
Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a publication.

Publications have not been scanned in their entirety for the purpose of digitization. To see the full publication please search online or visit the Clinton Presidential Library's Research Room.

Digital Telephony and Communications Privacy Improvement Act of 1994



*A legislative proposal to protect the American public from
criminal activity and ensure privacy in telecommunications.*

4/28/94

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a publication.

Publications have not been scanned in their entirety for the purpose of digitization. To see the full publication please search online or visit the Clinton Presidential Library's Research Room.

Digital Telephony and Communications Privacy Improvement Act of 1994



*A legislative proposal to protect the American public from
criminal activity and ensure privacy in telecommunications.*

Meeting w/ Sheila, Bork, Conrad 5/6/94
Div. Seven

- Digital telephony
 - Encryption
- } Should these be separated? (Sheila)

- Leahy has asked Biden to hold off introducing the bill until he meets w/ industry

3 areas that are problematic to Leahy

① FBI "No exception" rule

② Penalties are too strong

③ Unacceptable to use govt. as gatekeeper for new technology

In 92 there were 2 attempts to have legislation by the Admin.

Industry told Barr don't legislate, we will get all our techs together and work it out

Crim Div

↳ What does Leahy propose so that L.E. can protect itself?

2

Sheila → Leahy wants to work out his concerns before the bill is introduced

Leahy is staying in close contact w/ the House

Crin: Would he support some kind of legislation that would allow L.E. to function?

Sheila: yes

Digital telephony was not in the '92 Crime Bill that was filibustered

Podesta can't talk to FBI coz of Whitewater investigation ~~is~~ going on

How will Brooks react to this?

Brink: Brooks will not jump over Edwards & his sub. jurisdiction over this issue

Sheila: FBI wants to move this as quickly as possible

DoJ → keep encryption away from telephony for Brooks is safe
So 2 track approach

Brink -> FBI says telephony is more critically
timely

Chris Schroeder the world of encryption is OK as far
as we are concerned
Leahy will have to go on the
offensive legislatively
We don't need any legislation to get
what we want
we are trying to head off leg.

Sheila FBI is mtg w/ Biden's people on this
Biden will defer to Leahy until this mtg that
Leahy wants takes place

(EFF) Electric Frontier Foundation
(group founded by Mitch Kapor)
that is where the mtg is going to take place
w/ worried about protecting civil liberties in
cyberspace
they have opposed this & the clipper chip
Nelson (OTSP) doesn't think the Admin
should appear at this mtg.

MARK (rm) why don't we invite the techs in here to
mark id is north hill?

Nelson

↳ until Hill ~~makes some indication~~
gives some indication that they are going to
move then techs will stonewall

Will Biden's people going to be at this mtg?

→ It would be real helpful if they were there
cuz then indicate that they some movement

Brnk get Brooks staffer to go to counter Dempsey
↳ (Alan Ehrenbaum)

Will this mtg cover the 3 Leahy issues?

DT guy → techy to techy mtg. can't resolve those
3 issues

Sheila is going to talk to Bruce Cohen some
more

Industry is putting together a draft bill

MARK (ccrim) it would be very useful to see that
before Friday's mtg.

Sheila Brooks is not interested in doing anything
until after the crime Bill

ME FBI is not at this mtg?

FBI is taking the position that this bill
can not be changed

Sheila day's reluctance to move a bill is just
getting something to agree upon

→ 1st of wk set up ^{internal} mtg of FBI

reconvene of this group on Tuesday

Leahy will probably not bill of particulars
to Sheila until late Monday

[Telephony →
Whether you get the message

[Encryption →
Whether you can read it



U.S. Department of Justice
Office of Legislative Affairs

Office of the
Assistant Attorney General

Washington, D.C. 20530

Davis,
Here's the Spectrum
Language!

106

Spectrum

TITLE _____

SECTION _01. SHORT TITLE.

This Title may be cited as the "National Law Enforcement and Public Safety Communications Act of 1995."

SECTION _02. FINDINGS.

"(a) The Congress finds as follows:

(1) The National Telecommunications and Information Administration of the Department of Commerce manages the frequency spectrum for all federal agencies and authorizes frequency use for all federal radio communications systems. The Federal Communications Commission (hereafter referred to as "the Commission"), an independent agency created by the Communications Act of 1934, licenses frequencies for all non-federal radio users, including state and local law enforcement and public safety agencies.

(2) The Omnibus Budget Reconciliation Act of 1993 required the government to transfer a minimum of 200 Megahertz (MHz) of frequency spectrum from federal users to private users. A total of 235 MHz was transferred, but has not yet been auctioned or reallocated by the Federal Communications Commission. Of the 235 MHz transferred, 45 MHz of frequency spectrum between 1710 and 1755 MHz bandwidth was previously assigned to federal law enforcement agencies. The cost to the Department of Justice alone to vacate frequencies affected by this reallocation is estimated at \$144 million; however, no funding has been budgeted for the move to new frequencies or the purchase of new equipment.

(3) The President has announced his intention to expand the authority of the Commission to use competitive bidding in assigning licenses and other valuable telecommunications services or resources and to provide for the transfer of additional federal government frequency spectrum to non-federal users to facilitate and stimulate continued growth of commercial and other wireless telecommunications services.

(4) Federal, state, and local law enforcement and public safety agencies do not have sufficient frequency spectrum allocations to meet existing requirements. Increasing demands are being placed on law enforcement and public safety communications systems. Additional frequency spectrum is needed to meet basic voice and data communication requirements.

(5) Federal, state, and local law enforcement and public safety agencies require common blocks of frequency spectrum for interoperable radio communications. Interoperability is critical when communications must be coordinated and shared between multiple agencies and

jurisdictions, such as the recent bombing of the Murrah Federal Office Building in Oklahoma City, Oklahoma, the World Trade Center bombing in New York City, natural disasters and emergencies, and joint law enforcement operations and task forces.

(6) Additional frequency spectrum allocations are needed by law enforcement and public safety agencies to implement new telecommunications technologies and functionalities. For example, frequency spectrum availability is critical to implement features of the NCIC 2000 system which will provide police officers with the ability to send and receive, from patrol cars and other mobile units, digitized fingerprint images and photographs that will aid in the identification of fugitives, violent criminals, and missing persons. Absent frequency spectrum to support wideband communications, law enforcement agencies may not be able to take advantage of these new functionalities and capabilities, thus placing officer safety and communities at risk.

(7) The concept of a nationwide interoperable law enforcement and public safety wireless network has been suggested by the President's National Performance Review (NPR). The Attorney General and the Secretary of the Treasury have assumed leadership roles in establishing a nationwide interoperable wireless communication network for all federal, state, and local law enforcement and public safety agencies through the establishment of the Federal Law Enforcement Wireless Users Group (FLEWUG).

(8) The design and development effort for the NPR initiative is projected to cost \$75,000,000 over a five or more year period. This effort would be focused upon such activities as spectrum requirements studies, assessment of digital wireless communications technology, systems engineering, and pilot programs. Once standards are developed and a national interoperable wireless network defined, individual law enforcement and public safety agencies would begin migrating to the network."

SECTION 10. PRIORITY CONSIDERATION FOR REASSIGNMENT OF TRANSFERRED FREQUENCY SPECTRUM.

"(a) The Commission shall give priority consideration to the frequency spectrum needs of state and local law enforcement and public safety agencies when reallocating frequency spectrum between the 1710 - 1755 MHz bandwidth which was transferred from federal law enforcement agencies under the authority of the National Telecommunications and Information Administration Organization Act (47 U.S.C. Section 923) (hereafter referred to as "the NTIAOA").

(b) Frequency spectrum transferred from federal law enforcement agencies under the authority of the NTIAOA and not

assigned by the Commission to state and local law enforcement and public safety agencies within 24 months after enactment, shall be available for competitive bidding and/or reallocation by the Commission. The proceeds from the competitive bidding of frequency spectrum between 1710 and 1755 MHz shall be deposited into the National Law Enforcement and Public Safety Wireless Network Fund created under Section 30 without regard to the fiscal year limitation on deposits."

SECTION 20. PROTECTION OF INCUMBENT SPECTRUM USERS.

"(a) IN GENERAL - Reallocation of federal spectrum to the Commission shall not disrupt federal law enforcement and public safety communications services and activities, and shall minimize the economic effects to federal users and, thereby, the taxpayer, and shall foster the introduction of new radio-based services and devices.

(b) CONSULTATION WITH THE COMMISSION, THE ATTORNEY GENERAL, AND THE SECRETARIES OF DEFENSE AND THE TREASURY

(1) IN GENERAL - The Secretary of Commerce shall, in the course of identifying and recommending for future reallocation bands of frequencies, consult with the Attorney General, the Secretary of the Treasury, the Secretary of Defense, and the Commission to ensure that law enforcement, public safety, and national security interests and capabilities are not adversely affected by the proposed transfer of frequencies.

(2) SPECIFICALLY - The Secretary of Commerce, in consultation with the Attorney General, the Secretary of the Treasury, and the Secretary of Defense, shall prepare and include in reports submitted to the President and the Congress that identify future transfers of frequency spectrum from federal to non-federal users, a statement identifying the operational and cost impact of the proposed transfer of frequency spectrum upon the current and future operations of affected federal law enforcement, public safety, and national security users.

(c) PROTECTION OF FEDERAL LAW ENFORCEMENT AND EMERGENCY RESPONSE USERS IN SPECTRUM TO BE REALLOCATED.

(1) Notwithstanding any other provision of law, the Secretary of Commerce is prohibited from transferring to the Commission for purposes of auction or reallocation to non-law enforcement or public safety users frequency spectrum assigned to federal law enforcement and emergency response users until the report required under Section 20 has been submitted to the President and the Congress.

(2) In the event that non-federal users seek to use bands that include frequency spectrum licensed on a primary basis to federal law enforcement and emergency response users, the non-federal users will be required: (i) to restrict their use

so as not to cause harmful interference to such federal users, (ii) to compensate such federal users for the total cost of using other frequencies, including, but not limited to, the cost of replacing existing facilities, of conducting engineering and cost analyses of relocated facilities, of moving systems to other frequency spectrum or transmission technologies agreeable to the affected incumbent, or (iii) to take other measures pursuant to the mutual agreement of the government and non-government spectrum users. Federal law enforcement and emergency response users may negotiate with non-federal users for the purpose of agreeing to terms under which the federal entity would relocate to other bands of frequency spectrum or other media, or alternatively, may negotiate sharing agreements with non-federal users that allow acceptable levels of interference to the existing federal user.

(3) Federal law enforcement and emergency response users may enter into voluntary negotiated agreements with non-federal users whereby such federal users agree to withdraw from assigned spectrum prior to the delayed effective date of reallocation established pursuant to the NTIAOA, if such non-federal users agree to reimburse, through the payment of money or in-kind costs, or a combination of money and in-kind costs, to the federal users to defray the expenses of relocating to other frequencies. No federal law enforcement or emergency response user shall be required to enter into such negotiations. If a federal law enforcement or emergency response user does commence such negotiations, it shall not be required to complete such negotiations unless the negotiated terms are satisfactory to such federal user. A non-federal user shall not receive a preference in the spectrum assignment process due to willingness to pay such costs. Notwithstanding 31 U.S.C. Section 3302(b), federal law enforcement and emergency response users may accept and retain these payments, may credit receipt of such payments to the receiving agency's accounts, and may expend such deposits without further appropriation or fiscal year limitation.

(4) A federal law enforcement or emergency response user that is assigned frequencies in a frequency band that is also used by a non-federal user pursuant to paragraph (b)(2) of Section 113 of the NTIAOA may accept and retain payment by a non-federal entity of money or in-kind costs, or a combination of money and in-kind costs, for the federal user to prevent harmful interference to or from non-federal users. A non-federal user shall not receive a preference in the spectrum assignment process due to a willingness to pay for such costs. Notwithstanding 31 U.S.C. Section 3302(b), federal law enforcement and emergency response users may accept and retain these payments, may credit receipt of such payments to the receiving agency's accounts, and may expend such deposits without further appropriation or fiscal year limitation.

(d) PROTECTION OF INCUMBENT STATE AND LOCAL LAW ENFORCEMENT AND PUBLIC SAFETY USERS

(1) IN GENERAL - To the extent possible, the Commission shall give priority consideration in all frequency spectrum allocation matters to the needs of state and local law enforcement and public safety agencies and, except in extraordinary circumstances, shall not reallocate portions of the frequency spectrum in which state and local law enforcement or public safety agencies are primary users.

(2) SPECIFICALLY - In the event that the Commission authorizes non-governmental spectrum users in bands that include spectrum licenses on a primary basis to state or local government users, the non-governmental spectrum users shall be required: (i) to restrict their use so as not to cause harmful interference to such state or local government users, (ii) to compensate such state or local government users for the total cost of using other frequencies, including, but not limited to, the cost of replacing facilities, of conducting engineering and cost analyses of relocated facilities, of moving their systems to other spectrum or transmission technologies agreeable to the affected incumbent, or (iii) to take other measures pursuant to the mutual agreement of the state or local government and non-government spectrum users."

SECTION 20. IDENTIFICATION AND ALLOCATION OF COMMON SPECTRUM FOR FUTURE LAW ENFORCEMENT AND PUBLIC SAFETY USE.

"The Secretary of Commerce and the Chairman of the Federal Communications Commission, after consultation with the Attorney General and the Secretary of the Treasury, shall, within 18 months after the date of enactment, jointly prepare and submit to the President and the Congress, a report identifying the spectrum requirements: (i) for future use for federal, state, and local law enforcement and public safety agencies, including the requirements anticipated as a result of new communications and law enforcement technologies, and (ii) for development of a nationwide law enforcement and public safety wireless network."

SECTION 30. NATIONAL LAW ENFORCEMENT AND PUBLIC SAFETY WIRELESS NETWORK FUND.

"(a) IN GENERAL - There is hereby established in the United States Treasury a fund to be known as the National Law Enforcement and Public Safety Wireless Network Fund (hereafter referred to as "the Fund"), which shall be available without further appropriations or fiscal year limitation to the Attorney General and the Secretary of the Treasury for:

(1) the costs of planning, designing, developing, and implementing a nationwide interoperable wireless network for federal, state, and local law enforcement and public safety agencies; and

(2) the costs of federal law enforcement entities relocating their operations from frequencies reallocated to the

Federal Communications Commission, and not otherwise compensated, including frequency spectrum previously reallocated under Section 113 of the NTIAOA (47 U.S.C. Section 923).

(b) DEPOSITS TO THE FUND - There shall be credited and deposited to the Fund proceeds from the competitive bidding and/or auction of spectrum in excess of the estimated amounts, but not to exceed \$500,000,000 in any single fiscal year, beginning with fiscal year 1996.

(c) REPORTING REQUIREMENTS

(1) The use of funds credited and deposited to the Fund shall only be made after joint annual notification by the Attorney General and the Secretary of the Treasury to the Committees on Appropriation of the House of Representatives and the Senate.

(2) The Attorney General and the Secretary of the Treasury shall provide a joint annual report to the President and the Congress no later than March 31, 1997, and annually thereafter, delineating expenditures from the Fund during the previous fiscal year and the status and progress of the implementation of the nationwide interoperable wireless network for federal, state, and local law enforcement and public safety agencies.

(d) SUNSET PROVISION - The authority to credit and deposit to the Fund proceeds from the competitive bidding and/or auction of spectrum shall expire December 31, 2004, or upon joint determination and notice to the President by the Attorney General and the Secretary of the Treasury, whichever comes first."

jurisdictions, such as the recent bombing of the Murrah Federal Office Building in Oklahoma City, Oklahoma, the World Trade Center bombing in New York City, natural disasters and emergencies, and joint law enforcement operations and task forces.

(6) Additional frequency spectrum allocations are needed by law enforcement and public safety agencies to implement new telecommunications technologies and functionalities. For example, frequency spectrum availability is critical to implement features of the NCIC 2000 system which will provide police officers with the ability to send and receive, from patrol cars and other mobile units, digitized fingerprint images and photographs that will aid in the identification of fugitives, violent criminals, and missing persons. Absent frequency spectrum to support wideband communications, law enforcement agencies may not be able to take advantage of these new functionalities and capabilities, thus placing officer safety and communities at risk.

(7) The concept of a nationwide interoperable law enforcement and public safety wireless network has been suggested by the President's National Performance Review (NPR). The Attorney General and the Secretary of the Treasury have assumed leadership roles in establishing a nationwide interoperable wireless communication network for all federal, state, and local law enforcement and public safety agencies through the establishment of the Federal Law Enforcement Wireless Users Group (FLEWUG).

(8) The design and development effort for the NPR initiative is projected to cost \$75,000,000 over a five or more year period. This effort would be focused upon such activities as spectrum requirements studies, assessment of digital wireless communications technology, systems engineering, and pilot programs. Once standards are developed and a national interoperable wireless network defined, individual law enforcement and public safety agencies would begin migrating to the network."

SECTION 10. PRIORITY CONSIDERATION FOR REASSIGNMENT OF TRANSFERRED FREQUENCY SPECTRUM.

"(a) The Commission shall give priority consideration to the frequency spectrum needs of state and local law enforcement and public safety agencies when reallocating frequency spectrum between the 1710 - 1755 MHz bandwidth which was transferred from federal law enforcement agencies under the authority of the National Telecommunications and Information Administration Organization Act (47 U.S.C. Section 923) (hereafter referred to as "the NTIAOA").

(b) Frequency spectrum transferred from federal law enforcement agencies under the authority of the NTIAOA and not

assigned by the Commission to state and local law enforcement and public safety agencies within 24 months after enactment, shall be available for competitive bidding and/or reallocation by the Commission. The proceeds from the competitive bidding of frequency spectrum between 1710 and 1755 MHz shall be deposited into the National Law Enforcement and Public Safety Wireless Network Fund created under Section 30 without regard to the fiscal year limitation on deposits."

SECTION 20. PROTECTION OF INCUMBENT SPECTRUM USERS.

"(a) IN GENERAL - Reallocation of federal spectrum to the Commission shall not disrupt federal law enforcement and public safety communications services and activities, and shall minimize the economic effects to federal users and, thereby, the taxpayer, and shall foster the introduction of new radio-based services and devices.

(b) CONSULTATION WITH THE COMMISSION, THE ATTORNEY GENERAL, AND THE SECRETARIES OF DEFENSE AND THE TREASURY

(1) IN GENERAL - The Secretary of Commerce shall, in the course of identifying and recommending for future reallocation bands of frequencies, consult with the Attorney General, the Secretary of the Treasury, the Secretary of Defense, and the Commission to ensure that law enforcement, public safety, and national security interests and capabilities are not adversely affected by the proposed transfer of frequencies.

(2) SPECIFICALLY - The Secretary of Commerce, in consultation with the Attorney General, the Secretary of the Treasury, and the Secretary of Defense, shall prepare and include in reports submitted to the President and the Congress that identify future transfers of frequency spectrum from federal to non-federal users, a statement identifying the operational and cost impact of the proposed transfer of frequency spectrum upon the current and future operations of affected federal law enforcement, public safety, and national security users.

(c) PROTECTION OF FEDERAL LAW ENFORCEMENT AND EMERGENCY RESPONSE USERS IN SPECTRUM TO BE REALLOCATED.

(1) Notwithstanding any other provision of law, the Secretary of Commerce is prohibited from transferring to the Commission for purposes of auction or reallocation to non-law enforcement or public safety users frequency spectrum assigned to federal law enforcement and emergency response users until the report required under Section 20 has been submitted to the President and the Congress.

(2) In the event that non-federal users seek to use bands that include frequency spectrum licensed on a primary basis to federal law enforcement and emergency response users, the non-federal users will be required: (i) to restrict their use

so as not to cause harmful interference to such federal users, (ii) to compensate such federal users for the total cost of using other frequencies, including, but not limited to, the cost of replacing existing facilities, of conducting engineering and cost analyses of relocated facilities, of moving systems to other frequency spectrum or transmission technologies agreeable to the affected incumbent, or (iii) to take other measures pursuant to the mutual agreement of the government and non-government spectrum users. Federal law enforcement and emergency response users may negotiate with non-federal users for the purpose of agreeing to terms under which the federal entity would relocate to other bands of frequency spectrum or other media, or alternatively, may negotiate sharing agreements with non-federal users that allow acceptable levels of interference to the existing federal user.

(3) Federal law enforcement and emergency response users may enter into voluntary negotiated agreements with non-federal users whereby such federal users agree to withdraw from assigned spectrum prior to the delayed effective date of reallocation established pursuant to the NTIAOA, if such non-federal users agree to reimburse, through the payment of money or in-kind costs, or a combination of money and in-kind costs, to the federal users to defray the expenses of relocating to other frequencies. No federal law enforcement or emergency response user shall be required to enter into such negotiations. If a federal law enforcement or emergency response user does commence such negotiations, it shall not be required to complete such negotiations unless the negotiated terms are satisfactory to such federal user. A non-federal user shall not receive a preference in the spectrum assignment process due to willingness to pay such costs. Notwithstanding 31 U.S.C. Section 3302(b), federal law enforcement and emergency response users may accept and retain these payments, may credit receipt of such payments to the receiving agency's accounts, and may expend such deposits without further appropriation or fiscal year limitation.

(4) A federal law enforcement or emergency response user that is assigned frequencies in a frequency band that is also used by a non-federal user pursuant to paragraph (b)(2) of Section 113 of the NTIAOA may accept and retain payment by a non-federal entity of money or in-kind costs, or a combination of money and in-kind costs, for the federal user to prevent harmful interference to or from non-federal users. A non-federal user shall not receive a preference in the spectrum assignment process due to a willingness to pay for such costs. Notwithstanding 31 U.S.C. Section 3302(b), federal law enforcement and emergency response users may accept and retain these payments, may credit receipt of such payments to the receiving agency's accounts, and may expend such deposits without further appropriation or fiscal year limitation.

(d) PROTECTION OF INCUMBENT STATE AND LOCAL LAW ENFORCEMENT AND PUBLIC SAFETY USERS

(1) IN GENERAL - To the extent possible, the Commission shall give priority consideration in all frequency spectrum allocation matters to the needs of state and local law enforcement and public safety agencies and, except in extraordinary circumstances, shall not reallocate portions of the frequency spectrum in which state and local law enforcement or public safety agencies are primary users.

(2) SPECIFICALLY - In the event that the Commission authorizes non-governmental spectrum users in bands that include spectrum licenses on a primary basis to state or local government users, the non-governmental spectrum users shall be required: (i) to restrict their use so as not to cause harmful interference to such state or local government users, (ii) to compensate such state or local government users for the total cost of using other frequencies, including, but not limited to, the cost of replacing facilities, of conducting engineering and cost analyses of relocated facilities, of moving their systems to other spectrum or transmission technologies agreeable to the affected incumbent, or (iii) to take other measures pursuant to the mutual agreement of the state or local government and non-government spectrum users."

SECTION 20. IDENTIFICATION AND ALLOCATION OF COMMON SPECTRUM FOR FUTURE LAW ENFORCEMENT AND PUBLIC SAFETY USE.

"The Secretary of Commerce and the Chairman of the Federal Communications Commission, after consultation with the Attorney General and the Secretary of the Treasury, shall, within 18 months after the date of enactment, jointly prepare and submit to the President and the Congress, a report identifying the spectrum requirements: (i) for future use for federal, state, and local law enforcement and public safety agencies, including the requirements anticipated as a result of new communications and law enforcement technologies, and (ii) for development of a nationwide law enforcement and public safety wireless network."

SECTION 30. NATIONAL LAW ENFORCEMENT AND PUBLIC SAFETY WIRELESS NETWORK FUND.

"(a) IN GENERAL - There is hereby established in the United States Treasury a fund to be known as the National Law Enforcement and Public Safety Wireless Network Fund (hereafter referred to as "the Fund"), which shall be available without further appropriations or fiscal year limitation to the Attorney General and the Secretary of the Treasury for:

(1) the costs of planning, designing, developing, and implementing a nationwide interoperable wireless network for federal, state, and local law enforcement and public safety agencies; and

(2) the costs of federal law enforcement entities relocating their operations from frequencies reallocated to the

Federal Communications Commission, and not otherwise compensated, including frequency spectrum previously reallocated under Section 113 of the NTIAOA (47 U.S.C. Section 923).

(b) DEPOSITS TO THE FUND - There shall be credited and deposited to the Fund proceeds from the competitive bidding and/or auction of spectrum in excess of the estimated amounts, but not to exceed \$500,000,000 in any single fiscal year, beginning with fiscal year 1996.

(c) REPORTING REQUIREMENTS

(1) The use of funds credited and deposited to the Fund shall only be made after joint annual notification by the Attorney General and the Secretary of the Treasury to the Committees on Appropriation of the House of Representatives and the Senate.

(2) The Attorney General and the Secretary of the Treasury shall provide a joint annual report to the President and the Congress no later than March 31, 1997, and annually thereafter, delineating expenditures from the Fund during the previous fiscal year and the status and progress of the implementation of the nationwide interoperable wireless network for federal, state, and local law enforcement and public safety agencies.

(d) SUNSET PROVISION - The authority to credit and deposit to the Fund proceeds from the competitive bidding and/or auction of spectrum shall expire December 31, 2004, or upon joint determination and notice to the President by the Attorney General and the Secretary of the Treasury, whichever comes first."



U.S. Department of Justice
Office of Legislative Affairs

Office of the
Assistant Attorney General

Washington, D.C. 20530

Rob Walsh
324-6490
FAX

Rm 180

11 AM



U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

FAX COVER SHEET

TO: Rob Walsh

FAX NO. 324-6492

FROM: DENNIS BURKE

PHONE NO. 514-5360

FAX NO. 514 0452

DATE: July 20

NO. OF PAGES: _____ (EXCLUDING COVER)

COMMENTS: Spectrum

Approved: W.B. [Signature]

Date: 3/3/95

WIRELESS COMMUNICATIONS

- o A Memorandum of Understanding signed by the Secretary of the Treasury and the Attorney General on April 20, 1994 formalized the Wireless Communications initiative.
- o This is a joint Justice and Treasury initiative to plan and coordinate the land mobile radio telecommunications network for use nationally by Federal, state, and local law enforcement and public safety agencies. From the National Performance Review, IT04, is a recommendation to plan for the National Law Enforcement/Public Safety Wireless Network. This initiative:
 - o Formalizes the Federal Law Enforcement Wireless Users Group to develop an implementation plan for the Wireless Network.
 - o Will provide interoperability between Federal, state and local law enforcement and public safety organizations.
 - o Addresses such issues as radio spectrum efficiencies, support for technical standards, system and information security, competitive market, and multi-media communications capabilities.
 - o Supports the national security and emergency planning missions of the Federal law enforcement and public safety communities.
- o The estimated cost for this initiative is \$75 million funded over the first five years. Funding will be used over ten years to plan the implementation of a national network. Justice's portion would be \$37.5 million. Agencies will use their base funds to transition to the new digital narrowband technology mandated by the National Telecommunications and Information Administration (NTIA). This program will provide guidance and support in identifying applications and system development approaches which avoid redundant and inefficient use of resources during the transition period and in development of the national network.
- o Funding requested in the 1996 Violent Crimes Reduction Trust Fund (VCRTF) will be used to establish a Program Management Office, develop a baseline of present day wireless resources, conduct studies concerning the optimum radio spectrum for law enforcement use in various environments, and perform pilot tests of digital equipment which includes deployment and analysis of wireless equipment at a number of selected locations.
- o The equipment currently in place will grow obsolete. The ability to fight the war on crime is dependent on this initiative to make more efficient use of resources and technology in implementing new systems.
- o If \$2.5 million in VCRTF funding is received, the FBI's Wireless Communications 1996 base would consist of four support positions and \$451,000 in personnel funding and \$2,049,000 in nonpersonnel funding.

Approved: *WBL/JS*

Date: *3/3/95*

RADIO SPECTRUM ALLOCATION/AUCTION

- o Title VI - Communications Licensing and Spectrum Allocation
Improvement of the Omnibus Budget Reconciliation Act of 1993 required the Federal government to provide at least 200 MegaHertz (MHz) of Federal spectrum to the private sector for emerging technologies. The final report identifying the transferred spectrum will be sent to Congress in March 1995. Some of this spectrum will be auctioned.
- o Department of Justice operations affected by the spectrum transfer are fixed microwave links and video surveillance operations. All operations are required to vacate the 1710-1755 MHz band by January 1, 2004. Existing microwave links will be converted to leased telephone lines, where feasible, and to different frequency bands. Existing video equipment will be retuned to new frequencies and new equipment will be purchased in other, less optimum, frequency bands.
- o Additional requests for transfer of Federal spectrum to the private sector are anticipated. Frequencies used for law enforcement activities should be exempted from transfer. Law enforcement equipment is developed in specific frequency bands to provide optimum transfer of information. Transfer to new, less suitable, frequency bands would hamper investigative activities.
- o New radio spectrum is required for use by both Federal law enforcement and public safety agencies.
- o Federal law enforcement agencies have become increasingly involved in joint activities with state and local public safety agencies. Federal agencies use two frequency bands for radio communications; public safety operates in six frequency bands. No radio equipment can operate in all bands; common spectrum is needed for interoperability. This spectrum should be identified immediately so new equipment can be developed.

communications companies implement new technologies and services.

As the bill moves to conference, I will continue to do what I can to make further improvements and defend against efforts to weaken its provisions protecting consumer interests and assuring free and fair competition.

Through this legislation and this debate, we have a unique opportunity to craft a telecommunications policy framework for the next century. Today, Mr. President, each of us is in a sense a pioneer heading out on the new information highway. Each of us is not only a witness to, but a participant in, one of the most amazing technological revolutions in history. We, as legislators, bear a special responsibility to assure that competition in this new era is fair and that every American in this and future generations may enjoy the fruits of this competition. This is truly one of the greatest challenges we face as we enter the 21st century.

RADIO SPECTRUM FOR LAW ENFORCEMENT PURPOSES

Mr. HATCH. Mr. President, I share the concerns that have been expressed by others regarding the availability of radio spectrum for law enforcement purposes. I have been contacted by law enforcement organizations across the country, including those in my State of Utah, expressing these concerns.

A critical element in the effort to battle crime and to respond to emergencies of all types is the existence of reliable and secure radio communications facilities, which in turn depends on adequate spectrum availability. Yet, current allocations may well be inadequate to meet present needs. Many metropolitan police departments are unable to add new channels to alleviate congestion.

Moreover, spectrum space is also needed to bring new technologies online. Just last week, we passed a counterterrorism bill, which included important provisions to increase information sharing between law enforcement. Yet these provisions will be for naught if spectrum space is not available for the deployment of these technologies.

I appreciate the commitment expressed by the managers of this bill to address this issue. I know that the Senator from South Dakota, the Distinguished Chairman of the Commerce Committee, shares my concerns. As a former member of the Judiciary Committee, he understands the needs of law enforcement. I understand that he is committed to attempting to resolve these concerns as this legislation moves forward. I look forward to working with him and the Senator from South Carolina on this vital issue as the legislation moves through conference.

Mr. BIDEN. I am very concerned that Federal, State, and local law enforcement have adequate spectrum availability, and would like to work with the chairman of the Judiciary Committee and the managers of this bill to en-

sure that this vital issue is addressed in the conference on this legislation.

The reason this is so important is twofold. First, in this era where Federal, State, and local law enforcement often work together we need to maintain spectrum space so that these, and other public service agencies, can communicate with ease and with the most advanced technology available. If we develop better technology to allow the police to talk to each other without the bad guys listening in, we must have the spectrum available to use this technology.

Second, we must work to ensure sufficient spectrum space for the myriad technological advances being made in the area of secured communications. I have heard several of the law enforcement leaders in my home State of Delaware raise these key points. So, I believe this is a practical problem that we face in Delaware and around the Nation.

We do a disservice to law enforcement and to the American people if we do not provide these public servants with the many benefits of our rapidly advancing telecommunications industry. I look forward to working with my friend from Utah on this important effort.

Mr. HATCH. I thank my friend and colleague from Delaware for his support on this issue. As the former chairman of the Judiciary Committee, his strong support of law enforcement is wellknown, and I look forward to working with him in this.

Mr. BIDEN. I want to acknowledge and thank my colleagues for their efforts on this issue. In particular, Senator HATCH and the managers of this important legislation, Senator PRESSLER and Senator HOLLINGS not only for their support of this effort, but also their support of law enforcement.

Mr. PRESSLER. I do share my colleagues' concerns, and appreciate the interest of the chairman and ranking member of the Judiciary Committee in this issue. I look forward to working with them on it.

Mr. HOLLINGS. I, too, understand these concerns and look forward to addressing them.

—CABLE ISSUES

Mr. PRESSLER. Mr. President, I would like to engage my colleague from South Carolina in a colloquy on several cable issues. First, it is my understanding that neither section 204(a) of the bill nor the relevant provisions in the Dole-Daschle-Hollings amendment is intended to prevent the FCC and cable operators from entering into "social contracts" or other similar arrangements to settle rate complaints, under which the operator agrees to offer a low priced basic tier to offset an increase in the rate for cable programming services.

Mr. HOLLINGS. The Senator from South Dakota is correct.

Mr. PRESSLER. I thank the Senator. Second, it is my understanding that the reference to comparable video pro-

gramming, added by the Dole-Daschle-Hollings amendment to new section 623(l)(1)(D) of the Communications Act, has the same meaning as it does elsewhere in section 632(l)(1) of the Communications Act and the FCC's regulations defining comparable.

Mr. HOLLINGS. The Senator's understanding is correct.

Mr. PRESSLER. Finally, I call the Senator's attention to the managers' amendment to S. 652. As amended by the managers' amendment, new section 613(b)(2)(B) of the Communications Act clarifies that a Bell operating company providing cable service as a cable operator utilizing its own telephone exchange facilities is not required to establish a video platform. However, a Bell operating company that provides cable service as a cable operator, whether through its own telephone exchange facilities or otherwise, would be subject to the PEG and commercial leased access requirements of the Communications Act—sections 611 and 612—applicable to all cable operators.

Mr. HOLLINGS. The Senator accurately states the intent of the bill as amended by the managers' amendment.

Mr. PRESSLER. I thank the Senator from South Carolina.

POLE ATTACHMENT

Mr. MURKOWSKI. Mr. President, I have reviewed the provisions of S. 652, as reported, that seek to amend section 224 of the Pole Attachment Act of 1978. As a result of that review, I am deeply concerned that these provisions would have a significantly adverse impact on electric utility ratepayers throughout the Nation. I am particularly concerned that these provisions would require electric ratepayers to shoulder the burden of subsidizing not only cable operators but also telephone companies and telecommunications providers. The amount of money foregone by the bill as reported is not trivial. It amounts to tens of millions of dollars annually, if not hundreds of millions of dollars. Put simply, it is not fair to ask consumers of electricity to subsidize cable operators and telephone companies. In this connection, it is important to point out that this subsidy does not even necessarily go the customers of these companies.

From a consumer protection standpoint, I believe the legislation should be amended to ensure that all entities that attach to poles are required to pay a fair and proportionate rate that provides for recovery of the cost of installing and maintaining the entire pole, including the common space. I ask the chairman of the Committee, Senator PRESSLER, and the ranking minority member, Senator HOLLINGS, whether they have any concerns on this matter and what their plans are to remedy the situation.

Mr. PRESSLER. I agree with the Senator from Alaska [Mr. MURKOWSKI], that this is a real concern that needs to be addressed. I believe that many of these concerns are being addressed in the Manager's amendment, but to the

communications companies implement new technologies and services.

As the bill moves to conference, I will continue to do what I can to make further improvements and defend against efforts to weaken its provisions protecting consumer interests and assuring free and fair competition.

Through this legislation and this debate, we have a unique opportunity to craft a telecommunications policy framework for the next century. Today, Mr. President, each of us is in a sense a pioneer heading out on the new information highway. Each of us is not only a witness to, but a participant in, one of the most amazing technological revolutions in history. We, as legislators, bear a special responsibility to assure that competition in this new era is fair and that every American in this and future generations may enjoy the fruits of this competition. This is truly one of the greatest challenges we face as we enter the 21st century.

RADIO SPECTRUM FOR LAW ENFORCEMENT PURPOSES

Mr. HATCH. Mr. President, I share the concerns that have been expressed by others regarding the availability of radio spectrum for law enforcement purposes. I have been contacted by law enforcement organizations across the country, including those in my State of Utah, expressing these concerns.

A critical element in the effort to battle crime and to respond to emergencies of all types is the existence of reliable and secure radio communications facilities, which in turn depends on adequate spectrum availability. Yet, current allocations may well be inadequate to meet present needs. Many metropolitan police departments are unable to add new channels to alleviate congestion.

Moreover, spectrum space is also needed to bring new technologies online. Just last week, we passed a counterterrorism bill, which included important provisions to increase information sharing between law enforcement. Yet these provisions will be for naught if spectrum space is not available for the deployment of these technologies.

I appreciate the commitment expressed by the managers of this bill to address this issue. I know that the Senator from South Dakota, the Distinguished Chairman of the Commerce Committee, shares my concerns. As a former member of the Judiciary Committee, he understands the needs of law enforcement. I understand that he is committed to attempting to resolve these concerns as this legislation moves forward. I look forward to working with him and the Senator from South Carolina on this vital issue as the legislation moves through conference.

Mr. BIDEN. I am very concerned that Federal, State, and local law enforcement have adequate spectrum availability, and would like to work with the chairman of the Judiciary Committee and the managers of this bill to en-

sure that this vital issue is addressed in the conference on this legislation.

The reason this is so important is twofold. First, in this era where Federal, State, and local law enforcement often work together we need to maintain spectrum space so that these, and other public service agencies, can communicate with ease and with the most advanced technology available. If we develop better technology to allow the police to talk to each other without the bad guys listening in, we must have the spectrum available to use this technology.

Second, we must work to ensure sufficient spectrum space for the myriad technological advances being made in the area of secured communications. I have heard several of the law enforcement leaders in my home State of Delaware raise these key points. So, I believe this is a practical problem that we face in Delaware and around the Nation.

We do a disservice to law enforcement and to the American people if we do not provide these public servants with the many benefits of our rapidly advancing telecommunications industry. I look forward to working with my friend from Utah on this important effort.

Mr. HATCH. I thank my friend and colleague from Delaware for his support on this issue. As the former chairman of the Judiciary Committee, his strong support of law enforcement is wellknown, and I look forward to working with him in this.

Mr. BIDEN. I want to acknowledge and thank my colleagues for their efforts on this issue. In particular, Senator HATCH and the managers of this important legislation, Senator PRESSLER and Senator HOLLINGS not only for their support of this effort, but also their support of law enforcement.

Mr. PRESSLER. I do share my colleagues' concerns, and appreciate the interest of the chairman and ranking member of the Judiciary Committee in this issue. I look forward to working with them on it.

Mr. HOLLINGS. I, too, understand these concerns and look forward to addressing them.

CABLE ISSUES

Mr. PRESSLER. Mr. President, I would like to engage my colleague from South Carolina in a colloquy on several cable issues. First, it is my understanding that neither section 204(a) of the bill nor the relevant provisions in the Dole-Daschle-Hollings amendment is intended to prevent the FCC and cable operators from entering into "social contracts" or other similar arrangements to settle rate complaints, under which the operator agrees to offer a low priced basic tier to offset an increase in the rate for cable programming services.

Mr. HOLLINGS. The Senator from South Dakota is correct.

Mr. PRESSLER. I thank the Senator. Second, it is my understanding that the reference to comparable video pro-

gramming, added by the Dole-Daschle-Hollings amendment to new section 623(l)(1)(D) of the Communications Act, has the same meaning as it does elsewhere in section 632(l)(1) of the Communications Act and the FCC's regulations defining comparable.

Mr. HOLLINGS. The Senator's understanding is correct.

Mr. PRESSLER. Finally, I call the Senator's attention to the managers' amendment to S. 652. As amended by the managers' amendment, new section 613(b)(2)(B) of the Communications Act clarifies that a Bell operating company providing cable service as a cable operator utilizing its own telephone exchange facilities is not required to establish a video platform. However, a Bell operating company that provides cable service as a cable operator, whether through its own telephone exchange facilities or otherwise, would be subject to the PEG and commercial leased access requirements of the Communications Act—sections 611 and 612—applicable to all cable operators.

Mr. HOLLINGS. The Senator accurately states the intent of the bill as amended by the managers' amendment.

Mr. PRESSLER. I thank the Senator from South Carolina.

POLE ATTACHMENT

Mr. MURKOWSKI. Mr. President, I have reviewed the provisions of S. 652, as reported, that seek to amend section 224 of the Pole Attachment Act of 1978. As a result of that review, I am deeply concerned that these provisions would have a significantly adverse impact on electric utility ratepayers throughout the Nation. I am particularly concerned that these provisions would require electric ratepayers to shoulder the burden of subsidizing not only cable operators but also telephone companies and telecommunications providers. The amount of money foregone by the bill as reported is not trivial. It amounts to tens of millions of dollars annually, if not hundreds of millions of dollars. Put simply, it is not fair to ask consumers of electricity to subsidize cable operators and telephone companies. In this connection, it is important to point out that this subsidy does not even necessarily go the customers of these companies.

From a consumer protection standpoint, I believe the legislation should be amended to ensure that all entities that attach to poles are required to pay a fair and proportionate rate that provides for recovery of the cost of installing and maintaining the entire pole, including the common space. I ask the chairman of the Committee, Senator PRESSLER, and the ranking minority member, Senator HOLLINGS, whether they have any concerns on this matter and what their plans are to remedy the situation.

Mr. PRESSLER. I agree with the Senator from Alaska [Mr. MURKOWSKI], that this is a real concern that needs to be addressed. I believe that many of these concerns are being addressed in the Manager's amendment, but to the

JOHN W. WARREN, VIRGINIA, VICE CHAIRMAN
 HOWARD H. METZENBACH, OHIO
 JOHN GLENN, OHIO
 J. ROBERT F. NIENABER, NEBRASKA
 EDWARD H. BYRNE, NEVADA
 BOB GRAHAM, FLORIDA
 JOHN F. EITNER, MASSACHUSETTS
 MAX BAUCUS, MONTANA
 J. BENNETT JOHNSTON, LOUISIANA
 ALFONSO D'AMATO, NEW YORK
 JOHN C. DANFORTH, MISSOURI
 BLAKE GORTON, WASHINGTON
 JOHN H. CHAFFE, RHODE ISLAND
 TED STEVENS, ALASKA
 RICHARD G. LUGAR, INDIANA
 MALCOLM WALLOP, VIRGINIA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

GEORGE J. MITCHELL, MAINE, EX OFFICIO
 ROBERT DOLE, KANSAS, EX OFFICIO

NORMAN R. KRAVETZ, STAFF DIRECTOR
 JUDITH A. ANSLEY, MINORITY STAFF DIRECTOR
 KATHLEEN P. McQUEE, CHIEF CLERK

F A C S I M I L E T R A N S M I T T A L

DATE: _____

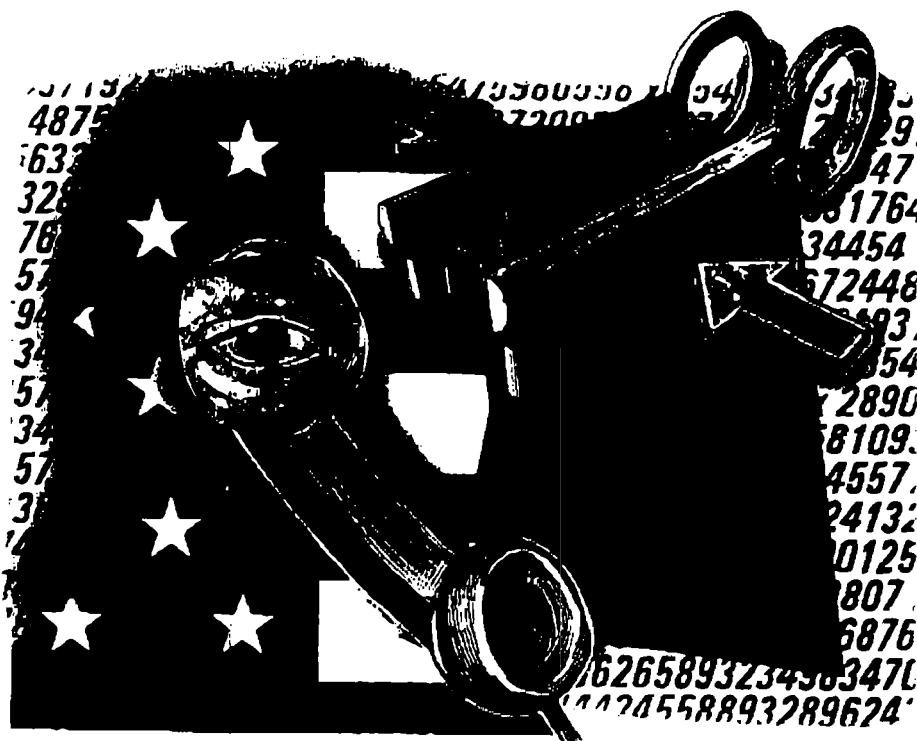
TIME: _____

PLEASE DELIVER THE FOLLOWING MESSAGE:

TO: DENNIS BURKE
 FROM: TIM CARLISBARD

TOTAL PAGES: 5 (including this page)

PLEASE CONTACT SENDER AT (202) 224-1700 IF FAX IS INCOMPLETE.



Open Secrets

Why the so-called Clipper chip—vilified as a threat to the privacy of electronic communications—is not worth losing sleep over

THE political problem the Clinton Administration least expected was a war with America's high-tech community. Between Al Gore's patronage of the "information superhighway" and the Administration's various policies favoring the computer and semiconductor industries, Bill Clinton might have imagined that the Americans who build, buy, and use computers would be among his biggest fans.

Instead, since late last year electronic forums, which are the talk shows of the computer world, have rung with bitter denunciations of Clinton and Gore for having "betrayed" and "sold out" their high-tech constituency. The complaints have to do with two related proposals affecting privacy in the electronic age: for the use of a new encryption device called the Clipper chip, and for updating the law concerning wiretaps, through the Digital Telephony bill.

The subject of these proposals are highly technical, yet the debate about them has become as intense and polarized as those over school prayer and gun control. In one month this spring some 50,000 computer users endorsed a petition circulated on the Internet which denounced the Clipper chip plan. "If this Clipper monster isn't stopped soon, we are going to witness the criminalization of anyone who insists on complete privacy of personal communications on computer networks," one wholly typical Internet message said. "Beating Clipper is a crucial step in freeing ourselves from all the dark possibilities of an authoritarian national security state."

When I first heard about these plans, I was ready to go on the warpath alongside my fellow on-line habitues. But the more I have learned about the proposals, the less wrought up I have become. The Clipper narrative, which has been the bet-

ter publicized of the two plans, seems to me to be foolish and misguided—but also quite easily thwarted by those who most oppose it. The Digital Telephony proposal, in comparison, seems more reasonable and balanced. Looked at closely, neither is the watershed in the history of American freedoms that the electronic community has made it out to be.

BEFORE going into the ugly to-and-fro over the Clipper proposal, let's consider the beautiful mathematical discoveries that have given rise to the whole debate.

The Clipper controversy concerns cryptography—putting messages into code. Codes have been around for about as long as people have been communicating, but until 1976 all codes shared one great flaw. Each relied on a secret "key," or coding method, with which the "plaintext" of the message could be encoded into "ciphertext" and then decoded into plaintext at the other end. The person sending the message had to agree beforehand with the person receiving it on what the key would be—references to pages in a book, a system of letter transposition, or one of countless other possibilities. The need for two or more people to agree ahead of time on a key created problems that have been the stuff of spy novels and war histories for hundreds of years: lost keys, stolen keys, counterfeit keys, keys that arrived after the message itself.

In 1976 Whitfield Diffie and Martin Hellman, both then at Stanford, wrote a paper proposing the radically different concept of a "public key" coding system, in which sender and receiver need never discuss a secret key. In 1978 Ronald Rivest, Adi Shamir, and Leonard Adleman, then all at the Massachusetts Institute of Technology, published a paper showing for the first time (at least in unclassified literature) exactly how a public-key system might work. This paper, which formulated what has come to be known as the RSA system, and the Diffie and Hellman paper before it are routinely referred to as being the "most innovative" or "most profound" steps in modern cryptography, because they eliminated the vulnerability that had afflicted all previous codes.

The basic mathematical idea behind public-key systems is that of the "one-way function." One-way functions are those that are much easier to perform in one direction than the other. Most people can quickly figure out, with a calculator or just a pencil, what 7^6 , or $7 \times 7 \times 7 \times 7 \times 7 \times 7$, equals. Very few people can quickly figure out what the sixth root of 117,649 is. (It's 7.)

The same principle applies even to powerful computers, with allowances for their far greater speed. They can add, subtract, and multiply numbers much more quickly than they can calculate a number's factors. The simplest calculator can determine almost instantaneously that $987 \times 1,013 = 999,831$. But if a computer starts with the number 999,831, it will take time for the machine to determine, through trial and error, that the number can be evenly divided by 987 and 1,013.

As numbers become larger, this period of time becomes significant. When numbers become very large, the slow part of a one-way function becomes so slow that completing it is virtually impossible. For example: if two prime numbers, each 100 digits long, are multiplied together, the result will be a number about 200 digits long. A computer can easily calculate that enormous product. But if it starts with the same 200-digit number and tries to find what those 100-digit factors are, the process will be much slower. (As a reminder: a prime number has only two factors, 1 and the number itself. Therefore a 200-digit number that is the product of two prime numbers will have only four factors: 1, the number itself, and the two prime numbers.) Finding the factors of such a 200-digit number on a modern top-speed supercomputer would require not milliseconds or minutes but at least several centuries. The task is, in computer terms, "computationally infeasible."

What Diffie, Hellman, and the three MIT authors proposed was that numbers hidden by computational infeasibility could serve as a kind of secret key in a variety of ways. The key is not really secret, of course, since with infinite time an outsider could calculate what the hidden numbers were. But no outsider would live long enough to see the results, so in practical terms the code is secure. In the RSA system, for example, messages can be decoded by anyone who knows the

two secret 100-digit prime numbers that were multiplied together to produce each recipient's 200-digit public key. (In the RSA system, to simplify slightly, each person chooses his own secret prime number, multiplies them together, and reveals the product as his "public key." Anyone wanting to send a message to that person applies this public key in an encryption formula. The original prime numbers are then used in a decryption formula to produce the original message.) Only the intended recipient knows the original prime numbers; no one else can figure them out from the public key.

For the world's cryptographers, the public-key concept was exhilarating. For the world's governments, its implications were more complicated. Public-key cryptography raised for the first time the prospect that completely secure communications systems might be available to almost anyone—including parties whose conversations a government would like to overhear. Various U.S. government agencies have long been confident of their ability to break a code if they really need to. Now officials became concerned that as public-key coding programs became cheap and widely available, the government would lose its ability to hear what other governments, and in certain cases its own citizens, were saying.

Two branches of the U.S. government were most immediately concerned: the Federal Bureau of Investigation, which has relied on wiretaps for domestic law enforcement, and feared that criminals would start scrambling all transmissions; and the National Security Agency, which exists in part for the purpose of intercepting telephone and broadcast transmissions around the world. (By law the NSA, like the Central Intelligence Agency, is not supposed to intercept data within the United States. Because the NSA's operations are more secret than those of any other major government agency, there is no way to be sure that it has followed this rule.)

The NSA, which arguably controls the greatest concentration of computing power in America, was the main bureaucratic force behind the Clipper chip. It feared that sooner or later public-key coding systems would become cheap and commercially available, so that citizens and businesses would routinely use them to scramble their telephone calls and data

transmissions. This in turn would make it nearly impossible for the government to decode messages it intercepted; not even the NSA's computers could break the public keys. To forestall this possibility, the NSA, with the eventual support of the FBI, threw its weight behind the Clipper proposal—for a government-approved encryption system that might prevent the spread of public-key codes. Early last year the Clinton Administration embraced this plan.

The Clipper chip, officially known as the MYK-78 device, is programmed by Mykotronx Inc., of California. Telephones and modems that meet the Clipper standard come with this chip built in. Clipper phones scramble messages not according to public-key systems but through a secret coding algorithm called Skipjack. Skipjack would work with several "keys," including unique numbers built into the chip supplied with each telephone, to produce what the government claims is virtually unbreakable code.

The classified nature of the Clipper-Skipjack coding system is one big cause of complaint in the high-tech world, which teems with people who believe that they can find the secret flaw in the code any big bureaucracy creates. But the real outrage about Clipper stems from another feature: its "key escrow" plan.

Unlike scrambled messages produced by public-key systems, which for all practical purposes are impossible for anyone except the recipient to understand, the scrambled messages produced by Clipper phones are vulnerable to anyone who somehow obtains their codes, including the ID number built into each phone. Under the Clipper plan the federal government will maintain a master list of ID numbers for all Clipper devices ever sold. Each number—which is, in effect, the key to its phone's Clipper code—will be split in two, and each half will be "escrowed" by a government agency. In the right circumstances—namely, the production of a wiretapping warrant—the two halves will be reunited and the government will be able to intercept and understand everything said on that phone. As Whitfield Diffie said of the Clipper system soon after it was announced, "The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of schoolchildren. The children open the locks with the

combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key."

That the government will have long-term possession of all secret Clipper keys is the reason the NSA and the FBI favored the proposal—and also the reason that nearly all of the high-tech community lined up against it. Privacy advocates were upset enough by the idea that the government would retain the keys. Even worse was the possibility that the bureaucrats guarding the keys could be bribed to turn them over to criminals or to foreign governments, which could then listen in on all supposedly "secure" conversations. (The arrest of Aldrich Ames, the alleged mole in the CIA, came in the middle of the Clipper debate.) Companies that make computers, modems, and telephone systems have unanimously opposed the Clipper plan. They say that as technology has evolved toward international standards, it has grown complicated and costly to make two different versions of all equipment—one with Clipper, for sales in America, and one without Clipper, for export. (Customers in, say, France or China would not be eager to buy scrambling equipment to which the U.S. government permanently held the keys.)

Nonetheless, the Clipper plan required no legislation, and early this year the Administration issued the orders putting it into effect. Clipper now exists as a standard for government contracts and purchases. Most of the secure, or encrypted, communications equipment sold in this country is sold to federal agencies (the military, the intelligence services, and law-enforcement divisions). Henceforth these agencies will not buy secure systems unless they are based on the Clipper chip.

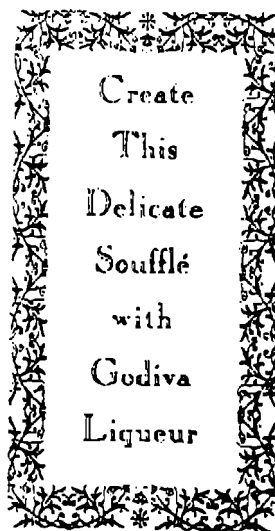
WAS this a wise decision? No. Is this the end of American civil liberties? I think not. The very trait that makes me wish the government had not adopted the Clipper standard also means that Clipper is not worth getting upset about.

This trait is the voluntary nature of the Clipper scheme. From now on, anyone who talks on a government-owned secure phone will be talking on Clipper, but no one else is obliged to use a Clipper

INNOVATIVE SPIRITS

When was the last time you tried making a soufflé? Or even ate a soufflé? Although no dessert is more elegant, a soufflé can be difficult and rich. But not this one. If you own an eggbeater or a mixer, this recipe is foolproof. And chocolate cake or real chocolate truffles are far more caloric than

these divine puffs of air, gooey with melting bits of chocolate and scented with Godiva Liqueur. The chef is Allen Sussner, a master of the new Miami cuisine, with its Southwestern, Caribbean, and Cuban touches. This can stretch to serve four, but you might want to share it with just one friend.



Godiva Liqueur Chocolate Truffle Soufflé

For 2-4:

- 4 large eggs, separated
- 1/2 cup flour
- 1/2 cup butter, softened
- 1 cup milk
- 1 teaspoon vanilla
- 1/2 cup sugar
- 1/2 cup cocoa
- 1/2 cup Godiva Liqueur
- 1/2 cup semi-sweet chocolate pieces

Using a wooden spoon, combine the flour and 1/2 cup of butter, beating until it forms a lump and comes off the sides of the bowl.

In a medium pot heat the milk with 1/2 teaspoon vanilla for five minutes, until it comes to a simmer. Mix in the flour-butter mixture and beat with a wire whisk until it dissolves and the milk begins to thicken. Continue to cook for 5 minutes, folding the mixture with a rubber

spatula until it is smooth and shiny. Remove from heat and pour into the bowl of an electric mixer. Beat at low speed, adding the egg yolks one at a time and then the sugar.

Once the mixture has cooled, mix the remaining vanilla, 1/2 cup cocoa, and the Godiva Liqueur into the soufflé base. In a separate bowl whip the egg whites only until they form soft, not stiff, peaks. Gently fold egg whites into the soufflé base in two batches.

Brush a straight-sided eight-inch baking dish that is at least four inches high with the remaining butter and dust it with sugar, knocking out the excess sugar. Ladle the soufflé base into the dish until half full. Drop in the chocolate pieces. Fill the soufflé dish to the rim with soufflé

mix. Bake in a preheated oven at 375° for 30 minutes.

Dust with cocoa powder and serve immediately.



For a free recipe brochure call 1-800-356GODIVA

phone. Nor is anyone forbidden to develop, sell, or use other encryption schemes. The three inventors of the RSA code, for example, have formed a company, RSA Data Security, that sells public key coding programs for less than \$500. Americans are as free to use them as they were before the jackboot of Clipper crashed down.

Both parties to the dispute had reasons not to emphasize the voluntary nature of Clipper. For Clipper's proponents, this was the obvious, gaping flaw in the entire scheme. The stated reason for a scrambling chip that permits wiretapping is that otherwise terrorists, drug dealers, and other criminals might use untappable scrambling schemes. With Clipper they still can.

The government at least acknowledged this objection, and tried to answer it in two ways. The first was to argue that most criminals would never hear about Clipper chips, or would forget about them when they were planning the big heist. "Thank God most criminals are stupid!" Jim Kallstrom, the FBI's special agent in charge for New York, told me in March. "If the smartest segment of the population ever went into crime, we would really have a problem. Will some criminals catch on to the system, and buy their encryption from, let's say, Israel? Yes. Will that be a problem? Yes. But it will be a substantially smaller problem than if we didn't do anything."

The government's other response has been to emphasize its ability to "make markets." If big companies are producing Clipper because that's all they use when doing business with the government, then in the long run Clipper encryption will crowd out rival schemes. Apart from the government itself, the biggest customers for coding systems today are banks and credit-card companies, which use encryption to safeguard the billions of financial transactions they handle each day. By establishing Clipper as a standard, the government hopes to keep encryption, especially public-key systems, from becoming so cheap and convenient that anyone can walk into a Radio Shack and buy a perfectly secure phone. This attempt to shut off the growth of a market enrages many of Clipper's foes—but its very indirectness illustrates the limits of Clipper's effects. It is guaranteed to be least effective against the most serious

criminal opponents, such as state-sponsored terrorist rings that will not be limited to what they can find at Radio Shack.

Yet Clipper's opponents have also downplayed the voluntary factor, because it makes adoption of the system seem less nightmarish. When pressed on this point, they have usually reverted to the "slippery slope" argument: today Clipper is voluntary; tomorrow it will be mandatory—and all other coding schemes will be outlawed. There is no peacetime precedent to suggest that Congress would pass, or the courts uphold, such a mandatory measure with sweeping controls on forms of speech. The likelihood of abuse would be reduced if Clipper's "key escrow" plan were changed in one significant way. Under current Clipper guidelines, the two agencies each designated to hold half the components of the secret keys will both be part of the executive branch. One is the Treasury Department; the other is the Commerce Department's National Institute of Standards and Technology. On familiar separation-of-power grounds, it would be safer for one of the "escrow agents" to be part of the judicial system, insulated from direct executive control. Those who are worried about Clipper no matter who its escrow agents are can and should start using some other encryption scheme.

CALMING down about Clipper might also keep the hyperbole of the battle from spilling over onto the Digital Telephony bill. Although this proposal's name sounds futuristic, the proposal itself is principally an attempt to maintain the wiretapping powers the police and the FBI have had for more than twenty-five years.

Under the Safe Streets Act of 1968 as amended in 1970, local telephone companies must cooperate with lawful wiretap requests from the FBI. Most states have passed laws based on this act, setting similar standards of their own for legal wiretaps. Law enforcement officials emphasize the many hurdles they must surmount before a judge grants such a request. The police or the FBI must show probable cause to suspect a crime, and demonstrate that all other investigative possibilities have been exhausted. Because of these requirements, fewer than 1,000 wiretap requests are granted each year.

According to the FBI, the conversion of telephone systems to digitally switched networks and the adoption of call forwarding and the like make it increasingly difficult to carry out lawful wiretap orders. Older phone systems had access points that police could use to put a tap on a single line; this was often as simple as attaching two alligator clips to a telephone wire. Newer systems lack simple mechanical access points and will become increasingly difficult to tap as time goes on. Therefore the FBI contends that for purely technical reasons, rather than for legal or political cause, the police are losing the ability to tap phones. The Digital Telephony bill would require telephone systems to build in the means for tapping on whatever new equipment they introduce.

Like any other on-line habitué, I am unenthusiastic about the whole idea of wiretaps. I realize that FBI Director Louis Freeh has himself sounded hyperbolic in making the case for the bill ("Without a new statute, law enforcement at the federal, state, and local level will be crippled," and so on). Yet I also recognize that no one could make a political or legal case that the wiretap powers granted since 1968 have been so grossly abused that they must now be revoked. These powers have, after all, been in place through the worst of the Vietnam War years, Richard Nixon's rise and fall from power, much of the Cold War, and the heyday of Oliver North, without leaving any powerful evidence that they have brought us noticeably nearer a national police state. (The opponents of the Digital Telephony bill also say that it would make too easy the collection of information about individual calling patterns, paving the way for Big Brother-style surveillance. Yet the bill would not at all relax the legal controls on how such information is collected or used.)

If the current ability of the police to tap phones is wrong, then this power should be withdrawn the normal way, by changing laws—not through the back door, as an unintended consequence of a technical change. So far the evidence suggests that the police have on the whole used the power responsibly. Therefore they deserve to retain it, under similar legal controls, through the Digital Telephony bill.

Send your complaints—in plaintext, please—to jmfallows@aol.com.

Digital Telephony Mtg. Shella
FBI

5/10/94

Leahy is aware of Biden's commitment to
introduce the bill on Monday

FBI - Bill has to be introduced next Monday
to get it going

FBI → believes they have presented the
most generic needs

left to industry how to do it

Industry will not propose anything

Chris key may be lingo dispute but might also be
substantive disagreements

Assertion been made by industry that some tech
will be impeded by this

↳ Industry could not produce 1 instant of this

~~§~~ Computers will not be covered by this bill

Nelson (OTSP) some techs exist that will not
allow FBI will not do what they want

↓ you will stifle tech

don't say "for all time here is where we are"

Industry is worried about these absolute requirements

Buckman (FBI)

↓ even George Fisher (Kodak) says that is BS
 ↓ We can talk about all the misleading issues
 in Leahy's memo attacking the bill

Nelson → Internet is e.g. ~~is~~ of where FBI
 would be very hard pressed to do what
 they want to do

Leahy memo came out yesterday

Shulka Biden is on board but thinks the bill is flawed

↳ Should we be antagonizing Leahy by taking
 him on w/ a inflexible front →
 Not good

Biden made no mention to Freeh that it is
 a flawed bill

The Friday mtg w/ industry has been moved to
 Tuesday

FBI Common carriers are the ones who have
 the most concerns about this bill

We can not surmise what ~~their~~ their problems
 are here, today w/ this crowd

Chris Schroeder (Office of Legal Counsel)

↳ Biden will not go to bat for this bill

→ The major industry players are the ~~7~~ 7 regional Bells

-
- got a bill introduced
 - make some changes now

Abschite Requirements

L, in Leahy's memo, shows they don't want this bill

FBI suggested Changes

- strike the trust Fund \$
- replace w/ general appropriation
(Biden is against this, too, & will take it out)
- add lingo on the closing provision
in Abschite Requirement Section

4

Bill has \$10,000 A DAY MAX PENALTY

MARK switch to appropriate amount under Sec 3