to Trial In California

## Defense Cites Issues Of Unequal Justice

By KENNETH B. NOBLE

COMPTON, Calif., Sept. 24 — In an unusual prelude to the extortion trial of Representative Walter R. Tucker 3d, lawyers asked prospective jurors whether they believed black politicians were targets for "takedown" by the Federal Government more often than their white counterparts.

The question is at the heart of Mr. Tucker's contention that as a black man representing a Congressional district with one of the largest black populations in the nation, he is the victim of overzealous white prosecutors. Jury selection was completed last week, and the trial is expected to begin in earnest on Monday.

Prosecutors have said they have thousands of documents and many hours of clandestine videotape and audiotape evidence that show the 38-year-old second-term Democrat taking \$37,500 in bribes and soliciting another \$250,000 in kickbacks from two waste disposal companies while he was the Mayor of Compton. Compton is the largest city in Mr. Tucker's district, which encompasses industrial suburbs south of Los Angeles.

If convicted on all counts, he could be sent to prison for up to 246 years and fined as much as \$2.7 million.

The often technical financial aspects of the case have been overshadowed by emotionally fraught legal, political and racial issues. Mr. Tucker, a lawyer and Baptist minister trained at Princeton and Georgetown Universities, is the youngest member of a powerful political dynasty, a family that has been described as the "Kennedys of Compton."

From the start, he has said the prosecution was the result of bias.

"Look at the list," Mr. Tucker told reporters recently on the front steps of the Federal courthouse in Los Angeles. "There was Marion Barry before me. There was O. J. Simpson before me. There was Mike Tyson and Mike Jackson. You may as well call me Mike Tucker."

In response to questions suggesting that some people might interpret the Government's efforts as an attempt to bring down a black official, the chief prosecutor in the case, Nora M. Manella, recently told reporters that her office was "an equal opportunity prosecutor."

In any event, Mr. Tucker's statement that black politicians are targets of unfair prosecution resonates powerfully in this predominantly black city of about 92,000, where he and his family have long commanded respect for championing black causes and for building a potent political machine. Mr. Tucker's father was a former school board member and Councilman who served as Mayor until his death in 1990.

The extent of that power was evident earlier this month outside the courthouse, where Tucker supporters, who include local businessmen and ministers, carried placards saying "Stop Racism" and "Witch Hunt."

The case has attracted not only local but also national attention because of what some blacks see as a pattern of the predominantly white

Federal law-enforcement establishment spending time and money prosecuting cases against blacks and members of other minority groups that it might not have pursued against white leaders.

Going back to Adam Clayton Powell Jr., the revered Harlem Congressman who was indicted on charges of tax evasion more than three decades ago, there have been 6 blacks among the 70 members of Congress indicted; according to the Joint Center for Political and Economic Studies, a Washington research organization. In other words, about 9 percent of those indicted have been black.

And when Hispanic members of Congress are included, the figure rises to about 15 percent — in a period when the number of black and Hispanic members of Congress accounted for less than 5 percent of all lawmakers.

Of the black Congressmen, Charles Diggs of Michigan and Mel Reynolds of Chicago were convicted, but the other three, Representatives Harold Ford of Tennessee, Floyd H. Flake of New York and Mr. Powell, were either acquitted or set free after a hung jury.

"Historically, African-Americans have had reason to question the criminal justice system," said Leo Terrell, a black civil rights lawyer in Beverly Hills, Calif. "So it is always reasonable to at least raise the racism issue."

Royce W. Esters, president of the Compton chapter of the National Association for the Advancement of Colored People, agreed. "They are targeting Compton because there are a lot of black people here," he said. "Every time there is a black person in a high place they try to get them."

Prosecutors will not comment on the evidence they plan to present. But court documents indicate that the investigation videotaped meetings in which Mr. Tucker appeared to take money from an undercover agent with the understanding that he would put certain items on the Compton City Council agenda.

Mr. Tucker and his lawyer have yet to offer any evidence that Federal officials are motivated by racism, except to loudly and repeatedly declare that they know it is true.

"I think that the case will show that I have been targeted, and I am obviously an African-American," Mr. Tucker said in an interview, kneading the air with long fingers. "I can tell you that based on the information I have, the city of Compton, over the years, over the last decade, has been targeted, and the city obviously is one associated with African-American leadership."

He talked at a table in his spacious office in a shopping center here. Hanging on the crowded walls were plaques from civic and political groups praising his community spirit and achievements. Renowned locally as an animated, charismatic speaker, Mr. Tucker was uncharacteristically subdued.

And then, lapsing into the language of the pulpit, Mr. Tucker added: "Even though my enemies have meant this for evil, God has used it for good, and it has strengthened me, it has made me stronger in the Lord. It's made me stronger in my resolve about what my life has meant."

This is not the first time Mr. Tucker has been charged with a crime while in government. An assistant district attorney from 1984 to 1986, he was dismissed after changing the date on a photograph being used as evidence in a narcotics case, reportedly in an attempt to cover up the fact that he had withheld the pictures from the defense. Accused of altering an official document and lying to a judge, he pleaded no contest to misdemeanor charges and did not serve any time in prison.

Despite the tampering charge, Mr. Tucker's political career flourished. In 1991 he was elected Mayor of Compton, succeeding his father. A year later Mr. Tucker survived a bitter Democratic primary fight and was easily elected to Congress. He was re-elected last year.

But Mr. Tucker's rise coincided with a series of scandals. In 1993, Compton became the only school district ever certified by the state as an academic and financial disaster. At about the same time, Patricia Moore, a Tucker family ally and one of the city's most prominent politicians, was indicted on Federal bribery charges.

In recent weeks, the United States Attorney's office appears to have intensified its investigation of city politics. On Aug. 29, Joseph Scraggins, a former owner of a Compton-based construction company, pleaded guilty to conspiring with Mr. Tucker to extort money from a business trying to build a waste-to-energy plant in Compton. Mr. Scraggins also pleaded guilty to filing a false Federal income tax return. Lawyers for Mr. Scraggins have said he would testify at the Tucker trial if subpoenaed.

Three days later, in a potentially even bigger blow to Mr. Tucker's case, Ms. Moore was charged again with bribery. One company from which Ms. Moore is charged with extorting money is Compton Energy Systems, the same business named in Mr. Tucker's case.

THE NEW YORK TIMES, MONDAY, SEPTEMBER 25, 1995

## Feds and private sector at odds over coded computer messages By Rory J. O'Connor Knight-Ridder Newspapers

WASHINGTON The battle over privacy on the Internet is about to get hot again, one year after the federal government appeared to abandon a controversial plan that would hand law enforcement agencies the "keys" to decipher all scrambled computer communications.

Civil libertarians fear the revival of the plan called key escrow encryption would put the government in a potential Big Brother role on the information highway.

That puts them at odds with law enforcement agencies, who insist the plan is necessary to prevent criminals like drug dealers and terrorists from proofing their electronic communications from police wiretaps.

In the middle are private individuals and businesses who want to secure their electronic mail and on-line business transactions from prying hackers, thieves and disgruntled employees but may find the government trying to mandate how they do so.

"It would be the equivalent of saying homeowners have a right to have secure locks to their homes, but (to get them) they have to give a set of keys to law enforcement or some other party dictated by law enforcement," said David Sobel of the Electronic Privacy Information Center (EPIC) in Washington, which opposes the key-escrow plan.

Still others argue that an encryption plan that has duplicate keys would be welcome not just by law enforcement. They said it would be favored by large corporations as protection against employees using encryption to commit fraud, or to let the company recover encrypted documents in case of the untimely death of a key executive.

"There's an investigation right now where an employee was unhappy with his company and encrypted all its (program) files, and said, 'How much will you pay me for the key?'" said Stewart Baker, former general counsel of the National Security Agency, which developed the government's key escrow algorithm. "That's a good reason to have key escrow."

The National Institute of Standards and Technology, an arm of the Commerce Department, plans to hold a two-day workshop next week on key-escrow technology. It is the first high-profile discussion of the idea since the Clinton administration withdrew its original proposal last July.

"We want to get a dialogue moving again, to come up with what we see as good guidelines for cryptography," said Anne Enright Shepherd, a spokeswoman for the NIST. "Key-escrow is something the government is still very interested in."

That has groups like EPIC concerned that the administration is taking the first step toward what law enforcement agencies would like: developing a key-escrow system that the computer industry would accept, then making other encryption schemes illegal to use.

"They're attempting to make the concept of key escrow more palatable to industry, and so far they've had some success," Sobel said. "But it's clear that ultimately, for it to work, (key escrow) has to become mandatory."

According to documents obtained by EPIC under the Freedom of Information Act, the FBI and other agencies have repeatedly recommended to the White House that the key-escrow plan be made mandatory.

The NIST's Shepherd said the administration has not changed its position of last year, that key escrow would be "voluntary for public use." She said the documents "reflect an internal discussion" within the administration, not a proposal. And Baker said the new proposal would not be a mandate, and that partial corporate adoption of it would prove valuable to law enforcement even if other encryption methods remain legal.

But the government would probably insist that anyone doing business with it use key escrow, meaning that industry might simply eliminate other offerings instead of spending the money

to make products that incorporated two encryption systems.

Key escrow is just one of many schemes that have been developed by cryptographers to scramble the contents of an electronic message so they cannot easily be read by unauthorized people. Like most of the other systems, it relies on a mathematical formula called an algorithm to encipher the message, and a secret "key" the recipient uses to decipher it. Without the key, anyone trying to read the message would see only gibberish.

That is not much different than the way people have tried to keep their communications private for centuries. But codes that humans or even simple machines could create have been broken by determined cryptanalysts. It is the power of the computer to scramble messages quickly and cheaply with incredibly complex formulas that worries law enforcement agencies. They fear they will be unable, even with the most powerful computers, to conduct successful wiretaps.

(EDITORS: STORY CAN END HERE)

Thus, as long ago as the beginning of the Bush administration, the FBI and other agencies pushed for the government to adopt an encryption scheme under which the keys would be held not only by the recipients, but also by independent "escrow" agents. If the police obtained a court order to conduct a wiretap on someone, they could present the order to the escrow agents and obtain the keys needed to unscramble the person's messages.

When the plan was finally proposed publicly in 1993, it raised howls of protest from civil libertarians, academics, computer users and the computer industry. Their basic complaint: allowing the government to hold the key to one's private communications invited abuse and illicit spying. They also questioned the security of the government's algorithm, which has been kept from public scrutiny as classified. *Encryption w/*

The administration eventually withdrew the plan, and another scheme called public key cryptography became the most popular way for individuals to scramble their communications. With the public key system, only the individual recipient knows the key for unscrambling a message; not even the sender of the message can read it once scrambled. It can be used to authenticate messages, and if employed properly is considered by most cryptographers to be unbreakable.

Companies like Apple Computer and Sun Microsystems bundle public key systems with many of their computers sold domestically—it is illegal for U.S. firms or citizens to export the technology—and companies like Netscape Communications rely on the scheme as the basic protection for their Internet software. They are unlikely to favor abandoning the scheme for one that has created such controversy.

A Netscape spokesman said Thursday that the company would be willing to sell a commercial key escrow system to someone who wanted it, but the company remains strongly opposed to a government mandated system.

The government has tried to anticipate that. The proposals for the NIST workshop include discussions that would remove some of the objections raised to the original plan. Among them would be designating private entities, rather than government agencies, as escrow agents, and increasing the complexity of the key to make messages more secure. The government is also proposing a plan to allow companies to export a more robust version of the system, although many companies maintain there is no foreign market for a protection scheme designed by the U.S. government whose algorithm is classified.

But even these changes do not satisfy privacy advocates, some of whom see any key escrow system as basically flawed.

"The NIST process is important because it is a forum to address these concerns, and we haven't gotten good answers to many of our questions yet," said Jonah Seiger, policy analyst for the Center for Democracy and Technology in Washington. "There are still many issues, notably what would be the

obligations and practices of escrow agents, and what procedures would law enforcement have to do to get the keys."

Even if those are answered, the plan is still likely to face opposition, especially any indication that the system would be made mandatory or established as the de facto standard.

"We certainly believe that everybody should be allowed to use whatever form of cryptography they want," he said.

---

## **NATO bombs rebel Serbs for 2nd day By Fawn Vrazo Knight-Ridder Newspapers**

ZAGREB, Croatia NATO fighter pilots bombed rebel Serb positions around the beleaguered Bosnian capital of Sarajevo Thursday for the second straight day, clearly hoping to pummel the Bosnian Serbs into substantive peace talks.

NATO officials did not divulge details of the latest attack, with Capt. Jim Mitchell, an alliance spokesman in Naples, Italy, saying only: "We have done some air strikes today. I'm not going to get specific on when or where."

The bombing hampered for much of the day by bad weather resumed in the afternoon even as American officials shuttled from city to city in the war-torn land that once was Yugoslavia searching for a peaceful settlement.

After meeting Wednesday in Belgrade, the Serbian capital, with Serbian President Slobodan Milosevic, Assistant U.S. Secretary of State Richard Holbrooke was in Zagreb, the Croatian capital, Thursday for talks with Croatian President Franjo Tudjman and Bosnian Muslim officials.

Holbrooke called a decision by Milosevic to begin representing rebel Bosnian Serbs in peace negotiations "a procedural breakthrough, but only a procedural one. ... Tough negotiations lie ahead."

Western officials did announce one bit of welcome news: Bosnian Serb television displayed videotape Thursday showing the five European Union monitors who were feared dead were still alive. A Bosnian Serb official said the five were heading for home, although that news could not be independently confirmed, the Associated Press reported. The Serbs had said Wednesday that the five were killed during the initial wave of air strikes.

Meanwhile, NATO jets continued to search for the two French pilots who were shot down Wednesday, but there was no word on their fate.

NATO planes began their strike the largest in the group's 46-year history early Wednesday morning to retaliate for a Serb mortar attack that killed 38 people in a crowded Sarajevo market. The stated goal of the attacks was to force the Serbs to pull heavy weapons out of the Sarajevo area and stop attacking the other three remaining U.N. "safe areas" in Bosnia.

A U.N. official said peacekeepers observed the Bosnian Serbs moving some heavy weapons north away from Sarajevo and out of the 12½-mile exclusion zone the United Nations hopes to impose around Sarajevo. The official, who spoke to the Associated Press on condition of anonymity, said the U.N. had not received any word from the Serbs that they were doing it to comply with demands of the United Nations or NATO.

NATO officials, who released aerial films of Serb targets exploding like huge white flowers as they were hit, were vague about the scope of the bombing.

"We obviously missed some targets," said U.S. Adm. Leighton Smith, NATO's southern Europe commander. "But overall, we're being very successful."

The Bosnian Serb rebels, who earlier suffered a humiliating defeat at the hands of Croatian forces who kicked them out of strongholds in northern Croatia last month, have sent mixed messages in response to the Western attack.

Bosnian Serb leader Radovan Karadzic said Thursday in a letter to the U.N. chief for former Yugoslavia, Yasushi Akashi, that his forces would not fire artillery at Bosnian "safe areas." But he added that if the NATO attacks continued, it would

"have the effect of hastening our preparations for a long-term conflict that the international community has no hope of winning."

By late Wednesday, NATO had conducted more than 300 flight missions over Bosnian Serb territory a third of those to drop bombs. The Serbs reportedly fired back fewer than 30 air defense missiles. Only one of those missiles hit its target Wednesday: the French fighter-bomber.

President Clinton, speaking in Honolulu, praised the allied bombing as "the right response to the savagery in Sarajevo."

"The campaign will make clear to the Bosnian Serbs that they have nothing to gain and everything to lose by continuing to attack Sarajevo and other safe areas and by continuing to slaughter innocent civilians," he said.

---

## **Chinese police allow activists to protest during women's conference By Loretta Tofani Knight-Ridder Newspapers**

HUAIROU, China Participants in the international women's conference clashed with Chinese police Thursday over the issue of free speech at the conference.

At one point a plain clothes police officer wrestled with women for possession of a videotape that dealt with China's abuses in Tibet, including the imprisonment and torture of Buddhist nuns.

The women won the wrestling match and kept possession of the tape. Later, they lodged a complaint with conference organizers, charging China with violating U.N. rules on freedom of expression at the conference.

Two demonstrations Thursday by members of the human rights group Amnesty International were uninterrupted by police, although they intentionally violated the ground rules set down by Chinese authorities for demonstrations.

The clash over the videotape brought to a climax the tension that has been brewing all week between China, which does not allow political dissent, and conference organizers, who have insisted on freedom of speech and assembly for their delegates.

The U.N. 4th World Conference on Women does not begin until Monday, but a related group, the NGO Forum, composed of advocacy groups known as NGOs (nongovernmental organizations), began meeting Wednesday.

Thursday, about 100 Forum delegates packed into a room for the showing of the tape on Tibet. After the viewing, Elizabeth Fabel of Boston said: "Someone said, 'get the tape, get the tape.' I stuck my hand in for the tape, and a plain clothes police tried to grab it from me. I struggled with him, and then a Westerner grabbed it."

A woman in the audience, Jimpa Tenzin of Canada, said the plain clothes officer "tried to take the tape from us." Then, she said, "someone threw the tape, and someone else caught it and ran out of the room."

"He didn't know who took it," she said.

During the showing of the videotape, Jimpa said, a different plain clothes police officer stood in the audience, a videocamera on his shoulder, and tried to film the videotape. A conference organizer asked him to stop, and he did.

The videotape, called "Voices in Exile," featured Tibetan women refugees. Some of the refugees had wanted to attend the conference in person but were denied visas by China. On the tape, the women tell stories of how and why they escaped from Tibet to India.

Two of the women on the tape were Tibetan Buddhist nuns who said they were tortured in prison after being jailed for chanting "Free Tibet" in public. Another woman on the tape said she was imprisoned for 30 years. She was part of the resistance movement that began after China occupied Tibet in 1950.

The videotape was brought to China by Tibetan refugees who had gained admission to the conference by not identifying

# Compromise Bills Due on Data Encryption

## Industry Opponents and Civil Libertarians Are Lukewarm, at Best

By JOHN MARKOFF

Legislation will be introduced in the House and the Senate tomorrow in an effort to break the deadlock between the computer industry and the Clinton Administration over the control and export of software and hardware used to scramble electronic data.

So far, though, the proposed measures have received only cautious endorsement from industry executives, while civil-liberties and privacy groups say they are worried that the bills would enable the Government to decode scrambled transmissions.

Senator Patrick J. Leahy, Democrat of Vermont, and Representative Bob Goodlatte, Republican of Virginia, plan to introduce similar bills that affirm the right of Americans to use any type of data-coding equipment without restriction and prohibit the mandatory use of special keys that would allow law-enforcement agencies to read scrambled data. Their bills would also make it a crime to

use encryption technology in committing a crime and would permit the export of data-coding software and hardware if similar technology was available from a foreign supplier.

Data-coding, or encryption, technology is based on mathematical formulas that rely on the immense computing challenge inherent in factoring large numbers. Until recently, such technology was largely used by military and intelligence organizations and by some corporations like banks. As electronic mail and commerce have become increasingly accessible, however, the technology has become more controversial.

In April 1993, the Clinton Administration proposed a national data-encryption standard known as Clipper, based on a system that would have made it possible for law-enforcement agencies, if authorized by a court, to decode private voice and data communications.

The Clipper initiative has been strongly opposed by industry executives and privacy advocates. They argue that reliable coding technology is essential for commerce and

privacy protection on the Internet. They also say that strict export rules are increasingly hindering the ability of United States corporations to compete with foreign suppliers.

The proposed legislation would ease some current restrictions on the exporting of data-coding systems, but civil libertarians still see areas of concern.

"The bills relax export controls, which is clearly a step in the right direction," conceded Marc Rotenberg, director of the Electronic Privacy Information Center, a Washington research and policy organization. But the negatives, he said, were that the bills opened the door to Government access to private transactions "and criminalize the use of cryptography when it is used to perpetrate a crime."

Industry officials said they expected the legislation to stir little enthusiasm from corporate users. "Corporate America is absolutely unwilling to give a third party control of their data," said Jim Bidzos, chief executive of RSA Data Security, a maker of encryption software based in Redwood City, Calif.

# Capitol Staffs Find Overtime Is Hard to Get

By ADAM CLYMER

WASHINGTON, March 3 — As Congress begins to apply standard labor laws to its own employees, Senators and Representatives have decided to make fewer than half of their personal staff members eligible for overtime pay.

The Congressional Accountability Act, the first bill passed by the 104th Congress more than a year ago, requires Congress to apply many labor laws that used to affect only private businesses to itself. One of those laws is the Fair Labor Standards Act, which generally requires time-and-a-half pay for work beyond 40 hours a week. The accountability act went into effect in January.

A voluntary study released today by the Congressional Management Foundation showed that in 11 percent of House members' offices, either one staffer or none was designated as eligible for overtime pay. The foundation is a privately financed organization that tries to educate Congress on running its business.

The study, based on questionnaires answered by 38 percent of the House members and 55 senators, found that 47 percent of the Senate staffers in those members' offices and 38 percent of their counterparts in the House had been made eligible for overtime pay. The remainder, generally in higher-ranking and higher-paid jobs, have been exempted as professional staff.

Representative Christopher Shays of Connecticut, the leading Republican sponsor of the accountability act, said he thought the survey showed that Congress was approaching the law responsibly. But there might be more evasion than the survey showed, he said, because the offices that volunteered to answer the questionnaires are the ones most likely to have taken the bill seriously.

Rick Shapiro, executive director of the foundation, said the study showed that members were recognizing that the law applied to them and not just to the general work force on Capitol Hill, which includes maintenance employees and police officers. When the bill was enacted, many lawmakers said it would affect those workers most.

But Mr. Shapiro acknowledged that the survey also showed that some representatives were not going along with the changes. Out of the 167 questionnaires returned voluntarily by House offices, 8 indicated that all staff members in the office were exempt. In 11 more offices, he said, only one worker was not exempt from overtime. The surveys were anonymous, he said, so he could not identify or describe those members.

Representative Barney Frank of Massachusetts, the leading Democratic advocate of the accountability measure, said that the percentage of exemptions was reasonable because members' staffs are small and professional. He said he still expected the greatest impact to be on Congress's blue-collar work force.

In the House and Senate offices that responded to the survey, the exempted staff members included all chiefs of staff and legislative directors and almost all press secretaries and office managers. Computer operators, office receptionists and the case workers who handle constituents' problems were almost always made eligible for overtime pay.

With the accountability act newly applicable this year, few offices have budgeted money for overtime pay. Mr. Shapiro said many were trying to schedule their staff members more efficiently to avoid doing so.

THE NEW YORK TIMES  
MONDAY, MARCH 4, 1996

# Still Waiting for a Victory But Determined to Go On

By ADAM NAĞOURNEY

ATLANTA, March 3 — By 8 P.M. on Saturday, an hour after the polls had closed in South Carolina, Lamar Alexander was in his hotel suite here, down for a night of room service and a few quiet hours of political reflection. As recently as a week ago, this was supposed to have been a big night of victory speeches and hotel ballrooms, celebrating the results of the first contest in the South and the start of a string of hoped-for victories in the corner of the country that Mr. Alexander calls home.

But it had not turned out that way, and Mr. Alexander instead found himself in a nearly empty room at the Holiday Inn Select on the outskirts of Atlanta, waiting out the remaining suspense left in his primary night to wonder, Would he come in third or fourth this time?

"I'm not happy about our result," Mr. Alexander said, leaning forward in an arm chair, his tie still tight and his shiny, black shoes still laced. Even now, after a long and distressing day, he was as earnest and disciplined as ever, methodically parrying every question about his bleak fortunes into an observation about the failings of his opponents.

"I'm in this for the long haul," Mr. Alexander said. "I have a long view. I mean, I'm the fellow who walked a thousand miles across Tennessee over six months when nobody thought it made any sense. I can go all the way to San Diego. My fundraisers are prepared to do that, and my family is prepared to do that.

"And sooner or later it's going to come down to Senator Dole and me and the issue is going to be who can beat Clinton and who can help make the Republican revolution real."

Mr. Alexander has arrived at a fateful moment in his campaign. He is a candidate whose strategy has from the start been predicated on the political collapse of his opponents, rather than any sudden rush by voters to his own campaign. And he has been forced, with each new success by an opponent, to move back the place where he will make his stand.

But now, two weeks after receiving fleeting attention from his third place finish in New Hampshire, Mr. Alexander stands alone as the only major Republican candidate not to have won a single contest. He has not even finished second. He remains the candidate on the launching pad, idle as his rivals ignite around him, resisting every day questions about whether the time had come to abandon his bid and leave the field to Senator Bob Dole, Patrick J. Buchanan and Steve Forbes.

"Sooner or later, I need to begin to do what any candidate does in a Presidential race," Mr. Alexander said with no apparent humor after addressing a listless rally at the food court of a Cobb County mall here. "I need to begin to win."

In truth, that is a variation on what Mr. Alexander has been saying for the better part of a month now. And while he had some explanations of why a Tennessean had done so poorly in South Carolina in a race against a Kansan and a Washingtonian, Mr. Alexander's poor performance in South Carolina was no surprise to anyone who has followed his lagging campaign these past few days.

The desultory rally at the Cobb Galleria Food Court this afternoon was typical of his campaign in recent days, where the crowds have been as small as those candidates find early in Iowa and New Hampshire. He has tended to go to places where he would be assured a crowd, be it a high school or an oyster roast. But even in the food court of a mall at lunch time, the audience was sparse and there were a half-dozen empty seats on the floor in front of him.

The lack of enthusiasm is infectious, and it is reflected at the top of his campaign. "I'd like to introduce you to the man who should be the next President of the United States," William J. Bennett, the former Education Secretary, said in Charleston, S.C. The phrase "should be" lending an air of plaintiveness to what should have been a stem-winder of an introduction.

Even people who are planning to vote for Mr. Alexander are growing discouraged. Jane Farrell, the director of a child-care center in Charleston, said she liked Mr. Alexander because he's a "problem solver" and she was "tired of people pointing fingers." Still, she said, this may not be his year: "I'm listening to him. I'm hoping that people will start listening to him. But maybe he has to do it again."

Through this all, Mr. Alexander seems locked in place. His rivals have all evolved these past few weeks, learning from their mistakes and failures.

Mr. Alexander has not, even in the face of evidence that he is having difficulty. His appearances still start with him awarding a red plaid shirt to a supporter, and end with him playing "God Bless America" on the piano. He tells the same stories, and makes the same jokes, tuning them only slightly to interject the name of the state he is in.

The other night at a Christian Coalition meeting in Columbia, S.C., Mr. Alexander was running through the failings of his rivals, and declared the country did not need a President who campaigned on a promise of "throwing someone out of the wagon." If Mr. Alexander realized he had by rote referred to Senator Phil Gramm of Texas, who had ended his Presidential campaign two weeks earlier and endorsed Mr. Dole, he did not show it.

If Mr. Alexander has changed his pitch at all these last few days, it is to more than ever define himself by what he is not, rather than what he is. He talks about his rivals more than they do about him.

"We have plenty of magazine salesmen," Mr. Alexander told a small Saturday morning crowd of perhaps 50 people at the Florida Coastal Law School in Jacksonville, Fla. "We got a lot of TV commentators. We have some excellent Congressional leaders in Senator Dole and Newt Gingrich. That's not what we're lacking. What we're lacking is someone to give Presidential leadership to the Republican agenda."

Mr. Alexander's candidacy has

been complicated by the fact that he has not found the South to be as hospitable as the former Tennessee governor had once hoped. Mr. Buchanan has outflanked him here, playing the kind of symbols that Mr. Alexander clearly views as a reminder of a time in his region's history that he did not approve.

There is no talk from Mr. Alexander about the Confederacy or state's rights. And even when Mr. Alexander very tentatively borrows a page from Mr. Buchanan's book — as he did in a drop-by at the Ocmulgee Gun Club in Macon — Mr. Alexander cannot pick bring himself to pick up a gun for the photographers.

It remains to be seen how successful this might be for Mr. Alexander. When he spoke at a Christian Coalition meeting in Columbia — a conservative audience that had whooped

its approval for both Mr. Buchanan and Mr. Dole earlier — a dozen people rose from their seats to leave. The audience sat silent for much of his speech, and Mr. Alexander, clearly uncomfortable, raced through his remarks.

"I don't think people perceive him as a fellow-Southerner," said former Gov. Carroll A. Campbell Jr., one of Mr. Dole's key supporters in South Carolina. "They perceive him as a nice guy."

Mr. Alexander has acknowledged that it was difficult going on, arguing that his failures so far reflected the fact that people did not know him. But as he gathered the final results in his hotel suite this weekend, Mr. Alexander rejected the suggestion that perhaps voters did know him, and had simply decided to vote against him.

"This is a long ride," Mr. Alexander said. "And as I look all the way down the road, I see Dole running out of money, I see Dole not an executive leader, I see Dole without fresh ideas. I see us raising money, I see me with fresh ideas, I see me as an executive leader, and I see a Dole versus Alexander race that I can win."

Mr. Campbell, the former South Carolina Governor, smiles at that assertion.

"He's always been praying for that to happen," Mr. Campbell said. "But it hasn't happened."

THE NEW YORK TIMES  
MONDAY, MARCH 4, 1996

# Cyberscope

RUSSIA

## Hot Copies

**W**INDOWS 95 HITS AMERICAN streets this week, but Russian computer users have had it for months. Though the final version of Windows 95 won't be released there until Sept. 1, Russians have been buying illegal copies of Microsoft's prerelease "beta" versions for as low as \$25 (compared with \$89 in



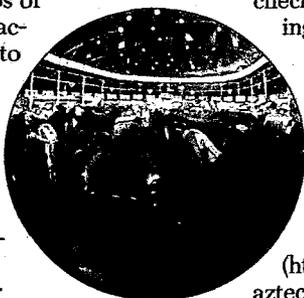
Russian vendor hawks software

the United States) at muddy outdoor software markets and kiosks. Industry experts estimate that only six of every 100 pieces of all software in Russia are originals. Moscow is cracking down, wary of being labeled a "software pirate" as it seeks acceptance to the World Trade

FAIRS

## Of Swine and Spam . . .

**T**HE ILLINOIS STATE FAIR went on the Web last year. Now about a dozen other fairs are posting Web pages—sending contest results and photos of mudslinging tractor pulls direct to your terminal. Iowa's fair last week boasted a Norman Rockwell painting sculpt-



At the Iowa fair

ed in butter, a 4-H swine-judging contest and the traditional Cowgirl Queen Crowning—on the grounds and on the Web. This week check out the Marching Elvis drill team at Minnesota's fair (<http://www.statefair.gen.mn.us/>) and the Spam Cook-off at the Nevada fair (<http://www.aztech-cs.com/nsf/>).



'This is what I do': Cryptomaster Zimmermann

ENCRYPTION

## Pretty Good Phone Privacy

**I**N THE WAKE OF REPORTS THAT THE CLINTON ADMINISTRATION is considering another Clipper-like scheme to ensure government access to encrypted conversations and e-mail, Phil Zimmermann is striking again. The 41-year-old author of the notorious PGP (Pretty Good Privacy) software program that scrambles e-mail so snoops can't read it is about to release a sequel: PGPfone, which allows people to use their computers as secure telephones. If you have a recent Macintosh (a Windows version comes next month) and a fast modem, you and a friend can speak in total privacy. As with its predecessor, Zimmermann is giving the software away, via MIT's Internet sites. Meanwhile, he's still waiting to hear whether the Feds will indict him for export violations in the distribution of PGP. Does Zimmermann worry that releasing PGPfone—which can theoretically frustrate law-enforcement wiretaps—will further inflame those who wish him arrested? "I'm a cryptographer," he says. "This is what I do."

Organization. A spokeswoman for a U.S.-based trade group of 16 software producers, including Microsoft, says: "Russia needs to get its house in order."

INTERNET

## Good Guide

**W**ITH THE WORLD WIDE Web growing faster than the weeds in your backyard, it was only a matter of time before something like the McKinley Internet Directory came along. This online guide to the Net (at <http://www.mckinley.com/>) debuted last week and on its first day received 10,000 hits. The free directory offers a one-to-four-star rating system that grades other Web sites on how complete, well organized and up to date they are. Created by a Sausalito-based Internet publishing company, the McKinley employs 30 full-time Net surfers and editors to write in-depth and time-saving text descriptions of 25,000 Internet sites, which are updated at least once a month. Yahoo—until now the only comprehensive online guide—better watch out.

ONLINE

## From Seconds Into Dollars?

**I**S AMERICA ONLINE OVERcharging its 3 million customers? California attorney Stephen Hagen thinks so. He filed a class-action lawsuit last month against the popular online service for overbilling. Hagen says that AOL's practice of charging customers by rounding up the time spent online to the next minute cost customers more than \$5 million last year. A recently issued **AMERICA Online** statement from AOL president



Steve Case defends this billing method as "common" in the industry. (CompuServe bills its customers in a similar manner, while Prodigy bills on a rounding-down basis.) Hagen is seeking damages for all AOL users. The case is pending a legal response from AOL.

JENNIFER TANAKA and TORIANO BOYNTON

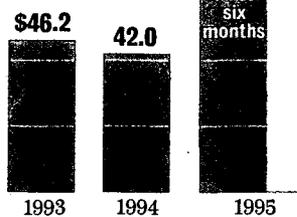
E-mail Cyberscope at [cscope@newsweek.com](mailto:cscope@newsweek.com)

VITAL STATS

## Net Ventures

The recent feeding frenzy over Netscape stock revealed what venture capitalists already knew: the Internet is hot property. This year's investments should triple 1994 levels.

Venture capital investment in Internet companies in millions of dollars



SOURCE: VENTUREONE CORP.

To: Elena

## Encryption-Software Plan Presented Using 'Keys' Held by Escrow Agents

By DANIEL PEARL

Staff Reporter of THE WALL STREET JOURNAL

WASHINGTON — Clinton administration officials said they would allow companies to sell stronger data-security software overseas, as long as the "keys" to break the codes are left with electronic escrow agents.

The pledge is an attempt to solve a two-year dispute between law-enforcement officials, who want to make sure criminals can't hide their data transmissions, and computer companies, which say their encryption programs are becoming hard to sell overseas because hackers can crack the codes.

### The Search for a Policy

The administration has withheld export approval for strong encryption schemes while struggling to come up with a policy acceptable to both sides. The White House's 1993 proposal for a "Clipper Chip" that would put the code-cracking key in the government's hands produced an uproar from the computer industry. Under the new scheme, which has more industry support, the government would have to get a search warrant to obtain the key from a company that is holding it on behalf of the person sending or receiving encrypted messages.

But in a presentation to computer-industry officials here, Clinton administration officials said they would still keep some limits on how strong encryption codes can be, even when the "key escrow" method is used. Also, companies hoping to start selling stronger encryption products will have to wait a few months, since the administration has yet to sort out important details. For instance, one unresolved issue is how to certify escrow agents to keep fly-by-night operators and organized-crime figures out of the business. And the administration's emerging policy doesn't deal with data-security hardware — products that wire the encryption schemes right into chips or other devices.

Because of those unresolved elements, industry reaction was mixed yesterday.

### Building Longer Keys

Robert Holleyman, president of the Washington-based Business Software Alliance, which includes Microsoft Corp., Novell Inc., Lotus Development Corp. and other major software companies, said the government's flexibility was "encouraging." But he said the continued limits on

the length of encryption keys were "unnecessary."

Keys are streams of bits, generated at random, that are used to scramble and unscramble data. U.S. officials generally limit exported security programs to 40-bit keys, though longer keys are available inside the U.S., or overseas from foreign suppliers. Recently, a computer hacker in France, using 120 computer workstations over eight days, was able to break a 40-bit code used in a foreign version of Internet navigation software sold by Netscape Communications Corp.

Yesterday, the administration said it would allow the exporting of software with 64-bit encryption schemes, as long as the software includes a requirement for keeping the keys in escrow. A 64-bit program would, theoretically, be 65,000 times harder to crack than a 40-bit program, but in reality wouldn't be that difficult, said Vinton Cerf, an Internet pioneer and senior vice president of MCI Communications Corp. He said as computing power increases, a 64-bit code could become vulnerable to hackers, too.

Clint Brooks, a technical adviser with the National Security Agency, the primary federal wiretapping agency, told computer executives that continued limits were needed because officials were "uneasy" about the possibility that software could be altered so that the key would no longer be accessible to law-enforcement officials.

Just as copy-protected software was overrun in the mid-1980s by special software that allowed people to copy disks freely, key-escrowing requirements could eventually be overridden by software posted on the Internet, agreed Bill Sweet, marketing director of National Semiconductor Corp. That company, along with Hewlett-Packard Co. and others, is trying to get export approval for an encryption scheme that's wired into hardware. In the case of Hewlett-Packard, the U.S. encryption requirements would be embodied in a stamp-sized "flag" — a chip that slips into a security card, which in turn fits into a laptop computer.

But "we're still where we were a year and a half ago" in talks with the State Department, said Frederick F. Mailman, a Hewlett-Packard regulatory manager in Washington. And government officials didn't indicate yesterday whether such hardware schemes would get speedier ap-

Please Turn to Page A7, Column 3

Continued From Page A3

proval under the administration's emerging plans.

Even with the export restrictions, U.S. officials haven't been able to stop widespread international distribution of an encryption program, called Pretty Good Privacy, that is nearly impossible to crack. The program's author, Philip Zimmermann, has been under federal investigation for more than a year but hasn't been charged with any crime. Mr. Zimmermann couldn't be reached yesterday.

The administration may have trouble persuading some programmers to leave their code-breaking keys with escrow agents instead of on users' computers. Vice President Al Gore indicated early last year the administration was receptive to the key-escrowing idea, and the government is moving toward using such encryption devices in its own computer purchases.

Some computer officials have been frustrated with the administration's pace in drafting export guidelines. Two groups of companies wrote to Mr. Gore last week urging fast action, and two groups — the Software Publishers Association and the American Electronics Association — sponsored a "policy workshop" here yesterday to apply more pressure. Administration officials yesterday said they would need more industry consultation, including two meetings next month, before producing final guidelines.

"This coffee klatsch thing was something of a surprise," said Renee Dankworth, a former National Security Agency official who works as an export consultant for RSA Data Security Inc. of Redwood City, Calif. "I was expecting sort of like Moses and the Ten Commandments."

— Steve Stecklow in Boston contributed to this article.

## LAW

# Seizure of Electronic Messages In Obscenity Case Raises Questions

By CONSTANCE JOHNSON

Staff Reporter of THE WALL STREET JOURNAL

Users of a small computer bulletin board in Ohio sued local authorities who seized their electronic mail and other materials as part of an investigation into obscene postings.

In their lawsuit, which appears to be the first of its kind, the plaintiffs contend that the Hamilton County Regional Computer Crimes Task Force and other authorities violated their rights to free speech and privacy by seizing their messages during a June raid of five bulletin boards.

The plaintiffs also allege that, by seizing their private electronic messages, the authorities violated the Electronic Communications Privacy Act.

The suit, filed in federal court in Cincinnati, comes as law enforcement authorities are investigating more allegations of crimes in cyberspace. "This is going to be increasingly more common as users are discovering that their rights are being implicated by these overbroad searches and seizures," predicted Mike Goodwin, staff counsel for the California-based Electronic Frontier Foundation.

In their lawsuit, the seven plaintiffs, who are seeking class-action status to represent as many as 7,000 subscribers to the Cincinnati Computer Connection, contend that the task force should have seized only the 45 allegedly obscene images it was seeking.

"We don't know whether they had a legitimate reason to investigate, but the method their investigation took violated the rights of folks who use the system," said Peter Kennedy, of Austin, Texas, who is one of two attorneys representing the bulletin board users. They are seeking the return of their electronic files and unspecified damages, which their other lawyer said could be as much as \$50 million.

Jim Harper, chief counsel for the Hamilton County prosecutor's office, defended the search, saying the authorities had to seize the bulletin board's hard drive containing all of the users' electronic files because they needed the "original evidence." He added that evidence of other crimes could also have been found on the hard drive.

Dale Menkaus, the task force's commander, also defended the seizure but acknowledged that searches in cyberspace raise new legal questions. "There isn't

clear protocol for how this evidence can be seized," he said.

Users of the Cincinnati Computer Connection say they were devastated by the seizure. "I lost many, many connections around the world that I communicated with through e-mail about my disabilities," plaintiff Randy Bowling, who is speech-impaired, said in an electronic message. "I had many personal letters that remained on the bulletin board that I now do not have and do not know who all is reading them."

Another plaintiff in the suit, computer consultant Steven Guest, said his business suffered because he uses the bulletin board to communicate with clients and associates. "I can't understand why you would go in and take an entire computer system when what you are looking for is one or two files," Mr. Guest said. "I don't want my rights violated by the people who are supposed to be protecting them."

Also named as defendants in the suit are the Hamilton County Sheriff's Department, Sheriff Simon L. Leis Jr. and Mr. Menkaus, among others.

After the raid, Hamilton County authorities charged Bob Emerson, who owns the Cincinnati Computer Connection, with disseminating obscene material and infringing on a software copyright. Mr. Emerson, who has since restarted the operation, has filed a separate civil suit against the task force and others, alleging reckless disregard of his rights to privacy, free speech and freedom from unreasonable searches and seizures.

"This is just a form of harassment," said H. Louis Sirkin, Mr. Emerson's attorney. "That's why they did it."

## Florida Supreme Court

The Florida Supreme Court agreed to a fast track schedule to decide the legality of a novel state law that empowers the state to sue to recoup from tobacco companies the cost of treating smoking-related illnesses.

The decision bypasses an intermediate appeals court, where the case had been pending, and means a final decision could be out by year end. Written briefs are due Sept. 5 and oral arguments are slated for Nov. 6, according to the court's schedule.

Three other states are seeking to recoup public costs of treating smoking-related illnesses by suing cigarette manufacturers, but Florida is the only state to pass a law empowering it to file such a suit. The law prohibits cigarette manufacturers from arguing that Medicaid patients knew the risks of smoking, thereby stripping the industry of its most potent defense. It also allows the state to use general statistics linking smoking to the cost of treating heart, lung and other respiratory diseases, rather than assessing costs on a case-by-case basis.

A state circuit court judge in Tallahassee upheld the law's constitutionality last June, but limited the tobacco industry's liability by ruling that Florida can recover damages incurred only since the date the law was enacted in 1994. He also found that the Florida agency charged with administering and enforcing the new law is unconstitutionally structured. Both sides are appealing.

—Milo Geyelin contributed to this article.



## Enabling legislation

- Establishes responsibility + obligations for p. who want to serve as escrow agents.

- KE gives copy way to do data recovery.

NOT everyone will start using them

But some will see there is a value to them.

# Industry Split Emerges Over Computer Data Secrecy Issue

By JOHN MARKOFF

Some of the biggest names in the computer hardware and software industries sent separate letters to the White House last week in pre-emptive moves aimed at a proposed regulation originally designed to insure that law-enforcement officials have access to all computer communications. The proposal may be released as soon as this week.

But as the Government's task force on the encryption issue prepared to disclose the closely held details of the proposal — the latest version of a measure unveiled more than two years ago but subsequently reconsidered in the face of industry opposition — the last-minute, scattershot lobbying revealed unexpected divisions.

These are emerging at a crucial moment. With the Government's interagency task force apparently split between those who favor maximum governmental access to communications and those who favor looser restrictions. Most industry executives had hoped to present a united front in favor of the more liberal position — a goal that now appears to be in jeopardy.

The two major groups sending letters to Vice President Al Gore, the Administration's point man on technology issues, were a group of computer hardware manufacturers and a group of the largest makers of software.

In a letter sent to the Vice President on Aug. 10, eight executives, including James Treybig, chairman of Tandem Computers Inc.; Gil F. Amelio, chairman of National Semiconductor Inc.; Edward McCracken, chairman of Silicon Graphics Inc.; Eugene Shanks Jr., president of Bankers Trust, which conducts electronic commerce internationally, and Stephen T. Walker, chairman of Trusted Information Systems, urged that the Government immediately establish a new standard to control the export of technology that is used to

Continued From First Business Page

encode communications, so that outsiders cannot tap in.

A day later, however, a group of software publishers, including William H. Gates, chairman of the Microsoft Corporation; Jim P. Manzi, president of the Lotus Development Corporation and a senior vice president of I.B.M.; Robert Frankenberg, chairman of Novell Inc.; Mark B. Hoffman, chairman of Sybase Inc., and Carol Bartz, chairwoman of Autodesk Inc., wrote arguing that the solution offered by the computer manufacturers would fail to remove current obstacles that keep American companies from competing in lucrative international markets.

Many off-the-shelf programs cannot be marketed abroad without alteration under current regulations. For example, before American publishers can sell the popular Lotus Notes program abroad, they must replace its encoding system with a weakened version that meets the current stringent United States export requirements. These restrictions date to the 1970's, when advanced computer technology was treated as the equivalent of military technology and subject to the same strict controls.

The software publishers have been able to sell their highly effective communications encoding products in this country, while sales abroad, they contend, have been hurt. Their letter also said that, although the Administration agreed last year to work with industry toward a compromise, "there has been only minimal consultation with the software industry with respect to basic questions. . . ."

"We're worried the Government is about to announce the son of Clipper," said Robert W. Holleyman 2d, president of the Business Software Alliance, referring to the Government's original proposal for changing the standard. This proposal, released in April 1993, would have replaced the Cold War-era restrictions with a coding standard that allowed sales of strong encryption programs, but would have given United States law enforcement agencies access to all communications through a back door with a numerical key.

"The Administration has been try-

ing to resolve how to keep U.S. companies competitive, but there remain individuals in the Government who want to do anything they can to slow the proliferation of new encryption technologies," Mr. Holleyman said.

In April 1993, the Administration proposed a hardware-based system for protecting the privacy of telephone calls and computer data transmissions. The standard, known as the "Clipper Chip," included a special "backdoor" that would permit law enforcement officials to listen to conversations and monitor data exchanges.

The original Clipper system called for a two-part key for decoding scrambled conversations. The two parts of the key — actually two large numbers — were to be held by two independent Government agencies. Under the plan, when a law enforcement agency had a warrant to listen to a conversation encoded by Clipper, it would obtain the keys from the separate agencies. By merging the keys, it could obtain a key that would unlock the coded conversation.

The Clipper proposal met with angry opposition both from advocates for civil liberties, who argued it would undermine the right to privacy, and by high-technology executives who said Clipper would be unacceptable for foreign users who would not want their conversations to be readable by the United States Government.

The announcement of the new proposal may be imminent. Next Friday, two trade associations, the Software Publishers Association and the American Electronic Association, are planning a conference on cryptography policy.

Several people familiar with Administration policy discussions said the Government had until recently remained divided and that the director of the Federal Bureau of Investigation, Louis J. Freeh, has been the most vocal advocate of placing strict limits on any use of unsanctioned encryption technology.

After the bombing of the Federal building in Oklahoma City, the F.B.I. circulated a proposed antiterrorism bill on Capitol Hill that would have banned even the domestic use of coding software except for systems approved by the Government.

brunt of several trends toward greater economic inequality, a new study shows.

Only in Israel and Ireland are poor children worse off than poor American youths, according to the study, an analysis of 18 nations by the Luxembourg Income Study, a nonprofit group based in Walferdange, Luxembourg.

The results are the most comprehensive of several recent analyses, and are particularly striking because the United States has the second highest level of economic output per person of the countries examined, after Luxembourg itself, and has the most prosperous affluent children of any of the 18 nations.

It may not be surprising that childhood poverty is worse in the United States than in Scandinavia, where governments have racked up huge national debts while trying to maintain elaborate social safety nets. But the United States also ranks below countries like Italy, which has a considerably smaller economy per person and has less generous social policies than many northern European nations.

The United States appears to have sunk through the rankings over the last 30 years, although no conclusive data are available now, said Timothy M. Smeeding, one of the study's

## *Data add to the debate over the future of Federal welfare programs.*

authors and director of the Luxembourg Income Study. The American lead in overall prosperity has dwindled since the 1960's, income inequality has risen briskly in the United States and child poverty spread here in the 1970's and 1980's, although it may have leveled off in the early part of this decade.

Child poverty has also risen in Britain and Israel, while showing relatively little change in Continental Europe, according to the latest study.

Some conservative economists have questioned the validity of studies that attempt to compare levels of income and distribution of wealth among nations with somewhat different economic systems and societies. There is general acceptance within the field, however, of the idea that the United States has proportionately more of its children in poverty than other affluent countries. The debate revolves instead around what to do about it.

The results of the Luxembourg Income Study report, which is based on census survey data from the various countries, are consistent with less statistically detailed work by other social scientists.

ate last week, ended up postponing action until after Labor Day following strong resistance from Democrats and from conservatives within his party.

During a press conference on Thursday, President Clinton expressed strong concern about stagnant incomes, particularly for less-affluent Americans. "We've got to grow the economy and raise incomes," he said. "That's why I want to raise the minimum wage, that's why I want to give every unemployed worker or underemployed worker the right to two years of education at the local community college, that's why I'm trying to have a tax cut that's focused on child rearing and education: to raise incomes."

Mr. Smeeding said there appeared to be several reasons why the United States had such extreme poverty among children.

The United States has the widest gap between rich and poor, he said. The United States also has less generous social programs than the other 17 countries in the study, which are Australia, Canada, Israel, and 14 European countries: Austria, Belgium, Britain, Denmark, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Norway, Sweden and Switzerland. The study did not include several Western European nations like Greece, Spain and Portugal that have very poor children but limited data.

American households with children tend to be less affluent than the average American household, a pattern that is not true in many other countries.

This trend may reflect that American mothers are less likely than European mothers to return to work quickly after childbirth, partly because inexpensive, high-quality child care is more widely available in Europe, said Lee Rainwater, the research director of the Luxembourg Income Study and the co-author with Mr. Smeeding of the latest report. The Luxembourg group sent copies of the report to prominent social researchers last week and will make it more broadly available in the coming days.

Some conservative analysts question whether international comparisons of prosperity should even be attempted. They point to the many differences among nations' economies and societies.

There are more poor children in the United States than in many affluent countries, but that partly reflects the high number of poor immigrants and unwed teen-age mothers here, said Douglas J. Besharov, a resident scholar at the American Economic Institute, a conservative research group here.

"Is there more poverty in a big, diverse country like ours than in Western Europe?" he asked. "The answer is yes."

He and other conservative economists argue that the price the other countries pay for avoiding extremes of childhood poverty may be slower economic growth, which, they assert, leads to lower living standards for

make reliable international comparisons. The group is a repository for computerized data on income distribution from 25 countries around the world, which it makes available for free to social researchers.

In addition to his work with the study, Mr. Smeeding is an economics professor at Syracuse University and one of the nation's leading experts on income calculations. While he personally favors expanded social spending in the United States, he is generally regarded in the field as an undogmatic thinker. Mr. Rainwater is a professor emeritus of sociology at Harvard University and the author of many books on poverty.

Their study is critical of Republican efforts to cut American social spending now.

The study compares incomes of poor and affluent households with children. The figures include not only after-tax wages and other personal income but also cash benefits from the government, like food stamps and the tax credit on earned income for low-income working parents with children. The calculations take into account differences among countries in the size of families and in the cost of living.

The figures do not include free government services, like the free medical and child-care services available in many European countries.

Sheila B. Kamerman, a professor of social policy and planning at Columbia University, said that for this reason, the latest analysis may have underestimated the extent to which poor American children lag in income. "If you were looking at in-kind benefits as well as cash benefits, the situation in the U.S. would look even worse," she said.

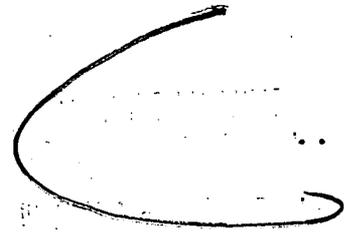
Professor Kamerman and Alfred J. Kahn, another Columbia University social policy professor, published a lengthy study two weeks ago reviewing social programs in Britain, Denmark, Finland, France, Germany, Italy and the United States and found that American poor children received the least help.

Poor children in Denmark do particularly well in comparison to poor American children. Vita Pruzan, the director of the children, youth and family research division at the National Institute of Social Research in Copenhagen, said in a telephone interview that in reducing child poverty, the Danish Government had found it particularly effective to provide free obstetric and nursing services.

Denmark also makes a particular effort to help single mothers who do not receive child support payments from the fathers of their children. "If the father is absent and doesn't pay, the state will pay what he is supposed to pay," Dr. Pruzan said. "The state tries to collect the money from the father, but that is not her problem."

Poor children in Italy are also better off than poor American children, even though the median income in Italy is considerably less than in the United States. Free child care for some poor children and a

LOW  
CLASSIFICATION



**JUSTICE**  
MSG NBR 576

TIME TRANSMITTED (LOCAL)

TIME RECEIVED (LOCAL)

FROM DAC/Vatis OFFICE/DESK 4127 PHONE NBR 307-3667  
SUBJECT Encryption

DELIVERY INSTRUCTIONS:

PAGES 18  
(INCLUDING COVER)

- HOLD FOR NORMAL DUTY HOURS/ROUTINE
- IMMEDIATELY/URGENT

NOTE: FURNISH AFTER DUTY HOUR CONTACT TELEPHONE NUMBER FOR EACH ADDEE REQUIRING AFTER DUTY HOUR DELIVERY

TRANSMIT TO

AGENCY	INDIVIDUAL (NAME)	OFFICE	ROOM NBR	PHONE NBR
C-	WH Leon Panetta	Chief of Staff	W Wing	456-6797
C-	WH Samuel Berger	NSC	W Wing	456-9481
C-	WH Abner Mikva	Counsel to President	W Wing	456-2632
C-	<del>VP</del> VP Leon Fuerth	Asst. to VP Int. Sec. Aff.	298 DEOB	395-4213
A-	CIA John Deutch	Director		(703) 487-6863
L-	Commerce David Barron	Dept. Sec.	5838	482-4625
Q2	FBI Louis Freeh	Director		324-3444
A-	CIA Adm. William Studeman	Dept. Director		(703) 482-6464
F-	NSA Adm. John McConnell	Director		(301) 688-7111

REMARKS:

LOW



## Office of the Deputy Attorney General

Washington, D.C. 20530

August 4, 1995

LIMITED OFFICIAL USE

## MEMORANDUM

TO: Leon Panetta, White House Chief of Staff  
John Deutch, Director of Central Intelligence  
Abner Mikva, Counsel to the President  
Sandy Berger, Deputy National Security Advisor  
Leon Fuerth, Assistant to Vice President for National  
Security Affairs  
David Barram, Deputy Secretary of Commerce  
Louis Freeh, Director, Federal Bureau of Investigation  
Admiral William Studeman, Deputy Director of Central  
Intelligence  
Vice Admiral John McConnell, Director, National  
Security Agency

FROM: Jamie S. Gorelick   
Deputy Attorney General

SUBJECT: Encryption Legislation

Attached for your consideration is a revised version of "soft" legislation, which would provide an antitrust exemption for manufactures who voluntarily decide to make key escrow encryption products, and would establish a regime for escrowing the keys.

Attachment

104th CONGRESS

1st Session

**H.R.** \_\_\_\_\_

\_\_\_\_\_  
IN THE HOUSE OF REPRESENTATIVES

Mr. \_\_\_\_\_ of \_\_\_\_\_ introduced the following bill; which was referred to the Committee on \_\_\_\_\_

\_\_\_\_\_  
**A BILL**

To ensure the public safety and national security by providing for a system of key escrow encryption, and to provide relief from antitrust liability for persons who voluntarily agree to develop, adopt, use or distribute only encryption products that permit appropriate government access, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

**TITLE I -- GENERAL PROVISIONS**

**SEC. 101. SHORT TITLE.**

This Act may be cited as the "Data Security Act of 1995".

**SEC. 102. FINDINGS AND PURPOSES.**

(a) **FINDINGS.** - The Congress finds the following:

(1) Advancements in communications and information technology and the widespread use of that technology have stimulated the volume and enhanced the value

of domestic and international wire and electronic communications and electronically-stored information.

(2) The development of the Nation's information infrastructure and the realization of the full benefits of that infrastructure require that wire and electronic communications and electronic information communicated over, and resident in, that infrastructure be secure, confidential, and authentic.

(3) Security, privacy, and authentication of wire and electronic communications and electronic information communicated over, or resident in, the Nation's information infrastructure are enhanced with the use of encryption technology.

(4) Although encryption technology is a valuable tool to protect the security and privacy of wire and electronic communications and electronic information, such technology can be misused by terrorists, other dangerous and violent criminals, organized crime syndicates, drug-trafficking organizations, and spies to avoid detection and to hide evidence of their criminal activity, thereby jeopardizing effective law enforcement, public safety, and the national security.

(5) The ability of individuals and business entities to secure and protect the transmission and storage of their wire and electronic communications and electronic information should be preserved.

(6) The authority and ability of government agencies, in a timely manner, to decipher and obtain the plaintext of wire and electronic communications and electronic

information necessary to provide for effective law enforcement, the public safety, and national security should also be preserved.

(7) There is a national need to encourage the development, adoption, and use of encryption products that are consistent with the foregoing considerations and are appropriate for use in both domestic and export markets and by the United States Government. The voluntary development, adoption, and use in the domestic market only of encryption products that are consistent with such considerations may be impeded by antitrust concerns.

(b) PURPOSES. - It is the purpose of this Act --

(1) to promote the development of the Nation's information infrastructure consistent with public welfare and safety, efficient law enforcement, national security, and the privacy and protection of communications and information;

(2) to encourage and facilitate the development, adoption, and use of encryption products that provide security, protection, and authentication of wire and electronic communications and electronic information and that reasonably satisfy the needs of government agencies to provide for effective law enforcement, the public safety, and national security;

(3) to carry out that policy through the development of a program to facilitate the use of key escrow encryption products; and

(4) to ensure that the voluntary development, adoption, and use of appropriate encryption products is not impeded by the risk of antitrust liability.

**SEC. 103. DEFINITIONS.** -- For purposes of this Act:

(1) The term "antitrust laws" means the antitrust laws, as such term is defined in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), and section 5 of the Federal Trade Commission Act (15 U.S.C. 45) (to the extent that such section 5 prohibits unfair methods of competition), and any State antitrust or unfair competition law.

(2) The term "electronic communication service" has the meaning given such term in section 2510 (15) of title 18, United States Code.

(3) The term "electronic communications system" has the meaning given such term in section 2510(14) of title 18, United States Code.

(4) The term "encryption product" means any product (including, but not limited to, hardware, firmware, or software, or some combination thereof), that is designed, adapted, or configured to use a cryptographic algorithm to protect the confidentiality of data.

(5) The term "key escrow encryption" means an encryption method that includes the storing of keys or components thereof with a key escrow agent who is not the owner, possessor, sender or recipient of information encrypted with the key or components thereof.

(6) The term "key escrow agent" means any person, including any entity approved by the Secretary in accordance with subsection 301(a)(1) of this Act, who holds and manages keys or components, for or on behalf of any other person or

entity.

⑦ The term "key escrow encryption product" means an encryption product that uses or includes key escrow encryption.

(8) The term "key" means a sequence of symbols that enables the transformation from plaintext to ciphertext and vice versa.

(9) The term "electronic information" means any information, including but not limited to texts, messages, recordings, images or documents, in any electronic, electromagnetic, photoelectronic, photooptical, or digitally encoded computer-readable form.

(10) The term "electronic communication" has the meaning given such term in section 2510(12) of title 18, United States Code.

(11) The term "wire communication" has the meaning given such term in section 2510(1) of title 18, United States Code.

⑫ The term "government" means the Government of the United States and any agency or instrumentality thereof, a State or political subdivision of a State, the District of Columbia, or a commonwealth, territory, or possession of the United States.

(13) The term "person" means any individual, corporation, company, association, firm, partnership, society, or joint stock company.

⑭ The term "Secretary" means the Secretary of Commerce or his or her designee.

(15) The term "Attorney General" means the Attorney General of the United States or his or her designee.

## TITLE II -- AMENDMENTS TO TITLE 15 OF THE UNITED STATES CODE

### SEC. 201. EXEMPTION.

No person shall be liable under the antitrust laws for damages, penalties, injunctive relief, or other sanctions, for negotiating, entering into, participating in or implementing an agreement to --

(1) engage in joint development of encryption products to the extent necessary to ensure the ability of government agencies to decipher, in a timely manner, wire and electronic communications and electronic information that have been intercepted pursuant to electronic surveillance laws or obtained under other lawful authorization; or

*what would this mean? why necessary?*

(2) make available only those encryption products that ensure the ability of government agencies to decipher, in a timely manner, wire and electronic communications and electronic information that have been intercepted pursuant to electronic surveillance laws or obtained under other lawful authorization.

### SEC. 202. LIMITATIONS.

The exemption provided in section 201 of this Act shall not apply to any agreement concerning price or other terms or conditions of sale of any such product produced or sold by any such person, or that results in a boycott of any person.

TITLE III -- AMENDMENTS TO THE DEPARTMENT  
OF LABOR AND COMMERCE ACT

SEC. 301. KEY ESCROW PROVISIONS

(a) ESCROW AGENTS --

(1) APPROVAL -- The Secretary may approve government agencies or suitable private sector entities that satisfy qualifications established by the Secretary, which shall include but not be limited to the qualifications enumerated in paragraph (2), to act as key escrow agents for encryption products. The Secretary shall also have the power, in consultation with the Attorney General, to revoke the authority of any such government agency or private sector entity to serve as such key escrow agent which has violated any provision of this Act or any rule, regulation or requirement prescribed by the Secretary under this Act.

(2) QUALIFICATIONS -- In order to be approved as a key escrow agent, an entity shall --

(A) possess the capability, competency, and resources to administer key escrow encryption, to safeguard sensitive information related to it, and to carry out the responsibilities set forth in paragraph (3) in a timely manner; but

(B) not be a law enforcement or intelligence agency, nor a foreign country or entity thereof, a national of a foreign country, a corporation organized under the laws of any foreign country, or a corporation of which an

alien is an officer or more than one-fourth of the stock of which is owned by aliens or which is directly or indirectly controlled by any such corporation.

(3) RESPONSIBILITIES -- A key escrow agent approved under paragraph (a) shall, consistent with regulations issued by the Secretary, establish procedures and take other appropriate steps--

(A) to ensure the confidentiality, integrity, and timely release of keys or components thereof held by the agent pursuant to this subsection;

(B) to protect the confidentiality of the identity of the person or persons for whom such key escrow agent holds keys or components thereof;

(C) to protect the confidentiality of the identity of the government agency requesting encryption keys or components thereof and all information concerning such agency's access to and use of encryption keys or components thereof; *on what showing?  
in what circumstances?*

(D) to hold and manage the keys or components thereof consistent with the requirements of this section; and

(E) to carry out the responsibilities set forth in this subsection in the most effective and efficient manner practicable.

(4) AUTHORITY -- A Federal agency approved as a key escrow agent under this section may enter into contracts, cooperative agreements, and joint ventures and take other appropriate steps to carry out its responsibilities.

(b) LIMITATIONS ON ACCESS AND USE --

*how do you ensure that  
people file w/ key escrow  
agents?*

(1) Release of Key Information to Certain Entities --

A key escrow agent, whether or not approved under subsection (a), shall, upon request, release a key or component thereof held by the agent to --

(A) A government agency that provides a certification that it is authorized by law to conduct electronic surveillance, a search, or other examination of communications or information and that it requires access to the key or component thereof in order to determine the plaintext of a wire or electronic communication or of electronic information that it has acquired or intercepted, or that it will acquire or intercept, in such surveillance, search or examination.

A key escrow agent shall release keys or components thereof to a requesting federal government agency only upon its receipt from such agency or from the Department of Justice of such a certification executed by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division of the Department of Justice, by a United States Attorney, Assistant United States Attorney, or other attorney for the government supervising the investigation in which such electronic surveillance, search or other examination of communications or information is being conducted, or by a judge or other authorized official of a Federal court of competent jurisdiction. A key escrow agent shall release keys or components thereof to a requesting agency of a state government or a political subdivision thereof only upon its receipt from such

agency or subdivision, or from the Department of Justice of a certification, but only if such certification is executed by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division of the Department of Justice, by the principal prosecuting attorney of such State or political subdivision, by a judge or other authorized official of a Federal court of competent jurisdiction, or by a judge or other authorized official of a State court of competent jurisdiction; or

(B) a Federal agency, or to the Department of Justice for conveyance to a Federal agency, if that agency or the Department of Justice provides a certification that the agency receiving the key or component thereof is authorized by law to collect foreign intelligence or foreign counterintelligence, and that such agency requires access to the key or component thereof in order to determine the plaintext of any wire or electronic communication or of any electronic information that it has acquired or intercepted, or that it will acquire or intercept, in the lawful collection of foreign intelligence or foreign counterintelligence. Key escrow agents shall release keys or components thereof to the requesting government agency upon their receipt of a certification, but only if such certification is executed by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division, or

the Counsel for Intelligence Policy, of the Department of Justice.

(2) A government agency to which a key or component thereof has been released under this paragraph may use the key or component thereof only to determine the plaintext of any wire or electronic communication or of any electronic information that the agency acquires or intercepts pursuant to its lawfully authorized surveillance, search or examination. Once such lawful use is completed, the government agency shall destroy the key or component thereof in its possession.

(3) Nothing in this subsection shall be construed to prohibit a key escrow agent from releasing keys or key components for encryption products to the owners of such products pursuant to contractual or other commercial arrangements therefor, nor to prohibit any key escrow agent from releasing keys or key components for encryption products to any person in conformance with a determination by a court of competent jurisdiction that such person is lawfully entitled to hold such keys or key components.

(c) KEY ESCROW FUNDING-- Within one hundred and eighty days after the date of enactment of this Act, the Secretary shall make recommendations to the congressional committees having oversight of the Department of Commerce regarding the estimated funding requirements for any key escrow agents approved by the Secretary, as may be deemed appropriate by the Secretary.

(d) **FEDERAL GOVERNMENT LIABILITY** -- The United States shall not be liable for any loss incurred by any individual or entity resulting from any violation of this Act or the failure to exercise reasonable care in the performance of any duties under any regulation or procedure established by or under this Act, nor resulting from any action by any person who is not an official or employee of the United States.

**SEC. 302. REGULATIONS** -- Within one hundred and eighty days after the date of the enactment of this Act, the Secretary shall, after notice to the public and opportunity for comment, issue any regulations necessary to carry out this Act.

**SEC. 303. UNLAWFUL ACTS.**

(a) It shall be unlawful for any person --

(1) intentionally to make available a key or component thereof required for decryption of wire or electronic communications or of electronic information encrypted with a key escrow encryption product to a government agency or employee thereof or other person, knowing that such agency, employee, or other person is not legally authorized to receive it;

(2) intentionally to obtain or use an encryption key or component thereof required for decryption of communications or information, pursuant to section 301(a)(2)(A), without lawful authority or, having received such key or component thereof with lawful authority, intentionally to exceed such authority for the purpose of decrypting information; or

(3) if a key escrow agent, or officer, employee, or agent thereof, intentionally to disclose to any person, except as authorized by this Act or regulations promulgated thereunder, the facts or circumstances of any release of keys or key components or requests therefor. This provision shall not, however, prohibit such key escrow agent, officer, employee, or agent thereof from providing evidence in any proceeding held under the authority of the United States or of any State or political subdivision thereof, or from disclosing such information as is necessary to permit audits of inspections of the operations of such key escrow agent in accordance with regulations promulgated by the Secretary.

(b) Any person who violates this section shall, upon conviction, be punished as provided in section 304.

#### **SEC. 304. PENALTIES --**

(a) **CRIMINAL PENALTIES --** Any person who violates section 303 of this Act shall be fined under title 18, United States Code, or imprisoned not more than five years, or both.

(b) **CIVIL PENALTY --**

(1) Any person who acts a key escrow agent without the approval of the Secretary under section 301(a)(1)(A) of this Act shall be subject to a civil penalty in an amount assessed by a court in a civil action.

(2) The amount of the civil penalty shall not exceed \$100,000, unless the

violation was willful, in which case the civil penalty may not exceed \$100,000 per day. In determining the amount of the penalty, the court shall consider the risk harm to law enforcement and national security interests, the risk of of harm to key owners, the gross receipts of the charged party, the judgment of the Attorney General concerning the appropriate penalty, and the willfulness of the violation.

(3) A civil action to recover such a civil penalty may be commenced by the Attorney General. The Attorney General must establish the right to recovery by a preponderance of the evidence.

(4) The Attorney General may, in a civil action in the appropriate United States district court, obtain an order against a key escrow encryption product manufacturer, vendor, or owner, or any other person, not a key escrow agent approved by the Secretary, who is in possession of keys or components thereof, or any other necessary person, to require that keys or components thereof are properly deposited with a key escrow agent certified by the Secretary.

(5) A civil action under this section may not be commenced later than 5 years after the cause of action accrues.

(6) The district courts of the United States shall have original jurisdiction of any action brought by the Attorney General under this subsection. An action for a civil penalty may be joined with an action for an injunction under section 305 of this Act.

(7) For the purpose of conducting a civil investigation in contemplation of a civil proceeding under this section, the Attorney General may (A) administer oaths and affirmations; (B) take evidence; and (C) by subpoena, summon witnesses and require the production of any books, papers, correspondence, memoranda, or other records which the Attorney General deems relevant or material to the inquiry. Such subpoena may require the attendance of witnesses and the production of any such records from any place in the United States at any place in the United States designated by the Attorney General. The same procedures and limitations as are provided with respect to civil investigative demands in subsections (g), (h), and (j) of section 1968 of Title 18 apply with respect to a subpoena issued under this subsection. Process required by such subsections to be served upon the custodian shall be served on the Attorney General. Failure to comply with an order of the court to enforce such subpoena shall be punishable as contempt.

**SEC. 305. INJUNCTION** -- The Attorney General may bring an action to enjoin any person (including an officer or employee of a government agency) from committing any violation of this Act. The district courts of the United States shall have jurisdiction of any action brought by the Attorney General under this paragraph.

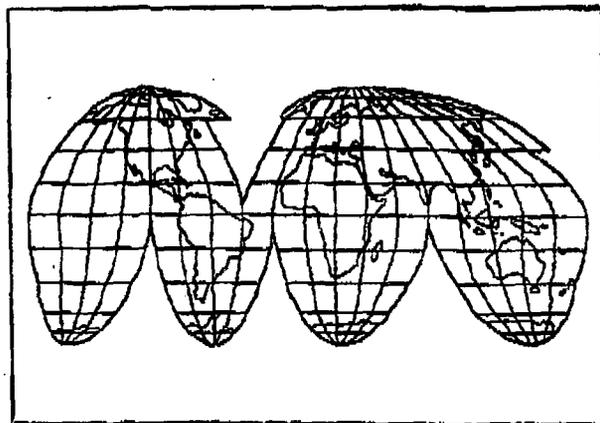
**SEC. 306. SEVERABILITY AND INTERPRETATION** -- If any provision of this Act, or the application thereof, to any person or circumstance, is held invalid, the

remainder of this Act, and the application thereof, to other persons or circumstances shall not be affected thereby. Nothing contained in this Act shall be deemed to preempt or otherwise affect the application of the Arms Export Control Act (22 U.S.C. § 2751 et seq.) or any regulations promulgated thereunder.

**SEC. 307. AUTHORIZATION OF APPROPRIATIONS.--** There are authorized to be appropriated to the Secretary of Commerce for the purpose of carrying out this Act a total of \$\_\_\_\_\_ for fiscal years 1996, 1997, 1998, and 1999. Such sums are authorized to remain available until expended.

**SEC. 308. EFFECTIVE DATE.--** This Act shall take effect on the date of its enactment.

**U.S. DEPARTMENT OF JUSTICE  
WASHINGTON, D.C.**



**DATE:** 5/5/95

**TO:**

**LEON PANETTA - 465-1121  
ERSKINE BOWELS - 456-6703  
SANDY BERGER - 456-9490  
JOHN DEUTCH - (703) 697-7374  
RON NOBLE - 622-5040  
LOUIE FREEH - 324-6856  
TOM CONSTANTINE - 307-7335  
ADMIRAL STUDEMAN - (703) 482-3064  
ADMIRAL McCONNELL - (301) 497-2888**

**FROM: JAMIE GORELICK  
DEPUTY ATTORNEY GENERAL**

**BY: MICHAEL A. VATIS  
COUNSEL TO THE  
DEPUTY ATTORNEY GENERAL  
DEPUTY DIRECTOR, EXECUTIVE OFFICE  
FOR NATIONAL SECURITY**

**SUBJECT: ENCRYPTION**

**MESSAGE: ATTACHED ARE RELIMINARY DRAFTS OF ENCRYPTION LEGISLATION: ONE VERSION  
SETS UP A MANDATORY LICENSING REGIME: THE OTHER ESTABLISHES AN ANTITRUST ENCRYPTION  
FOR MANUFACTURERS OF ENCRYPTION PRODUCTS. *exem***

**(TOTAL NUMBER OF PAGES INCLUDING THIS ONE) 35**

**TRANSMITTED BY: Denise Gaston**

**FOR VOICE COMMUNICATIONS WITH THIS OFFICE, PLEASE TELEPHONE (202-307-3667)  
TO TRANSMIT TO THIS OFFICE VIA TELEFAX, PLEASE TELEPHONE (202-616-1080)**

# DRAFT

104th CONGRESS

1st Session

**H.R.** \_\_\_\_\_

---

IN THE HOUSE OF REPRESENTATIVES

M . \_\_\_\_\_ of \_\_\_\_\_ introduced the following bill;  
which was referred to the Committee on \_\_\_\_\_

---

## A BILL

To amend the Department of Commerce and Labor Act to ensure the public safety and national security through encryption management and licensing, and for other purposes.

1 Be it enacted by the Senate and House of Repre-  
2 sentatives of the United States of America in  
3 Congress assembled,

4 **SEC. 1. SHORT TITLE.**

5 This Act may be cited as the "Encryption Manage-  
6 ment and Licensing Act of 1995".

7 **SEC. 2. FINDINGS AND PURPOSES.**

8 (a) **FINDINGS.** - The Congress finds the following:

2

1           (1) Advancements in communications and  
2 information technology and the widespread use of that  
3 technology have stimulated the volume and enhanced the  
4 value of domestic and international wire and  
5 electronic communications and electronically-stored  
6 information.

7           (2) The development of the Nation's information  
8 infrastructure and the realization of the full  
9 benefits of that infrastructure require that wire and  
10 electronic communications and electronic information  
11 communicated over, and resident in, that infra-  
12 structure be secure, confidential, and authentic.

13           (3) Security, privacy, and authentication of  
14 wire and electronic communications and electronic  
15 information communicated over, or resident in, the  
16 Nation's information infrastructure are enhanced with  
17 the use of encryption technology.

18           (4) Although encryption technology is a valuable  
19 tool to protect the security and privacy of wire and  
20 electronic communications and electronic information,  
21 such technology can be misused by terrorists, other  
22 dangerous and violent criminals, organized crime  
23 syndicates, drug-trafficking organizations, and spies  
24 to avoid detection and to hide evidence of their  
25 criminal activity, thereby jeopardizing effective law

1 enforcement, public safety, and the national security.

2

3 (5) The rights of individuals and business  
4 entities to secure and protect the transmission and  
5 storage of their wire and electronic communications  
6 and electronic information should be preserved.

7 (6) The ability of government agencies, in a  
8 timely manner, to decipher and obtain the plaintext  
9 content of wire and electronic communications and  
10 electronic information necessary to provide for  
11 effective law enforcement, the public safety, and  
12 national security should also be preserved.

13 (7) There is a national need to develop, adopt,  
14 and use encryption management methods and procedures  
15 that advance the development of the Nation's infor-  
16 mation infrastructure and enhance the ability of law-  
17 abiding citizens to secure and protect their wire and  
18 electronic communications and information while at the  
19 same time preserving the government's ability to  
20 decipher and obtain the plaintext of communications in  
21 a timely way, through a Government licensing program.

22 (b) PURPOSES. - It is the purpose of this Act--

23 (1) to promote the development of the Nation's  
24 information infrastructure consistent with public  
25 welfare and safety, efficient law enforcement,

4.

1 national security, and the privacy and protection of  
2 communications and information;

3 (2) to encourage and facilitate the development,  
4 adoption, and use of encryption products that provide  
5 security, protection, and authentication of wire and  
6 electronic communications and electronic information  
7 and that reasonably satisfy the needs of government  
8 agencies to provide for effective law enforcement, the  
9 public safety, and national security; and

10 (3) to carry out that policy through the  
11 development and use of a program to facilitate the  
12 production of such encryption products through  
13 Government licensing.

14 **SEC. 3. UNLAWFUL ACTS.**

15 (a) It shall be unlawful for any person --

16 (1) knowingly to import, or to manufacture an  
17 encryption product for the purpose of distributing  
18 such product, or attempt to so import or manufacture,  
19 without a license issued under this Act, provided,  
20 however, that it shall not be a violation of this  
21 paragraph to manufacture an encryption product for the  
22 sole purpose of developing a prototype with the  
23 objective of testing such prototype prior to obtaining  
24 a license and submitting such prototype to the  
25 Secretary for licensing pursuant to section 4;

1           (2) knowingly to withhold material information; or  
2           knowingly to make any false, fictitious or fraudulent  
3           statement or representation, either orally or in  
4           writing; or to make or use any false writing or  
5           document knowing the same to contain any false,  
6           fictitious, or fraudulent statement or entry; for the  
7           purpose of obtaining a license under the provisions of  
8           this Act;

9           (3) knowingly to distribute, or to cause to be  
10          distributed, any unlicensed encryption product, or to  
11          attempt to do so, provided, however, that it shall be  
12          an affirmative defense to a prosecution under this  
13          paragraph that the defendant had a good faith belief  
14          that the encryption product was properly licensed or  
15          that no license was required, and the defendant shall  
16          have the burden of proving, by a preponderance of the  
17          evidence, such affirmative defense;

18          (4) if a licensee, knowingly to distribute, or to  
19          cause to be distributed, any licensed encryption  
20          product that fails to comply with the terms or  
21          conditions of the license therefor;

22          (5) intentionally to make available a key or  
23          component thereof or disclose other information  
24          required for decryption of an encryption product  
25          licensed under this Act to a government agency or  
26          employee thereof or other person, knowing that such

6

1 agency, employee, or other person is not legally  
2 authorized to receive it;

3 (6) intentionally to obtain or use an encryption  
4 key, a component thereof, or decryption information  
5 required for decryption of communications or  
6 information, pursuant to section pursuant to section  
7 5(a)(2)(A) or (B), without lawful authority or, having  
8 received such key, component thereof or decryption  
9 information with lawful authority, to exceed such  
10 authority for the purpose of decrypting information.

11 (7) having notice that a government agency has  
12 requested or has had released to it keys, components  
13 thereof or other decryption information required for  
14 decryption of communications or information pursuant  
15 to Section 5(a)(2) of this Act, to give notice or  
16 attempt to give notice of the request or release to  
17 any person in order to obstruct, impede, or prevent  
18 the use of such keys, components thereof or other  
19 decryption information by such government agency, or  
20 in order to obstruct, impede, or prevent the search,  
21 seizure or interception of wire, oral or electronic  
22 communications for which the keys, components, or  
23 other decryption information is required.

24 (b) Any person who violates this section after  
25 the effective date set forth in section 13, upon

7

1 conviction, shall be punished as provided in section.  
2 8.

3

4 **SEC. 4. ENCRYPTION MANAGEMENT AND LICENSING.**

5 The Secretary shall establish an Encryption  
6 Management and Licensing Program to carry out this  
7 Act.

8 (a) Establishment of Criteria -- In carrying out  
9 this Act, the Secretary, with the concurrence of the  
10 Attorney General, shall through this program estab-  
11 lish and publish criteria for encryption products that  
12 will ensure that government agencies can decrypt, on  
13 a timely basis, communications and information  
14 lawfully obtained. The Secretary shall grant a  
15 license request for the manufacture or import of an  
16 encryption product only if that product meets the  
17 criteria established by the Secretary.

18 (b) Considerations for Criteria.

19 (1) In establishing the licensing criteria  
20 pursuant to subsection (a), the Secretary shall  
21 consider (to the maximum extent feasible consistent  
22 with the need for government agencies to retain the  
23 ability to decipher, in a timely manner, wire and  
24 electronic communications and electronic information  
25 lawfully obtained) the need to preserve the security,  
26 confidentiality, integrity and authenticity of wire

1 and electronic communications and electronic  
2 information; and the need to advance the Nation's  
3 information infrastructure. Nothing in this  
4 subsection is intended to permit the Secretary to deny  
5 a license request for the manufacture or import of any  
6 encryption product on the ground that such product  
7 fails to meet standards of performance with respect to  
8 the security, confidentiality, integrity and  
9 authenticity of wire and electronic communications and  
10 electronic information.

11 (2) In establishing the licensing criteria  
12 pursuant to subsection (a), the Secretary shall not  
13 diminish the statutory and constitutional privacy  
14 rights of individuals and other persons.

15 (c) Consultation -- In developing any criteria under  
16 subsection (a), the Secretary shall consult with other  
17 appropriate Federal agencies, and may consult with  
18 representatives of manufacturers and importers of  
19 encryption products.

20 (d) Exemptions -- The Secretary, upon obtaining the  
21 concurrence of the Attorney General, shall be  
22 authorized to exempt from coverage under this Act any  
23 type or level of encryption product deemed  
24 appropriate, as long as such exemption is consistent  
25 with the purposes of this Act.

1 (e) Validation Procedure -- As part of the Licensing  
2 Program described in subsection (a), the Secretary  
3 shall establish a validation procedure by which the  
4 Secretary may determine the extent to which encryption  
5 products submitted for licensing meet the licensing  
6 criteria established by the Secretary.

7 (f) Licensing Procedures

8 (1) An application for a license to import or  
9 manufacture an encryption product shall be made to the  
10 Secretary and shall be in such form and contain such  
11 information as the Secretary shall by regulation  
12 prescribe. Each applicant for a license shall pay a  
13 fee to be charged as set by the Secretary. Each  
14 license shall be valid for no longer than three years  
15 from date of issuance and shall be renewable upon the  
16 same conditions and subject to the same restrictions  
17 as the original license upon payment of a renewal fee,  
18 unless such product is found not to permit the  
19 decryption as required or not to be otherwise in  
20 substantial compliance with the license or any rule,  
21 regulation, or requirement prescribed by the Secretary  
22 under this Act.

23 (2) The Secretary shall approve or deny any  
24 application within a period of sixty days beginning on  
25 the date such application is received.

1           (3) The Secretary may revoke any license issued  
2 under this section if in the opinion of the Secretary  
3 the holder thereof has violated any provision of this  
4 Act or any rule, regulation, or requirement prescribed  
5 by the Secretary under this Act.

6           (g) Audit Procedures -- The Secretary shall establish  
7 audit procedures to ensure that the purposes of the  
8 program are appropriately carried out.

9  
10       **SEC. 5. KEY-ESCROW AND NON-KEY ESCROW ENCRYPTION**  
11       **PRODUCT PROCEDURES**

12           The Secretary shall grant a license request for  
13 the manufacture or import of any encryption product  
14 that meets the criteria established by the Secretary  
15 pursuant to section 4, including key-escrow encryption  
16 products and non-key-escrow encryption products. As  
17 part of the Licensing Program established pursuant to  
18 section 4, the Secretary shall establish procedures  
19 and requirements for key-escrow encryption products  
20 and non-key escrow encryption products, which shall  
21 include the following.

22           (a) Key-Escrow Encryption Products -- The Secretary  
23 shall establish the following procedures and  
24 requirements for key-escrow encryption products.

25

11

1 (1) ESCROW AGENTS --

2 (A) APPROVAL -- The Secretary may approve  
3 Federal agencies or suitable private sector entities  
4 that satisfy qualifications established by the  
5 Secretary, which shall include but not be limited to  
6 the qualifications enumerated in paragraph (B), to act  
7 as key-escrow agents for encryption products for which  
8 a license is granted pursuant to section 4 of this  
9 Act. The Secretary shall also have the power, in  
10 consultation with the Attorney General, to revoke the  
11 authority of any such Federal agency or private sector  
12 entity to serve as such key-escrow agent.

13 (B) QUALIFICATIONS -- In order to be approved as a  
14 key escrow agent, a Federal agency or a private sector  
15 entity shall --

16 (i) possess the capability, competency, and  
17 resources to administer key escrow encryption, to  
18 safeguard sensitive information related to it,  
19 and to carry out the responsibilities set forth  
20 in paragraph (C) in a timely manner; but

21 (ii) not be a Federal law enforcement agency.

22 (C) RESPONSIBILITIES -- A key escrow agent approved  
23 under paragraph (A) shall, consistent with regu-  
24 lations issued by the Secretary, establish procedures  
25 and take other appropriate steps--

12

1 (i) to ensure the confidentiality, integrity,  
2 and timely release of keys or components thereof held  
3 by the agent pursuant to this subsection;

4 (ii) to protect the confidentiality of the  
5 identity of the person or persons owning encryption  
6 products for which such key escrow agent holds keys or  
7 components thereof;

8 (iii) to protect the confidentiality of the  
9 government agency and all information concerning such  
10 agency's access to and use of encryption keys or  
11 components thereof;

12 (iv) to hold and manage the keys or components  
13 thereof consistent with the requirements of this  
14 section and the encryption criteria established in  
15 accordance with section 4; and

16 (v) to carry out the responsibilities set forth  
17 in this subsection in the most effective and efficient  
18 manner practicable.

19 (D) AUTHORITY -- A Federal agency approved as a  
20 key escrow agent under this section may enter into  
21 contracts, cooperative agreements, and joint ventures  
22 and take other appropriate steps to carry out its  
23 responsibilities.

24 (2) LIMITATIONS ON ACCESS AND USE --

25 (A) Release of Key Information to Certain Entities --

13

1 A key escrow agent approved under subsection (a) (1) (A)  
2 shall release a key or component thereof held by the  
3 agent pursuant to that subsection only to --

4 (i) A government agency that provides a  
5 certification that it is authorized by law to conduct  
6 electronic surveillance, a search, or other  
7 examination of communications or information pursuant  
8 to such lawful authority and requires access to the  
9 key or component thereof in order to determine the  
10 plaintext of the communication or information so  
11 acquired. Key escrow agents shall release keys or  
12 components thereof to the requesting government agency  
13 upon their receipt of such a certification executed by  
14 the Attorney General, Deputy Attorney General,  
15 Associate Attorney General, any Assistant Attorney  
16 General or Acting Assistant Attorney General, or any  
17 Deputy Assistant Attorney General in the Criminal  
18 Division of the Department of Justice; by a United  
19 States Attorney, Assistant United States Attorney, or  
20 other attorney for the government supervising the  
21 investigation in which such electronic surveillance,  
22 search or other examination of communications or  
23 information is being conducted; in the case of an  
24 agency of a State or political subdivision thereof, by  
25 the principal prosecuting attorney of such State or  
26 political subdivision; by a judge or other authorized

---

1 official of a Federal court of competent jurisdiction;  
2 or, in the case of an agency of a State or political  
3 subdivision thereof, by a judge or other authorized  
4 official of a State court of competent jurisdiction.  
5 A government agency to whom a key or component thereof  
6 has been released under this paragraph may use the key  
7 or component thereof only in a manner consistent with  
8 the court order or other lawful authorization  
9 permitting the acquisition of the communication or  
10 information; or

11 (ii) a Federal agency for use by such agency, or  
12 for conveyance to another Federal agency for the use  
13 of the latter, in the lawful collection of foreign  
14 intelligence or counterintelligence. Key escrow  
15 agents shall release keys or components thereof to the  
16 requesting government agency upon their receipt of a  
17 certification executed by the Attorney General, Deputy  
18 Attorney General, Associate Attorney General, any  
19 Assistant Attorney General or Acting Assistant  
20 Attorney General, or any Deputy Assistant Attorney  
21 General in the Criminal Division, or the Counsel for  
22 Intelligence Policy, of the Department of Justice.

23 (B) No key escrow agent, or officer, employee,  
24 or agent thereof, shall disclose to any person, other  
25 than authorized personnel of the Federal government,  
26 the facts or circumstances of any release of keys or

15

1 key components or requests therefor. This provision  
2 does not, however, prohibit such escrow agent,  
3 officer, employee, or agent from providing evidence in  
4 any proceeding held under the authority of the United  
5 States or of any State or political subdivision  
6 thereof, nor from disclosing such information as is  
7 necessary to permit audits or inspections of the  
8 operations of such key escrow agent in accordance with  
9 regulations promulgated by the Secretary.

10 (C) Nothing in this subsection shall be  
11 construed to prohibit a private sector key escrow  
12 agent from releasing keys or key components for  
13 encryption products to the owners of such products  
14 pursuant to contractual or other commercial  
15 arrangements therefor, nor to prohibit any key escrow  
16 agent from releasing keys or key components for  
17 encryption products to any person in conformance with  
18 a determination by a court of competent jurisdiction  
19 that such person is lawfully entitled to hold such  
20 keys or key components.

21 (3) RESPONSIBILITIES OF MANUFACTURERS AND  
22 IMPORTERS -- A manufacturer of a key-escrow encryption  
23 product licensed under this Act shall, no later than  
24 the time any individual unit of such licensed product  
25 leaves its control, deposit with one or more approved  
26 key escrow agents, keys, components thereof, or other

---

16

1 information necessary for decryption applicable to  
2 that unit; and an importer of a key-escrow encryption  
3 product licensed under this Act, shall, no later than  
4 the time any individual unit of such licensed product  
5 enters the United States, deposit with one or more  
6 approved key escrow agents, keys, components thereof,  
7 or other information necessary for decryption  
8 applicable to that unit.

9 (4) KEY ESCROW FUNDING--

10 Within one hundred and eighty days after the  
11 date of enactment of this Act, the Secretary shall  
12 make recommendations to the congressional committees  
13 having oversight of the Department of Commerce  
14 regarding the estimated funding requirements for any  
15 key escrow agents as may be deemed appropriate by the  
16 Secretary.

17 (5) LIABILITY -- Any key escrow agent approved  
18 by the Secretary shall be held to a standard of  
19 reasonable care in carrying out those responsibilities  
20 prescribed by the Secretary.

21 (b) NON-KEY ESCROW ENCRYPTION PRODUCTS -- The  
22 decryption methodologies required to meet governmental  
23 requirements for non-key escrow encryption products  
24 may be retained by the manufacturer, the vendor, or  
25 any other entity, including a key escrow agent,  
26 approved by the Secretary. The types of

17

1 responsibilities and the limitations on access  
2 specified for key escrow agents under subsection (a)  
3 (1) (c) and (a) (2), respectively, shall also apply to  
4 non-key escrow product manufacturers, vendors, or  
5 other entities that retain decryption methodologies.  
6 The manufacturer, vendor, or other entity shall be  
7 held to a standard of reasonable care in carrying out  
8 those responsibilities prescribed by the Secretary and  
9 in providing access to decryption methods.

10 (c) FEDERAL GOVERNMENT LIABILITY -- The United States  
11 shall not be liable for any loss incurred by any  
12 individual or entity resulting from any violation of  
13 this Act or the failure to exercise reasonable care in  
14 the performance of any duties under any regulation or  
15 procedure established by or under this Act, or  
16 resulting from any action by any person who is not an  
17 official or employee of the United States.

18

19 SEC. 6. REGULATIONS -- Within one hundred and eighty  
20 days after the date of the enactment of this Act, the  
21 Secretary shall, after notice to the public and  
22 opportunity for comment, issue any regulations  
23 necessary to carry out this Act.

24

25 SEC. 7. LIABILITY OF MANUFACTURERS -- Manufacturers of  
26 encryption products which are licensed under this Act

1 shall be held to a standard of reasonable care with  
2 regard to the manufacturing of such products.

3

4 **SEC. 8. PENALTIES** -- Any person who violates section  
5 3 of this Act shall be fined under title 18, United  
6 States Code, or imprisoned not more than five years,  
7 or both.

8 **SEC. 9. INJUNCTION** -- The Attorney General may bring  
9 an action to enjoin any person (including an officer  
10 or employee of a government agency) from committing  
11 any violation of this Act. The district courts of  
12 the United States shall have jurisdiction of any  
13 action brought by the Attorney General under this  
14 paragraph.

15

16 **SEC. 10. SEVERABILITY** -- If any provision of this Act,  
17 or the application thereof, to any person or  
18 circumstance, is held invalid, the remainder of this  
19 Act, and the application thereof, to other persons or  
20 circumstances shall not be affected thereby.

21

22 **SEC. 11. DEFINITIONS** -- For purposes of this section:

23 (1) The term 'content', when used with respect  
24 to a wire or electronic communication or to electronic  
25 information, includes the substance, purport, or  
26 meaning of that information.

1           (2) The term 'electronic communication service'  
2 has the meaning given such term in section 2510 (15)  
3 of title 18, United States Code.

4           (3) The term 'electronic communications system'  
5 has the meaning given such term in section 2510(14) of  
6 title 18, United States Code.

7           (4) The term 'encryption product' means any  
8 product (including, but not limited to, hardware,  
9 firmware, or software, or some combination thereof),  
10 that is designed, adapted, or configured to use a  
11 cryptographic algorithm to protect the confidentiality  
12 of data.

13           (5) The term 'key escrow encryption' means an  
14 encryption method that allows for the storing of keys  
15 or components thereof with the intent of using the key  
16 or component thereof to decipher encrypted  
17 communications or information.

18           (6) The term 'key escrow agent' means an entity  
19 approved by the Secretary to hold and manage keys or  
20 components thereof associated with key escrow  
21 encryption products licensed under this Act.

22           (7) The term 'key' means a sequence of symbols  
23 that determines the transformation from unencrypted  
24 plaintext to encrypted ciphertext and vice versa.

25           (8) The term 'electronic information' means the  
26 content of any information in any electronic form

1 which is stored, processed, transmitted or otherwise  
2 communicated, in an electronic communications system.

3 (9) The term 'electronic communication' has the  
4 meaning given such term in section 2510(12) of title  
5 18, United States Code; or

6 (10) The term 'wire communication' has the  
7 meaning given such term in section 2510(1) of title  
8 18, United States Code.

9 (11) The term 'government' means the Government  
10 of the United States and any agency or instrumentality  
11 thereof, a State or political subdivision of a State,  
12 the District of Columbia, or a commonwealth,  
13 territory, or possession of the United States.

14 (12) The term 'person' means any individual,  
15 corporation, company, association, firm, partnership,  
16 society, or joint stock company.

17 (13) The term 'distribute' means to sell, issue,  
18 give, transfer, transport, ship, or make available to  
19 another individual, corporation, company, association,  
20 firm, partnership, society, or joint stock company.

21 (14) The term 'Secretary' means the Secretary of  
22 Commerce or his or her designee.

23 (15) The term 'Attorney General' means the  
24 Attorney General of the United States or his or her  
25 designee.

26

1       **SEC. 12. AUTHORIZATION OF APPROPRIATIONS.--**

2                   There are authorized to be appropriated to  
3       the Secretary of Commerce for the purpose of carrying  
4       out this Act a total of \$50,000,000 for fiscal years  
5       1996, 1997, 1998, and 1999. Such sums are authorized  
6       to remain available until expended.

7

8       **SEC. 13. EFFECTIVE DATE.--**

9                   (a) IN GENERAL.-- Except as provided in  
10       subsection (b), this Act shall take effect on the date  
11       of enactment.

12                   (b) The provisions of Sections 3 and 8 of  
13       this Act shall take effect on the date that is 3 years  
14       after the date of enactment of this Act.

15

---

~~SENSITIVE~~~~SENSITIVE~~**DRAFT**

104th CONGRESS

1st Session

**H.R.** \_\_\_\_\_

---

**IN THE HOUSE OF REPRESENTATIVES**

Mr. \_\_\_\_\_ of \_\_\_\_\_ introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

**A BILL**

To ensure the public safety and national security by providing for a system of key-escrow encryption, and to provide relief from antitrust liability for persons who voluntarily agree to develop, adopt, use or only distribute encryption products that permit appropriate government access, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

**TITLE I -- GENERAL PROVISIONS****SEC. 101. SHORT TITLE.**

This Act may be cited as the "Data Security Act of 1995".

**SEC. 102. FINDINGS AND PURPOSES.**

(a) **FINDINGS.** - The Congress finds the following:

(1) Advancements in communications and information technology and the widespread use of that technology have stimulated the volume and enhanced the value

---

of domestic and international wire and electronic communications and electronically-stored information, as well as the ability to preserve the security, protect the privacy, and authenticate the origin, of such communications and information.

(2) The development of the Nation's information infrastructure and the realization of the full benefits of that infrastructure require that wire and electronic communications and electronic information communicated over, and resident in, that infrastructure be secure, confidential, and authentic.

(3) Security, privacy, and authentication of wire and electronic communications and electronic information communicated over, or resident in, the Nation's information infrastructure are enhanced with the use of encryption technology.

(4) Although encryption technology is a valuable tool to protect the security and privacy of wire and electronic communications and electronic information, such technology can be misused by terrorists, other dangerous and violent criminals, organized crime syndicates, drug-trafficking organizations, and spies to avoid detection and to hide evidence of their criminal activity, thereby jeopardizing effective law enforcement, public safety, and the national security.

(5) The rights of individuals and business entities to secure and protect the transmission and storage of their wire and electronic communications and electronic information should be preserved.

(6) The authority and ability of government agencies, in a timely manner, to

encryption products is not impeded by the risk of antitrust liability.

**SEC. 103. DEFINITIONS. -- For purposes of this Act:**

(1) The term "antitrust laws" means the antitrust laws, as such term is defined in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), and section 5 of the Federal Trade Commission Act (15 U.S.C. 45) (to the extent that such section 5 prohibits unfair methods of competition), and any State antitrust or unfair competition law.

(2) The term "content", when used with respect to a wire or electronic communication or to electronic information, includes the substance, purport, or meaning of that information.

(3) The term "electronic communication service" has the meaning given such term in section 2510 (15) of title 18, United States Code.

(4) The term "electronic communications system" has the meaning given such term in section 2510(14) of title 18, United States Code.

(5) The term "encryption product" means any product (including, but not limited to, hardware, firmware, or software, or some combination thereof), that is designed, adapted, or configured to use a cryptographic algorithm to protect the confidentiality of data.

(6) The term "key escrow encryption" means an encryption method that allows for the storing of keys or components thereof with the intent of using the key or component thereof to decipher encrypted communications or information.

(7) The term "key escrow agent" means an entity approved by the Secretary to hold and manage keys or components thereof associated with key escrow encryption products licensed under this Act.

(8) The term "key" means a sequence of symbols that determines the transformation from unencrypted plaintext to encrypted ciphertext and vice versa.

(9) The term "electronic information" means the content of any information in any electronic form which is stored, processed, transmitted or otherwise communicated, in an electronic communications system.

(10) The term "electronic communication" has the meaning given such term in section 2510(12) of title 18, United States Code; or

(11) The term "wire communication" has the meaning given such term in section 2510(1) of title 18, United States Code.

(12) The term "government" means the Government of the United States and any agency or instrumentality thereof, a State or political subdivision of a State, the District of Columbia, or a commonwealth, territory, or possession of the United States.

(13) The term "person" means any individual, corporation, company, association, firm, partnership, society, or joint stock company.

(14) The term "Secretary" means the Secretary of Commerce or his or her designee.

(15) The term "Attorney General" means the Attorney General of the United

States or his or her designee.

**TITLE II -- AMENDMENTS TO TITLE 15 OF THE UNITED STATES CODE**  
**SEC. 201. EXEMPTION.**

No person shall be liable under the antitrust laws for damages, penalties, injunctive relief, or other sanctions, for negotiating, entering into, participating in or implementing an agreement to --

(1) engage in joint development of encryption products to the extent necessary to ensure the ability of government agencies to decipher, in a timely manner, wire and electronic communications and electronic information that have been intercepted pursuant to electronic surveillance laws or obtained under other lawful authorization;

or

(2) make available only those encryption products that ensure the ability of government agencies to decipher, in a timely manner, wire and electronic communications and electronic information that have been intercepted pursuant to electronic surveillance laws or obtained under other lawful authorization.

**SEC. 202. LIMITATIONS.**

The exemption provided in section 4 of this Act shall not apply to any agreement concerning price or other terms or conditions of sale of any such product produced or sold by any such person, or that results in a boycott of any person.

**TITLE III -- AMENDMENTS TO THE DEPARTMENT  
OF LABOR AND COMMERCE ACT**

**SEC. 301. KEY-ESCROW ENCRYPTION PRODUCT PROCEDURES**

The Secretary shall establish procedures and requirements for operation of a system of key-escrow encryption, including provisions for access, when necessary, to keys or components thereof.

**(a) ESCROW AGENTS --**

**(1) APPROVAL --** The Secretary may approve Federal agencies or suitable private sector entities that satisfy qualifications established by the Secretary, which shall include but not be limited to the qualifications enumerated in paragraph (2), to act as key-escrow agents for key-escrow encryption products. The Secretary shall also have the power, in his sole discretion, to revoke the authority of any such Federal agency or private sector entity to serve as such key-escrow agent.

**(2) QUALIFICATIONS --** In order to be approved as a key escrow agent, a Federal agency or a private sector entity shall --

**(A)** possess the capability, competency, and resources to administer key escrow encryption, to safeguard sensitive information related to it, and to carry out the responsibilities set forth in paragraph (3) in a timely manner; but

**(B)** not be a Federal law enforcement agency.

**(3) RESPONSIBILITIES --** A key escrow agent approved under paragraph (1)

shall, consistent with regulations issued by the Secretary, establish procedures and take other appropriate steps--

(A) to ensure the confidentiality, integrity, and timely release of keys or components thereof held by the agent pursuant to this subsection;

(B) to protect the confidentiality of the identity of the person or persons owning encryption products for which such key escrow agent holds keys or components thereof;

(C) to protect the confidentiality of the identity of the government agency requesting encryption keys or components thereof and all information concerning such agency's access to and use of encryption keys or components thereof;

(D) to hold and manage the keys or components thereof consistent with the requirements of this section; and

(E) to carry out the responsibilities set forth in this subsection in the most effective and efficient manner practicable.

(4) **AUTHORITY --** A Federal agency approved as a key escrow agent under this section may enter into contracts, cooperative agreements, and joint ventures and take other appropriate steps to carry out its responsibilities.

**(b) LIMITATIONS ON ACCESS AND USE --**

**(1) Release of Key Information to Certain Entities --**

A key escrow agent approved under subsection (a)(1) shall release a key or

component thereof held by the agent pursuant to that subsection only to --

(A) A government agency that provides a certification that it is authorized by law to conduct electronic surveillance, a search, or other examination of communications or information pursuant to such lawful authority and requires access to the key or component thereof in order to determine the plaintext of the communication or information so acquired. Key escrow agents shall release keys or components thereof to the requesting government agency upon their receipt of such a certification executed by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General or Acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division of the Department of Justice; by a United States Attorney, Assistant United States Attorney, or other attorney for the government supervising the investigation in which such electronic surveillance, search or other examination of communications or information is being conducted; in the case of an agency of a State or political subdivision thereof, by the principal prosecuting attorney of such State or political subdivision; by a judge or other authorized official of a Federal court of competent jurisdiction; or, in the case of an agency of a State or political subdivision thereof, by a judge or other authorized official of a State court of competent jurisdiction. A government agency to whom a key or component thereof has been released under this paragraph may use the key or component thereof only in a manner

consistent with the court order or other lawful authorization permitting the acquisition of the communication or information; or

(B) a Federal agency for use by such agency, or for conveyance to another Federal agency for the use of the latter, in the lawful collection of foreign intelligence or counterintelligence. Key escrow agents shall release keys or components thereof to the requesting government agency upon their receipt of a certification executed by the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General or Acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division, or the Counsel for Intelligence Policy, of the Department of Justice.

(2) No key escrow agent, or officer, employee, or agent thereof, shall disclose to any person, other than authorized personnel of the Federal government, the facts or circumstances of any release of keys or key components or requests therefor. This provision does not, however, prohibit such escrow agent, officer, employee, or agent from providing evidence in any proceeding held under the authority of the United States or of any State or political subdivision thereof, nor from disclosing such information as is necessary to permit audits or inspections of the operations of such key escrow agent in accordance with regulations promulgated by the Secretary.

(3) Nothing in this subsection shall be construed to prohibit a private sector key escrow agent from releasing keys or key components for encryption

products to the owners of such products pursuant to contractual or other commercial arrangements therefor, nor to prohibit any key escrow agent from releasing keys or key components for encryption products to any person in conformance with a determination by a court of competent jurisdiction that such person is lawfully entitled to hold such keys or key components.

(c) **AUDIT PROCEDURES** -- The Secretary shall establish audit procedures to ensure that the purposes of the program are appropriately carried out.

(d) **KEY ESCROW FUNDING**-- Within one hundred and eighty days after the date of enactment of this Act, the Secretary shall make recommendations to the congressional committees having oversight of the Department of Commerce regarding the estimated funding requirements for any key escrow agents as may be deemed appropriate by the Secretary.

(e) **LIABILITY** --

(1) Any key escrow agent approved by the Secretary shall be held to a standard of reasonable care in carrying out those responsibilities prescribed by the Secretary.

(2) The United States shall not be liable for any loss incurred by any individual or entity resulting from any violation of this Act or the failure to exercise reasonable care in the performance of any duties under any regulation or procedure established by or under this Act, nor resulting from any action by

any person who is not an official or employee of the United States.

**SEC. 302. REGULATIONS** -- Within one hundred and eighty days after the date of the enactment of this Act, the Secretary shall, after notice to the public and opportunity for comment, issue any regulations necessary to carry out this Act.

**SEC. 303. UNLAWFUL ACTS.**

(a) It shall be unlawful for any person --

(1) intentionally to make available a key or component thereof to a government agency or employee thereof or other person, knowing that such agency, employee, or other person is not entitled to receive it;

(2) intentionally to obtain or use an encryption key, a component thereof, or decryption information required for decryption of communications or information, pursuant to section 301(b)(1), without lawful authority or, having received such key, component thereof or decryption information with lawful authority, exceeding such authority for the purpose of using such key, component thereof, or decryption information improperly; or

(3) having notice that a government agency has requested or has had released to it keys, components thereof or other decryption information required for decryption of communications or information pursuant to Section 301(a) of this Act, in order to obstruct, impede, or prevent the use of such keys, components thereof or other decryption information by such government agency, gives notice or attempts to give notice of the request or release to any person.

(b) Any person who violates this section shall, upon conviction, be punished as provided in section 304.

**SEC. 304. PENALTIES** -- Any person who violates section 303 of this Act shall be fined under title 18, United States Code, or imprisoned not more than five years, or both.

**SEC. 305. INJUNCTION** -- The Attorney General may bring an action to enjoin any person (including an officer or employee of a government agency) from committing any violation of this Act. The district courts of the United States shall have jurisdiction of any action brought by the Attorney General under this paragraph.

**SEC. 306. SEVERABILITY** -- If any provision of this Act, or the application thereof, to any person or circumstance, is held invalid, the remainder of this Act, and the application thereof, to other persons or circumstances shall not be affected thereby.

**SEC. 307. AUTHORIZATION OF APPROPRIATIONS.**-- There are authorized to be appropriated to the Secretary of Commerce for the purpose of carrying out this Act a total of \$\_\_\_\_\_ for fiscal years 1996, 1997, 1998, and 1999. Such sums are authorized to remain available until expended.

**SEC. 308. EFFECTIVE DATE.**-- This Act shall take effect on the date of its enactment.