

1. Is there a problem?

Yes. Pursuant to an informal FBI survey conducted one year ago, 91 cases were documented where court orders for electronic surveillance or pen registers/trap and traces were frustrated, in whole or in part. These include cellular interception impediments and cellular port capacity impediments, custom calling and dialing impediments, including automatic redial and call forwarding, as well as other impediments. This survey was a "snapshot" in time of recent impediments. It did not purport to be a rigorous or exhaustive study, but it is illustrative of the breadth of the problem. The number of problems encountered is not limited to these instances. We know, for example, that in a number of localities where impediments are known to exist, law enforcement agencies simply have declined to prepare and apply for court orders, knowing that the local telephone company could not fully satisfy the court order or do so on a timely basis. Also, in 1992, one state law enforcement agency advised the FBI that approximately 25% of its electronic surveillances were impeded by advanced telecommunications technology. However, more importantly, it is critical to understand that emerging technologies undoubtedly will have a broader and more devastating effect on electronic surveillance in the future, if accommodations for law enforcement are not required by law now.

Both Mr. Neel and Mr. Plessner cited a Computer Professionals for Social Responsibility (CPSR) FOIA request regarding the foregoing informal survey for the proposition that no problems have been encountered. This proposition is a completely false one, and it evidences a fundamental misunderstanding of what the FOIA response they received actually indicated. As a result, they were led to misrepresent that FBI records contain no information regarding such impediments. As noted above, the file contains documents indicating that there were 91 problems. The FBI file documents containing this "positive" information about technological impediments were not released based on the FBI's assertion of lawful "exemptions" to FOIA disclosure, because such disclosure would have identified specific ongoing investigations or investigative subjects, identified specific electronic surveillance vulnerabilities in specific localities, or disclosed classified information associated with foreign counterintelligence or national security investigations.

In his written statement, at page 9, Mr. Berman, quoting a Digital Privacy Security Working Group (DPSWG) report, states: "First, there is no evidence that current law enforcement efforts are being jeopardized by new technologies...." At page six, he similarly states, with reference to "call setup information" (dialing information obtained through pen register/trap and trace devices): "...no case has been made that demonstrates any current or potential difficulty in getting this non-content information under current practices." However, in his oral testimony, and in apparent disagreement both with his written statement and with Messrs.

Plessner and Neel, Mr. Berman testified: "There are going to be problems. There are problems...."

Mr. Neel, who was representing the telecommunications industry (particularly regarding technological capabilities), asserted, inconsistently, both that there was no problem at all and that the problem was so big and costly as to defy remedy.

At page one of his written statement, Mr. Neel states: "... I am not aware of a single instance in which a wire line local telephone company has not been able to effect a lawful intercept due to complications related to advancements in technology." In oral testimony, the following exchange occurred:

Senator Leahy: "Are there features in the present system, features or services, which are untappable?"

Mr. Neel: "In the present system, I believe not."

Yet, both before and after this colloquy, Mr. Neel stated: "The cost of fixing call forwarding alone could be \$1.8 billion dollars." (In his written testimony, at page 7, he indicates: "Preliminary USTA estimates are that software upgrades alone necessary to capture the needed information at the originating end of these calls would cost between \$180 million and \$1.8 billion.") **Why such a large expense for this custom feature in a present system if there is no problem?**

Earlier in his testimony, Mr. Neel stated: "I don't know anyone in this industry that believes that this problem can be fixed only during a 3 year window and thereafter that it's a no brainer. The fact of the matter is the lead time to develop technology that is typically deployed in the Nation's telephone network is about five years or even longer. So it's hard to imagine that we can do this in the three years envisioned and at the cost that is suggested."

Although the Government disagrees with him as to the time, level of effort, and cost required to fix these problems, nevertheless Mr. Neel's apparent admission is telling: there is a problem.

The most obvious evidence of the variety of technical impediments facing law enforcement is the work of the so-called Technical Working Group. Presumably, these technical representatives would not have been dedicated to the task of addressing both current and imminent technological problems, and would not have been meeting with law enforcement for two years, if there were no technological problems.

For a more complete statement as to the nature and extent of the problem, please refer to pages 29-35 of Director Freeh's Congressional testimony submitted for the record.

2. Isn't the current law adequate?

No. The language of the "assistance provision" in the various Federal electronic surveillance and pen register/trap and trace statutes is silent on, and therefore gives no guidance concerning, what level of effort or cost, if any, must be expended when a provider's system as deployed or planned does not readily accommodate execution of electronic surveillance or pen register/trap and trace court orders, or, when impediments are encountered, how quickly an effort must be undertaken and completed.

Referring to the current "assistance" language and arguing against legislation, Mr. Neel states, at page 3 of his written statement: "It is hard to imagine statutory language that more fully mandates cooperation with any possible needs law enforcement may have." Mr. Neel misses the point. There is no disagreement that service providers and others are mandated to assist. The issue is the nature and extent of that mandate.

Attorneys for the FBI, Bellcore, and the telecommunications industry believe the current language does not clearly define the responsibilities of service providers, particularly when some level of effort is required beyond the rudimentary furnishing of line information and leased line facilities. The current language was adequate when enacted in 1970, since telephony technology then was relatively simple and there were relatively few service providers. Today's telecommunications marketplace is vastly different, more complex, and abounding with service providers (e.g., over 2,000 common carriers alone).

Hence, it is imperative that the generic electronic surveillance requirements be articulated formally, that common carrier responsibilities be spelled out, and that a reasonable compliance period be set. Legislation is the only way to put all common carriers on notice regarding these requirements and to legally obligate the over 2,000 carriers to act in a timely and comprehensive fashion. Further, legislation is needed in order to formally enlist the cooperation of support service providers and equipment manufacturers upon whom common carriers rely for provisioning service. So also it is necessary to define the Government's legal and equitable remedies regarding common carriers who fail or refuse to comply and to provide a mechanism for reimbursement to common carriers for costs expended in making the modifications associated with achieving compliance.

If there were any doubt about whether new legislative language is needed to clarify those responsibilities, one need only consider the complaints and false accusations made by opposition spokespersons, particularly those of the DPSWG, concerning the proposed legislation's memorialization of law enforcement's long-standing requirements. A detailed statement of the inadequacy of the current "assistance provision" language is set forth at pages 24-27 of Director Freeh's Congressional testimony submitted for the record.

3. Is this a "course correction" or a "fundamental change in course"?

Neither. This represents "staying the course." The proposed legislation simply would maintain the status quo by elaborating on and clarifying the "assistance requirement" enacted by Congress in 1970, which evidenced the Congress' clear intent that lawful court orders should not be frustrated due to a common carrier's failure to provide needed technological assistance and facilities.

In fact, without this legislation, the Congress would in essence be accepting a course change occasioned by the vagaries of telecommunications technology. The reality is that, in the absence of a formal legislative policy review, telephone companies have been introducing (and continue to introduce) systems, features, and services that do not accommodate law enforcement and lawful court orders and which impair, or even preclude, electronic surveillance -- a de facto repeal of the 1970 legislation.

Senator Cohen's comments were quite insightful when he raised strong concerns about the sometimes mindless deployment of technology that can pose threats to the safety and privacy of the public. He indicated that people should be the master of technology, rather than technology being the master of people.

A more complete statement of the proposed legislation's adherence to current legal authorities can be found at pages 3, 40-41, 49-51, and 57-60 of Director Freeh's Congressional testimony submitted for the record.

4. Won't legislation requiring current telecommunications systems and new telecommunications services to accommodate law enforcement's electronic surveillance requirements stop or delay the deployment of such systems or services?

No. Notwithstanding loose talk and pure speculation from industry lobbyists and some special interest groups, no authoritative telecommunications industry technology spokesperson has claimed, or offered any specific evidence, that the telecommunications industry cannot modify existing or future systems without disrupting or delaying service, if it is given a reasonable time period, such as three years, within which to comply.

The fact is that telecommunications networks are in a continuous state of modification or change. That is, telecommunications upgrades/features are constantly being designed, developed, tested, and scheduled for deployment. These modifications or changes are the result of requested or anticipated needs of customers for new services and features. A "law enforcement electronic surveillance feature package" likewise can be devel-

oped and deployed in the exact same fashion as "commercial" upgrades and feature modifications -- without disruption.

It is noteworthy that industry lobbyists only claim negative impacts on the introduction of new commercial services when the electronic surveillance requirements are addressed in legislation, as opposed to voluntary cooperation. Such a notion is fundamentally and logically inconsistent. Either there will be an adverse impact, with or without legislation, or not, with or without legislation, assuming a reasonable period of time is established for making needed modifications. As recently as March 11, 1994, telecommunications industry representatives were asked point blank to tell us if the three year period set for compliance would be a problem, would be unrealistic, or would disrupt or delay services. Not one person said that it would.

Further, as you may recall from our March 11 meeting with the telecommunications industry representatives, they were asked to identify for us any technology that might be a candidate for compliance beyond the three year period specified in the proposed legislation. We indicated a willingness to consider postponing compliance for any such technology where it was justified. To date, we have received no reply from industry in this regard.

Mr. Berman alleged in his oral statement that legislatively-required assistance amounts to "industrial policy." **This hyperbole, of course, is false.** Oddly, Mr. Berman appears to have no problem with electronic surveillance requirements being implemented, but he objects to having them made clear in legislation, so that every common carrier is put on notice and legally obligated, and so there would be a level playing field.

For a more complete statement on this issue, see pages 54-55 of Director Freeh's Congressional testimony submitted for the record.

5. Won't this allow the Government to "veto" telecommunications technology?

No. The characterization of the Government's imposition of some requirements in an area of technology or commerce constituting a "veto" is entirely false and misleading. Requiring industries to meet various requirements for the public safety or the national security is a routine occurrence and a common policy of Government. The proposed legislation simply indicates that whatever technologies are fielded by common carriers after three years must accommodate legitimate law enforcement, public safety, and national security needs.

As noted above, no industry technical representative has identified a single telecommunications technology whose

development or deployment would be prevented by law enforcement's electronic surveillance requirements, assuming sufficient time is given for compliance. Hence, assertions of a Government "veto" of technology are simply flippant mischaracterizations.

Mr. Neel in his written statement, at page 8, states: "This legislation would make the Attorney General the arbiter of whatever technologies and equipment can be deployed in the public telecommunications network." (emphasis added) To the contrary, the Attorney General will not judge or ordain which technologies are fielded, nor will she judge or ordain how any needed modification may be made. All such decisions rest exclusively with the common carriers.

Such comments also completely ignore the countless Federal laws and regulations that impose legitimate duties on almost all of our industries and areas of commerce when required for the public good. It is unclear why the telecommunications industry would consider itself exempt from the sorts of public safety laws applied to all other sectors of industry, especially given the fact that common carriers historically have been licensed and regulated to a higher standard than other sectors of industry.

Importantly, by having legislation address not only current technologies but emerging technologies as well, there will be an assurance of a smooth technology transition, where there will be no surprises or technologies that so prevent or hamper court-authorized electronic surveillance as to lead some in the future to call for their embargo. By pursuing comprehensive coverage, and avoiding a limited, "band aid" legislative approach, common carriers can plan for the future with certainty, and cost-effective compliance can be achieved with the least amount of disruption.

The bottom line is: the proposed legislation doesn't "veto" technology or technological advancement; rather, as Senator Cohen suggests, it brings common sense to bear regarding it. For further information regarding this issue, refer to pages 54-55 of Director Freeh's Congressional testimony submitted for the record.

6. Isn't it true that the legislation will allow law enforcement to obtain more and different information than it does now? Won't privacy rights, as encompassed in information such as medical records, be adversely affected in some new fashion?

No. The proposed legislation simply would allow law enforcement to maintain the status quo as it relates to legal authorities under our electronic surveillance and pen register/trap and trace statutes, and as it relates to the types of information obtainable today through interception and pen register and trap and trace devices used pursuant to court order.

As part of the "false transactional data scare," privacy-based groups, such as the DPSWG, and others have inaccurately charged that law enforcement is attempting, through the proposed legislation, to expand its legal authorities or obtain new types of information heretofore not obtained through these legal authorities and devices. This is categorically untrue.

At page six of his written statement, Mr. Neel states: "In describing its proposal, the FBI strongly asserts that it is not seeking expanded authority. We must, with all due respect, disagree. We believe that this is a level of surveillance capability unprecedented in terms of immediacy, breadth of application or capability for routine surveillance of individual citizens." He also alleges the public will fear that "their local sheriff will be developing a dossier on them based on call setup information...." (Emphasis added.)

Similarly, at page five of Mr. Berman's written statement, he alleges that the proposed legislation "threatens privacy rights" since it provides for obtaining "call setup information" (which he falsely characterizes as "transactional information") by subpoena. (Telecommunications-based transactional information, as defined in Federal law (Chapter 121 of Title 18), is not the subject of this legislation. The proposed legislation explicitly states that it exclusively relates to electronic surveillance and pen register and trap and trace authorities found in Chapters 119 and 206 of Title 18 and Chapter 36 of Title 50.)

At page five of his written statement, Mr. Berman states: "This transactional data certainly could make it possible to build a detailed model of an individual's behavior and movements. The net result could be government dictating to industry that it create a surveillance-based system that would allow federal, state, and local governments to use a service provider's electronic communication facilities to conduct minute-by-minute surveillance of individuals." (Emphasis added.)

(Mr. Berman previously has stated in a 2/24/94 Electronic Frontier Foundation (EFF) Statement on the FBI Draft Digital Telephony Bill:

"The real impact of the FBI proposal turns, in part, on the fact that it is easy to obtain court approval for seizing transactional data.

The change from existing law contained in the FBI proposal is that carriers would have to deliver this call setup information *in real time* directly to a remote listening post designated by law enforcement. Today, the government can obtain this information, but generally has to install a device (called a 'pen register') which is monitored manually at the telephone company switching office." (Emphasis added.))

Mr. Berman and Mr. Neel have their facts completely wrong. Law enforcement agencies do not monitor pen registers at telephone company switching offices. They certainly do not manually monitor them there. In fact, for decades law enforcement agencies, assisted by common carriers, have received such dialing information from pen registers "in real time" and at "remote listening posts designated by law enforcement." The legislation does not require common carriers to "create" some new technological capability; rather, it simply requires them to maintain the current one.

To the extent the "call setup information" (dialing information) tells something about people and their activities, this has been the case since the first primitive "pen registers" were employed decades ago. Under the proposed legislation, law enforcement would acquire this dialing information as it does today -- contemporaneous with the call placement and at a monitoring site removed from the initial technical point of acquisition. There is no change -- it maintains the **status quo**.

All pen registers and dialed number recorders on the market and used throughout the law enforcement community are analog-based. These analog pen register/dialed number recorder devices, used pursuant to the Federal and state laws which regulate them, require court orders and do not acquire communications "content" or file or data information transmissions.

In his oral testimony, Mr. Berman stated, with regard to "call setup information" (which, as noted before, he inaccurately defines as transactional information): "This dwarfs NCIC. This is NCIC squared, because this really is the real time transactions not of people arrested or wanted, but of every live American human being dealing in the electronic communications era." (Emphasis added.)

Such a characterization is palpably false. Court orders are neither sought by government attorneys nor granted by courts for the purpose of acquiring information about persons who are not centrally involved in a criminal investigation. There are no "routine surveillances" of innocent people. Nor are court orders issued for irrelevant, noncriminal, or privileged information. Hence, law enforcement's maintaining a capability to acquire "call setup information" pursuant to court order would in no way lead to the acquisition of medical records or any other such data, from either criminals or noncriminals.

Even if an electronic surveillance court order were obtained (to allow for the interception of communications content), a medical file or other such information would not be acquired, since pursuant to the electronic surveillance law's "minimization" requirement this type of information would not be monitored or recorded since it would be non-criminal, irrelevant, and privileged information. Further, doctor-patient records/communications are privileged by statute in most states, and, in any event, are not the type of records that interest investigators.

As a practical matter, the FBI and other law enforcement agencies do not ever have an interest in such information as medical records, magazine subscriptions, or video rental records. In those unusual circumstances when such information is directly related and relevant to the ongoing investigation being conducted by the law enforcement agency, this information is acquired by subpoena or court order. Suggestions that law enforcement officers are petty voyeurs or snoops are both false and slanderous.

Finally, the acquisition of the type of electronically transmitted "transactional information" records that some privacy advocates appear to fear, pales in comparison to the volume of documentary information, such as bank/credit card purchasing information that is lawfully available to law enforcement, pursuant to the Right to Financial Privacy Act, by subpoena, administrative subpoena, or even formal agency request. More telling, such information is routinely sold and exchanged in the private sector with little or no legal constraint. By comparison, the use of pen register/trap and trace devices always requires a court order. The notion propounded by Mr. Berman that transactional information should only be available based upon a probable cause warrant is a radical departure from past law and jurisprudence and would cause the acquisition of electronic transactional information to be treated vastly differently than documentary transactional information.

Whereas the Government's legislative proposal seeks to maintain the legal/technical **status quo**, Mr. Berman and the DPSWG appear to be seeking a repeal of the pen register/trap and trace provisions enacted in the Electronic Communications Privacy Act of 1986. At page 5 of his written statement, Mr. Berman states: "Extending the legislation's scope beyond the acquisition of content (pursuant to a [Title III] warrant under Section 2518) to the independent acquisition of call setup information raises many issues that require examination." Mr. Berman fails to state that this precise authority that so concerns him currently exists in statute (18 U.S.C. 3121-27) and had existed for years before.

For a more complete statement regarding this issue, refer to pages 57-62 of Director Freeh's Congressional statement submitted for the record.

7. Won't this legislation require common carriers to become "agents of law enforcement"?

Absolutely not. The proposed legislation simply specifies that law enforcement's electronic surveillance requirements shall be included among the scores of other features and services that comprise the Nation's telephone networks.

At page three of his written statement, Mr. Neel states: "It [the legislation] also forces local exchange

carriers to become, in effect, agents of the law enforcement community, rather than maintaining the more appropriate arms-length relationship between common carriers and law enforcement."

Mr. Neel nowhere describes specifically how the proposed legislation's clarification of the current "assistance provision" leads to such a conclusion. Also at page three, Mr. Neel quotes the current "assistance requirement" language, emphasizing the breadth and mandatory nature of this language (e.g., an order ... shall ... direct a ... common carrier...[to] furnish ...forthwith all information, facilities, and technical assistance necessary to accomplish the interception..."), stating: **"It is hard to imagine statutory language that more fully mandates cooperation with any possible needs law enforcement may have."**

If the current language fully mandates cooperation with any possible needs law enforcement may have, and if Neel supports the current language, as he appears to, it's unclear how the proposed legislation, which only clarifies that language, could make a common carrier an "agent of law enforcement" **any more** than the current language does. The electronic surveillance requirements set out in the legislative proposal simply memorialize long-standing requirements known to major common carriers for years...

The fact of the matter is that, aside from the "assistance provisions" at issue here, telephone companies have been mandated for years to take steps which further legitimate and important law enforcement needs by providing needed assistance (e.g., they are required to retain telephone toll records beyond the period required by the telephone company for billing purposes; in many areas, they are required to provide "911" service; etc.) Such requirements are indicative of the special responsibilities conferred upon common carriers as publicly-regulated utilities and otherwise.

Further, Mr. Neel's "alternative" to legislation requiring the removal of technological impediments after three years (i.e., voluntary cooperation through the industry technical working group) presumably would in no way make a common carrier less of an "agent of law enforcement." Indeed, **numerous telephone companies have told us directly in the past that legislation is needed to prevent the perception that some subscribers may have that a telephone company was "in bed with law enforcement," if it undertook to modify its network voluntarily.**

8. Is it inappropriate to limit the coverage of the legislation to common carriers?

No. Recognizing that legislation should be used as a last resort and then surgically, the Administration has determined to focus the legislation narrowly and specifically where the technological impediments have had the greatest impact on law enforcement -- within the networks of common carriers.

In Mr. Neel's oral statement he argued that any legislation should apply to all providers, not just common carriers. Apparently arguing on behalf of law enforcement's needs, he stated that it would be wrong "to take out of the picture those who would oppose the legislation" and that "by exempting these we dramatically restrict the ability of law enforcement to get information." The current legislation's coverage intentionally focuses on where the greatest impediments are. The legislation intentionally excludes telecommunications services, such as PBXs, where relatively few wiretaps are conducted and where the impediments have been minor. Secondly, non-common carrier computer networks have been excluded for the same reasons. It should be noted that Messrs. Berman and Plesser specifically advised the FBI, with regard to inclusion of computer networks and PBXs in the 1992 draft of legislation, that the Government should not include such entities absent documented problems in those areas.

Mr. Neel further objected to what he believed was the exclusion of the now-emerging Personal Communications Services (PCS) networks. PCS carriers, of course, are common carriers and are included. Mr. Plesser, who advised in his testimony that he represents PCS companies, stated: "PCS, by the way, is covered. There is forbearance, but they would be subject to and covered in this area, so I'm not sure where that information comes from."

The fact of the matter is that the overwhelming majority of criminals use mainstream telephone service for voice communications, provided by common carriers, as they plan and execute their criminal conspiracies and activities. The impediments of concern in this legislation are clearly those occurring within common carrier networks.

The informal 1993 FBI survey of impediments discloses:

Networks/Systems	Number of Impediments
Common Carrier (CC)	91
Private Branch Exchange	0
Non-CC Computer Networks	0

The allegation that, in order to avoid electronic surveillance, criminals will cease, or minimize, using the public switched telephone network (PSTN) or common carrier networks, if they are maintained as wiretapable, is not supported by the facts and, in fact, is contradicted by past experience.

9. Are the cost estimates of the proposed legislation unrealistically low?

No. Although it is impossible to specify the costs exactly, the amount authorized to be appropriated (\$500 million) in the legislative proposal is believed to be a reasonable estimate. Failure to act now and comprehensively would lead to substantially greater costs in the future. Given the importance of electronic surveillance in preventing acts of terrorism and other grave crimes, where great loss of life and billions of dollars in harm are at stake, Government cannot afford not to address this problem now.

At the outset, it is critical to understand that in the proposed legislation Government does not dictate to common carriers how to configure their networks to achieve compliance. Each carrier will undoubtedly proceed in a fashion offering the greatest technological ease and cost-effectiveness. This circumstance and the fact that there are over 2,000 common carriers preclude exact pricing. At the March 11 industry meeting, one common carrier representative opined that costs for making all the technological modifications would be much greater than \$500 million, while another carrier representative believed the cost of the modifications would be less and, in some instances, negligible.

In oral testimony, Mr. Neel repeated several times that the cost of fixing one part of the call forwarding problem alone "could be \$1.8 billion dollars." However, his written statement indicates: "Preliminary USTA estimates are that the software upgrades alone necessary to capture the needed information ... would cost between \$180 million and \$1.8 billion." Such a wide discrepancy (\$180 million vs. \$1.8 billion -- a tenfold factor) by industry itself demonstrates the difficulty in estimating cost and the possibility that it could be one-tenth (or even less) the cost cited by Mr. Neel in his oral testimony.

There is one certainty as to the cost: the longer the Government waits to rectify this problem, the greater the cost. Hence, the cost today is substantially greater than it would have been had industry responded three years ago. Further, passage of noncomprehensive, "band aid" legislation will assure future technological problems in emerging and future technologies which, if addressed later, will cost vastly more than if addressed prospectively, as they are developed, pursuant to this legislation.

In considering cost, one must evaluate "societal costs." Electronic surveillance directly enabled law enforcement to prevent a terrorist rocket attack on a commercial airliner, where hundreds of lives would have been lost. Similarly, electronic surveillance assisted in foiling another recent terrorist attack which would have imperiled hundreds of lives and caused billions of dollars in economic damage in one of our Nation's largest commercial marketplaces. These are only two of the numerous "societal costs" that must be considered.

10. Are there viable solutions short of legislation? Won't the efforts of the Industry Technical Working Group suffice?

No. Voluntary approaches clearly will not work. Because of the fact that there are over 2,000 common carriers; that the ATIS-based Technical Committee/Working Group has no authority to require any carrier to implement needed modifications at all, let alone on a timely basis; that there is no mechanism to require the critical cooperation of equipment manufacturers and support service providers, and no clear and meaningful enforcement authorities; and the fact that there is no funding mechanism to remunerate common carriers for current and future compliance.

In his testimony, Mr. Neel stated legislation is not needed. He said the solution was to "redouble the efforts of the Quantico Working Group [now working under the aegis of ATIS]," which he asserted "had only had a chance to work together for one year." Later, he stated: "The entire local telephone industry is represented in these meetings. My information is that the participation in that work is enthusiastic, that attendance is universal, and I don't think our industry would have any problems with sterner mandates for participation in that process." He further characterized the legislative initiative as an indication that law enforcement was "walking away" from this process.

There are numerous flaws in these assertions. First, this group was the idea of industry, and was specifically designed by industry to supplant the prior (1992) legislative proposal. Industry executives who pushed this approach assured then Attorney General Barr that they would institute a technical committee of "the right people" to solve the problem. Given that industry was trying to avoid legislation, its difficult to understand why efforts have been less than fully dedicated if this was a serious proposal -- efforts should not have to be "redoubled."

Second, contrary to Mr. Neel's assertion, this working group has been meeting for two years--not one, during which time not one implementable solution has been produced, let alone actually implemented in a broad, industry-wide fashion.

Third, the FBI voiced grave concerns about the major inadequacies of the Technical Working Group: the Committee is not equipped to implement the technical solutions which it identifies; some companies have not supported these efforts and others have not contributed meaningfully to the effort; and efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all representatives on the Committee. In response, ATIS Committee Chairman, NYNEX Chairman Casimir S. Skrzypczak, stated, "...these observations which you find troubling are aspects of the committee process which are fundamental to the operation and interest of open industry forums. One of the basic principles of any inter-industry committee or forum is that solutions reached

are proposals for voluntary implementation by the participants: recommendations are non-binding." (Emphasis added.) The FBI's correspondence with Mr. Skrzypczak and his reply are attached.

Fourth, how does one interpret Mr. Neel's avowed willingness for industry to accept "sterner mandates for participation in that process?" If he is willing to have ~~mandated~~ participation and timely solutions, how is that different than the gist of the legislation? How does one mandate such activities? There is only one way that such a mandate can be dictated--legislation. Congressional resolutions, "senses of Congress," or the like have no legally binding effect. However, if he really isn't endorsing legislation, then talk of "sterner mandates" is just talk.

Fifth, the proposed legislation clearly states that law enforcement has no intention of "walking away" from the efforts begun under the ATIS committee process. To the contrary, Section (g) of the legislative proposal, "Consultation," indicates that the Attorney General is to "consult with ... common carrier representatives and to utilize common carrier standards bodies, associations, and other such organizations to discuss details of the requirements, such as those relating to capacity, and cost effective approaches in order to facilitate compliance"

The section-by-section analysis of the proposed legislation further elaborates, and makes clear why the reliance on informal bodies alone is unworkable:

"... because of the voluntary basis and elective nature of participation in and commitment to this body [the Working Group], its lack of authority to require the implementation of solutions or to assign funding responsibility, and given that there is no clear legal mandate to fulfil the government's requirements on a timely basis, these committees have not been effective to date in engendering the development, let alone the implementation, of the required solutions. With legislation mandating future compliance and addressing funding concerns, it is reasonable to assume that common carriers and others will utilize such committees in a more meaningful and beneficial fashion." See Section-by-Section Analysis page 13.

Indeed, one must remember that when the FBI began talking to industry executives approximately four years ago that some of them expressed the opinion that they could not undertake corrective efforts absent some mandate. They cited perceptions that subscribers and shareholders might have (that 'they were in bed with law enforcement') and that there needed to be "a level playing field" among common carriers, so that a responsible telephone company would not be placed at a competitive disadvantage vis a vis a carrier lacking social responsibility.

Senator Cohen echoed these serious concerns in his remarks at the hearing:

"As the race for superiority in this technological field continues to escalate, there will be some firms that will say 'we really don't want to be a part of this. We think we got a better deal than AT&T, or whatever, and we will get there faster and not comply with what these responsible firms are trying to do to accommodate law enforcement's needs. We really don't have that interest. What we want to do is make it there first, to get there first. We want to get there fast and make the biggest amount of money, and if we can get there domestically and internationally, that's what we're going to do, and to hell with the FBI and law enforcement in general.'"

In spite of Mr. Neel's assertions of industry's good faith and desire to assist law enforcement, the stark fact is that, even though the FBI has been imploring the telecommunications industry to develop and implement the needed modifications for nearly four years, to our knowledge there has not been any commitment for industry-wide implementation of these modifications. Consequently, the problem continues to grow and the costs continue to skyrocket.

For a more complete statement regarding law enforcement efforts to resolve the problem through dialogue with industry and through the Technical Working Group, refer to pages 35-39 of Director Freeh's statement submitted for the record.

RESPONSES TO SENATOR PRESSLER'S WRITTEN QUESTIONS OF FBI DIRECTOR FREEH CONCERNING THE ADMINISTRATION'S PROPOSED "DIGITAL TELEPHONY AND COMMUNICATIONS PRIVACY IMPROVEMENT ACT OF 1994."

Question: Why is further legislation necessary? What is lost now that will be gained by this legislation?

There is no disagreement that under current law telecommunications companies and others are mandated to assist law enforcement agencies execute court orders for electronic surveillance and pen registers/trap and traces, pursuant to court orders directing them to do so. **The issue is the nature and extent of that mandate.** The current language of the "assistance provision" in the various Federal electronic surveillance and pen register/trap and trace statutes, though unambiguous in its mandate, is silent on (and therefore gives no guidance concerning) what level of effort or level of cost, if any, must be expended by a provider when its system, as deployed or planned, does not readily accommodate execution of electronic surveillance or pen register/trap and trace court orders, or, when impediments are encountered, how quickly an effort must be undertaken and completed.

Attorneys for the FBI, Bellcore, and the telecommunications industry believe **the current language does not clearly define the responsibilities of service providers**, particularly when some level of effort is required beyond the rudimentary furnishing of line information and leased line facilities. The current language was adequate when enacted in 1970, since telephony technology then was relatively simple and there were relatively few service providers. Today's telecommunications marketplace is vastly different, more complex, and abounding with service providers (e.g., over 2,000 common carriers alone).

Hence, it is imperative that the generic electronic surveillance requirements of law enforcement be articulated formally, that

common carrier responsibilities be spelled out, and that a reasonable compliance period be set. Legislation is the only way to put all common carriers on notice regarding these requirements and to legally obligate the over 2,000 carriers to act in a timely and comprehensive fashion. Further, legislation is needed in order to formally enlist the cooperation of support service providers and equipment manufacturers upon whom common carriers rely for provisioning service. So also it is necessary to define the Government's legal and equitable remedies regarding common carriers who fail or refuse to comply or who are dilatory, and to provide a mechanism for reimbursement to common carriers for costs expended in making the modifications associated with achieving compliance.

If there were any doubt about whether new legislative language is needed to clarify and memorialize the above-mentioned requirements and responsibilities, one need only consider the complaints and false accusations made by some opposition spokespersons concerning the proposed legislation's memorialization of law enforcement's long-standing requirements.

A detailed statement of the inadequacy of the current "assistance provision" language is set forth at pages 24-27 of Director Freeh's statement submitted for the record.

Question: How much of a problem is this today? In how many actual cases, roughly, has the FBI been unable to accomplish a court-approved wiretap due to a telecommunications company's inability to make the tap?

The problem, though hard to quantify, is significant and is clearly growing. The informal FBI survey documented 91 such problems, but there have been many more. Over the last decade, we estimate that several hundred court orders have been frustrated or were not sought because of these problems.

With the introduction and growth of cellular telephone systems, and the introduction and use of sophisticated features and services, the number of court orders for electronic surveillance and/or pen register/trap and traces that were frustrated, in whole or in part, or delayed, or were not sought, grew. With the on-going introduction of even newer, more sophisticated features and services, wireless systems, etc., the number of technological problems will grow at an accelerated rate and the ability of law enforcement agencies to fully and properly execute these court orders will continue to erode.

There is no single repository for information regarding the number of court orders that could not be properly executed with regard to the hundreds of criminal Title III wiretap and thousands of pen register court orders executed each year by hundreds of law enforcement agencies throughout the U. S. It was precisely this circumstance that led the FBI to conduct an informal survey in 1992 to attempt to gather some data, however imprecise, regarding this serious problem. This informal survey disclosed 91 "recent" problems. Information regarding these problems was retrieved by FBI field office Technically Trained Agents (TTAs), and most of the information reported on pertained to FBI cases. It is unclear how effective these TTAs were in obtaining sensitive information from state and local law enforcement authorities about problems they were encountering in executing court orders, particularly regarding then pending electronic surveillance efforts.

The FBI relies upon Technically Trained Special Agents (TTA) throughout the United States to technically implement the execution of the court orders. This duty also involves technical liaison with the telecommunication companies. Problems encountered by these TTAs are sometimes brought to the attention of FBIHQ through requests from the field TTAs for assistance from the FBIHQ's Engineering Section. It is usually through these requests that such problems become known, though they are not tabulated. In

addition to the court orders that cannot be executed (fully executed), many requests for electronic surveillance or pen registers/trap and traces by field office Special Agents have been discouraged by the TTAs in a number of field offices due to known on-going impediments in a particular area that have frustrated court orders in the recent past. Thus, a significant number of requests were never pursued and never reached the stage of being submitted for court approval. Such "discouraged" requests are not reported formally to FBIHQ and they were not counted in the survey. A third category of problems are those where court orders have been delayed due to capacity limitations within the telecommunications companies' switches. Although such court orders may ultimately be executed, they may be delayed to the point where critical and valuable information is lost or not collected. Finally, there have been a great number of court orders that are not successfully executed because of problems that do not permit the comprehensive interception and acquisition of the subject's communications and/or "call setup information" (dialing information), and therefore have been of limited investigative value. See pages 29-35 of Director Freeh's statement for the record regarding this issue.

Question: Is the problem that the technology is too sophisticated or is it that the companies do not provide adequate access points?

Generally, the latter. The level of sophistication of the new technology is not viewed as a problem. To the contrary, the sophisticated switches and equipment being developed and deployed today are more capable than the less sophisticated switches that have been in use for many years. As service providers deploy more sophisticated switches, they develop more sophisticated features and services in response to or in anticipation of the **commercial** demands of their customers. If service providers view the electronic surveillance requirements of law enforcement as sophisticated functional "features," there is no reason to believe that the switches (which are essentially specialized computers)

cannot accommodate this functionality. The real problem is that the companies that manufacture and operate this equipment currently have no economic incentive or clear, specific legal requirement to include these functions as features in their developmental effort. If the needs of law enforcement agencies are accommodated during the developmental phase of new systems, features, and equipment, as is the case with other commercial services and features that are marketed to the public, adequate capabilities and access for electronic surveillance can be provided to law enforcement agencies without any adverse impact on the networks and without delaying the introduction of new commercial services and features.

Question: Can you describe several examples?

During the early 1980s, there was an explosive growth in the use of cellular telephones. The need to conduct electronic surveillance and pen register investigations within cellular systems became evident at an early stage. Unfortunately, the systems had been developed several years earlier and were being deployed rapidly. After unsatisfactory attempts to intercept cellular telephones on the radio frequency portion of the cellular system, law enforcement agencies sought the assistance of cellular providers in order to execute the court orders. Many cellular service providers (and there are literally hundreds of new companies for law enforcement agencies to deal with) were not aware of, or always responsive to, their legal obligation to assist law enforcement agencies with the execution of court orders. After a number of years, a number of technical solutions were eventually developed and deployed on a case-by-case basis (often with the government funding the system upgrade). The delayed deployment of these solutions led to an unknown (but we estimate significant) number of court orders not being executed, not being fully executed, or being delayed in their execution. Additionally, since these solutions were not considered in the development cycle of the cellular equipment and were of a "band aid," retrofit nature, in

many instances the capacity range of some of these solutions was limited, which affected the number of simultaneous court orders that could be conducted, and in others their overall capability or functionality was limited.

Another example is call forwarding. When call forwarding was first introduced by telecommunications providers, the element that "forwarded" or re-directed telephone calls was the central office switch. As such, even though a subject might forward his calls across the country, the content of the call itself still passed through the central office switch that served his telephone instrument. However, once forwarded, the subject's call did not appear in the local loop -- law enforcement's traditional access point. Further, since no provision was made for lawful law enforcement electronic surveillance access during the development and deployment of call forwarding, service providers **themselves** were unable to afford law enforcement an effective means of acquiring such forwarded communications, even though they pass through their switches.

Question: I understand that the General Services Administration (GSA) was opposed several years ago to an earlier FBI proposal regarding this same issue.

Are they opposed to this latest version?

Please explain what changes were made from the earlier version to the latest one?

As you are aware, the Administration's Digital Telephony legislative proposal, as well as an earlier legislative proposal formally transmitted to the 102nd Congress under the Bush Administration, deals with the issue of law enforcement's continued technical ability to conduct court-authorized electronic surveillances as advanced telecommunication technologies, services, and features are introduced into the nation's telecommunications

networks. GSA is not a law enforcement agency and therefore has no expertise in the area of court-authorized electronic surveillances, nor does it have any particular expertise relative to any possible impact the incorporation of law enforcement's electronic surveillance requirements might have with regard to current or future networks, systems, features, or services. (By comparison, neither the FCC nor the National Institute of Standards and Technology (NIST), which also possesses telecommunications expertise, interposed any objection to the legislative proposal.) Unfortunately, in 1992, GSA comments were solicited by OMB in the context of an expedited legislative proposal clearance process, without GSA being privy to the numerous, lengthy, and in-depth legal and technical discussions and briefings which preceded the clearance process.

Consequently, although GSA's comments were considered along with those from other agencies within the Bush Administration, given the above, GSA's comments were evaluated accordingly. The important position was not GSA's but that of the Bush Administration. The Bush Administration determined that the only realistic way to effectively address the "digital telephony" problem was through a comprehensive legislative solution. Such a comprehensive legislative solution was formally transmitted to the 102nd Congress by the Bush Administration in September of 1992; however, time did not permit any action being taken on it.

In April, 1993, President Clinton directed that an interagency working group be established to examine, among other things, telecommunication technology trends and their impact on court-ordered electronic surveillances. After an in-depth eight month study, the Clinton Administration likewise determined that the only effective way to address the so-called "digital telephony" problem is through a comprehensive legislative solution; and a formal administration legislative proposal, entitled the "Digital Telephony and Communication Privacy Improvement Act of 1994," was transmitted to Congress on March 25, 1994. Fundamental to this decision was the

Clinton Administration's belief, like that of the Bush Administration, that it would be unacceptable for the safety of the American public to be imperiled, the national security to be endangered, and effective law enforcement to be eroded through the diminishment or loss of this critical and essential tool of our nation's law enforcement and intelligence agencies.

The current legislative proposal is a significant improvement over the prior proposal, and includes a number of new and important provisions, many of which were developed after we received input from the telecommunications industry regarding the 1992 proposal. The current legislative proposal focuses on where the problems are -- within the networks of common carriers. Hence, all other types of service providers (computer networks, PBX operators, etc.) have been eliminated from coverage. The time period for common carrier compliance has been doubled from 18 months to three years. The wording of the electronic surveillance requirements has been refined based on industry suggestions. A "systems security provision" has been added to reflect that any premises/switch-based intercepts will only be initiated by designated common carrier personnel. The assistance of the FCC is included. Importantly, a provision for on-going "consultation" using industry standards bodies and other fora is established to ensure cost-effective compliance, and the Attorney General is authorized to reimburse common carriers for all reasonable costs directly associated with the modifications required to be performed in order for common carriers to comply with the Act, up to \$500 million under the current proposal. Finally, the proposed legislation includes provisions that improve communications privacy protection for cordless telephones, certain radio-based data communications, and communications transmitted using certain privacy-enhancing modulation techniques.

Question: The telecommunications industry claims this legislation would go well beyond the status quo by allowing the FBI to be part of the front-end design process, where it has not been previously.

How do you respond to their concerns?

The industry's claim is erroneous. The purpose and effect of the Administration's proposed legislation is to clarify and define the existing responsibilities of common carriers to provide the "technical assistance necessary to accomplish the interception." The proposed legislation does not require common carriers to design their systems in any one, particular way; and it certainly doesn't contemplate the FBI or any other law enforcement agency dictating network design. The legislative proposal simply requires that common carriers be able to respond to the long-standing generic electronic surveillance requirements of law enforcement and be able to meet their current legal responsibility to effectively "assist" law enforcement when served with a court order.

This legislation also does not propose that industry design systems with the ability to wiretap as the "design goal." Law enforcement is simply requiring common carriers to craft appropriate electronic surveillance solutions that interface with their networks' designs. Industry is in the best position to develop reasonable and cost-effective design solutions which accommodate, rather than frustrate, court orders for electronic surveillance and pen registers/trap and traces, and, at the same time, maintain the security and reliability of telecommunications networks.

Further, this legislation does not prohibit or impede the development or deployment of new telecommunications technologies. We are unaware of any authoritative industry statement that these requirements would significantly delay development or deployment of new technologies. Advanced technologies support a number of features that make systems more intelligent. **The basic technology underpinning the introduction of advanced features and services,**

which often impedes electronic surveillance, likely will also offer solutions to these very problems.

Finally, law enforcement's requirements will not dictate the course or pace of technology. However, with this legislation, our requirements will intentionally be included, rather than excluded, in the development of new technologies in much the same fashion that other legislation requires new technologies and products to take public safety into account and in much the same way that new commercial features and services are developed and deployed by telephone companies for purely economic gain. (For further information, see pgs. 54-55 of Director Freeh's statement for the record.)

Question: As telecommunications technology progresses will the FBI accidentally acquire "content-based" information after only receiving authority to obtain "transactional" information (e.g., banking information) such as with a pen register, which only requires a grand jury subpoena - a lower standard to meet than a warrant issued from a judge?

How should the FBI address this problem?

Is "content" information, obtained according to a subpoena, not a warrant, admissible in court?

Should there be a heightened standard for content information, somewhere between "probable cause" and "reasonable suspicion"?

At the outset, the foregoing questions include a number of mistaken assumptions of fact, law, and investigative procedures. By clarifying these, a meaningful response best can be made.

First, contrary to the false assertions of some in the privacy community, it should be made absolutely clear that the FBI and other law enforcement agencies do not focus investigative efforts on individuals who are not centrally involved in serious (felony) criminality. Further, United States Attorneys/District Attorneys do not authorize grand jury subpoenas or court orders, and courts

do not issue court orders, where relevancy to a criminal investigation is not demonstrated. There are no "routine surveillances" of innocent people. Nor are court orders or subpoenas issued for irrelevant, noncriminal, or privileged information.

Second, under Federal law (18 U.S.C. 3121-27), a pen register lawfully acquires "numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. 3127 (3). Such dialing information or "call setup information" is distinguished under law from call content which is dealt with under the Title III provisions (18 U.S.C. 2510-21) and from telephone transactional records which are dealt with under 18 U.S.C. 2701-11.

Third, use of pen registers by the FBI requires a Federal court order issued from a court of competent jurisdiction. Pen registers may not be used based upon a grand jury subpoena.

Fourth, if Title III content information is introduced in court, the provisions of Title III, including obtaining a Title III court order, must be followed in order to introduce such evidence. The use of pen registers to acquire the numbers dialed is expressly excluded from the treatment of interception of communications content under Title III. 18 U.S.C. 2511(h)(i).

Fifth, when the FBI acquires dialed numbers through the use of a pen register, these numbers mean nothing per se to the FBI. To determine the subscriber information pertaining to the party called (through the numbers dialed), the FBI must then obtain a second form of legal process under 18 U.S.C. 2703 (a subpoena or court order) and serve it on the telephone company. The telephone company in such situations, of course, only possesses and hence only provides the telephone subscriber or listing information that identifies the called party (e.g., (202) 324-3000 is listed to FBIHQ, 10th and Penn. Av., N.W., Washington, D.C.).

Sixth, assuming that the telephone number dialed by the criminal subject is determined to be (after subpoenaing the telephone company subscriber records) a banking or credit card institution, and assuming the FBI desires to examine the subject's financial records, then the FBI is legally obligated to obtain a third form of legal process and serve it on the institution, pursuant to the provisions of the Right to Financial Privacy Act, codified at 12 U.S.C. 3401-3422, especially 3413.

To the extent that dialing information (call setup information) tells something about criminal subjects and their activities, this has been the case since the first primitive "pen registers" were employed decades ago. Under the proposed legislation, law enforcement would acquire this dialing information as it does today -- no more no less.

Although we are sensitive to legitimate privacy concerns, we have not received any information on this topic to suggest that any new laws are required or that current laws require amendment. For example, the notions propounded by Mr. Berman that either telephone transactional information under 18 U.S.C. 2703, or the call setup information (dialing information) obtained through pen registers under 18 U.S.C. 3121 et seq., or both, should only be available based upon a probable cause warrant is a radical departure from past law and jurisprudence and would cause the acquisition of electronic transactional information or records to be treated vastly differently than documentary transactional information and records. There simply is no legal or rational basis for according any type of telephone transactional information or records higher privacy protection than other documentary transactional information or records. As stated above, the dialing information obtained by a pen register always requires a court order, whereas telephone and documentary transactional information and records can be (and historically always have been) obtained through use of a subpoena.

Whereas the Government's legislative proposal simply seeks to maintain the legal/technical status quo, Mr. Berman and the DPSWG appear to be seeking a repeal of the pen register/trap and trace provisions enacted in the Electronic Communications Privacy Act of 1986.

It is particularly puzzling why some privacy rights spokespersons, under the guise of a "false transactional information scare," loudly advocate raising the legal bar to extreme heights for law enforcement's limited access to information concerning criminal subscribers, when telephone companies can afford **broad access (and routinely sell, disclose, or exchange)** much of the same type of information at issue here with the private sector regarding all subscribers with little or no legal constraint.

For a more complete statement regarding this issue, refer to pages 57-62 of the Director Freeh's statement submitted for the record.

Question: The telecommunications industry also is concerned that this legislation will harm their ability to compete with foreign competitors.

First, this legislation applies to all systems and equipment used in the United States, not just American-made equipment and systems, is that correct?

Second, how do you respond to the industry's concern that their ability to compete for contracts in foreign countries will be harmed by this legislation?

First, the Administration's legislative proposal applies to "common carriers" who offer communications services which are deployed within the United States. The legislative proposal requires such common carriers to ensure that their systems have the capabilities and capacities to permit law enforcement to conduct court-authorized electronic surveillance. The proposed does not

specifically address or apply to a single piece of telecommunications equipment but applies to a common carriers services overall.

Secondly, the proposed legislation does not prohibit U.S. manufacturers or service providers from developing or deploying telecommunications equipment or service for sale outside the United States which is different from that required pursuant to the proposed legislation. Domestically, the proposal would mean that all 2,000 common carriers would be competing on a "level playing field" because all common carriers would be required to meet the same requirements within the same compliance period.

Very importantly, other democratic governments also have basic law enforcement and security needs that are nearly identical to those in the United States. Consequently, because of undoubted demands for interception capabilities from law enforcement agencies in other democratic nations, United States manufacturers and providers are very likely to see increased demands from such foreign governments for this type of equipment and service, which will likely offer significant international sales opportunities. (See pages 55-56 of Director Freeh's statement submitted for the record for further information regarding this issue.)

RESPONSES TO SENATOR LEAHY'S WRITTEN QUESTIONS OF FBI DIRECTOR
FREEH CONCERNING THE ADMINISTRATION'S PROPOSED "DIGITAL TELEPHONY
AND COMMUNICATIONS PRIVACY IMPROVEMENT ACT OF 1994."

1. In your written statement, you refer to "numerous situations...where service providers...have been unable to provide assistance to law enforcement agencies," and cite the service provider's inexperience and lack of understanding of law enforcement requirements as the source of the problem. Was digital telephony or any new technology involved? In each situation, please identify the date, the service provider involved, and the specific nature of the problem. In addition, please describe for each situation whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each situation, please indicate whether law enforcement and the service providers involved have been able to resolve the problem.

Generally speaking, most of the impediments encountered by law enforcement within the telecommunications networks are the result of advanced telecommunications technologies. These advanced technologies which support the deployment of new and emerging telecommunications systems, services, and features (e.g. cellular telephony, custom calling features, digital subscriber services) are largely based on digital telephony.

With regard to when, where, and the nature of the problems encountered, and whether any of the problems have been resolved, refer to the answers provided regarding questions 6, 7, and 9, below. Further information, as available, will be provided at a later date.

As stated below, the FBI has made numerous attempts to obtain the assistance of the telecommunications industry to resolve this problem voluntarily--but to no avail. Substantial efforts were made through the industry's Telephone Security Association (TSA), through meetings with Regional Bell Operating Company (RBOC) top executives, meetings with major manufacturer executives, Bellcore, and, for the last two years, through an industry-created ad hoc technical committee, which now meets under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS).

To date, industry has failed to devise solutions to most of the problems, and the technical committee cannot guarantee the implementation of any solutions that may be developed. This critical circumstance was confirmed by ATIS Chairman Mr. Casimir Skrzyczak in his letter to the FBI dated March 1, 1994, which was furnished to the Subcommittees with Director Freeh's statement for the record.

To date, companies have been reluctant to undertake greater efforts to provide assistance absent a clear legal mandate, because they perceive that such assistance places them at a disadvantage when compared to other companies that simply refuse to expend developmental resources for law enforcement needs. The FBI has attempted to encourage service providers to voluntarily comply in different ways; for example, purchasing a known solution for the service provider.

Historically, law enforcement agencies have not taken any steps to compel cooperation by the service providers through legal action for several reasons. First, due to the time-critical nature of most investigations, the length of time needed to resolve a problem through litigation would not result in a satisfactory resolution. Second, litigation concerning such a problem would very likely compromise not just an investigation of a particular subject and his use of a subject telephone but potentially an

entire investigation of a criminal group or organization. Three, there is no clear consensus that such legal action would result in the service providers being compelled to provide the needed assistance or held in contempt under the current law, where the provider is not technically capable of doing so at the time. The prevailing attitude expressed by industry representatives has been that the current statutory "assistance" requirement does not clearly extend to modifications of existing systems or to the development of new equipment or systems to support law enforcement electronic surveillance needs. Fourth, since the working relationships between law enforcement agencies and service providers have been generally good in the past, there has been a fear of damaging these relationships and ultimately impacting many **other** critical investigations negatively. In particular, within the last few years (**and during which time the survey was conducted**), law enforcement has been attempting to have a dialogue with telephone companies to obtain a firm and comprehensive commitment to meeting law enforcement's electronic surveillance requirements within a fixed and reasonable period of time. Seeking contempt of court or other such remedies during this time would fly in the face of this effort and undoubtedly would have been viewed as confrontational and counterproductive. For more detailed information, see pages 35-39 of Director Freeh's statement for the record.

2. What steps have been taken by law enforcement to educate and inform inexperienced service providers?

When law enforcement agencies first become aware of a problem with the inexperience of some service providers, the problem was usually addressed by putting the service provider in contact with other service providers that had previous experience with the specific technological problem being addressed. Secondly, FBI TTAs frequently met with industry technical counterparts, advised them of the law, suggested technical solutions, and often identified or even funded modifications that would allow for at least some level

of improvement. Such efforts, however, did not prevent the routine frustration of court orders, in whole or in part, and/or delays in executing court orders which often impaired investigations.

In 1991, the FBI next brought this problem to the attention of the Telephone Security Association (TSA), the industry association comprised of security office managers upon whom court orders are normally served and with whom arrangements are made to effect electronic surveillance court orders. However, TSA was unable to resolve the problems.

Later (in early 1992), the FBI along with other federal, state, and local law enforcement agencies, after consulting with industry representatives, developed and published a document entitled "Law Enforcement Requirements For The Surveillance Of Electronic Communications." The purpose of this document was to provide telecommunications industry representatives with a generic set of requirements that can be referred to during the design of new systems. In addition to this document, in early 1992 the FBI began to meet on a regular basis with telecommunications industry representatives under the auspices of an industry-created Technical Committee to discuss these requirements. This committee, which was created by industry to avoid legislation, and which began as an ad hoc gathering, has since been chartered under the Alliance for Telecommunications Industry Solutions (ATIS) (formerly the ECSA) as the Electronic Communications Service Provider Committee (ECSPC). The ECSPC is made up of federal, state, and local law enforcement representatives, service providers, and manufacturers. Participation is voluntary and membership is open to all service providers and manufacturers. The ECSPC meets in committee on a quarterly basis with action teams meeting when necessary. The purpose of the ECSPC is to create a forum for dialogue between law enforcement agencies and telecommunications industry representatives to discuss the legitimate needs of law enforcement with respect to new and emerging technologies.

Though helpful, this committee can only recommend solutions, assuming they are developed-- it cannot dictate that any known solution be implemented. As important, there are over 2,000 common carriers and that number is increasing daily. As a practical matter, it is impossible for such a committee to bring about the deployment of needed solutions on a timely and comprehensive basis for over 2,000 common carriers. Legislation alone can assure this.

3) The United States Telephone Association estimated that 1200 digital switches in the U.S. are currently operational. Of the 919 wiretap orders and estimated 9,000 pen register orders authorized in 1992 for all federal, state, and local law enforcement agencies, were any such interception orders conducted on facilities using digital switches? If so, how many?

See Answer to #4 below

4) Up to this point, how many wiretap orders could not be executed because digital switches were used? For each non-executed order, please identify the date, the service provider involved, and the specific nature of the problem. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

It is certain that many of the estimated 919 wiretap orders and 9,000 pen register orders authorized within the U. S. during 1992 were carried out within facilities that use digital switches. For the most part, the local loop, which connects the customer to the central office, has been one of the few links within the network to remain relatively unchanged by the advent of digital

switches, since the local loop is normally an analog link. This has allowed law enforcement agencies to continue to conduct court-ordered wiretaps on the local loop without regard to the type of switch being used. The digital switches that are being deployed today are capable of supporting sophisticated digital transmissions over the local loop; however, to date, these particular services have been sparsely deployed and have caused few problems for law enforcement agencies. However, the use of digital switches by service providers has led to the introduction of many new and sophisticated features and services that were not practical in an analog switching environment. It is the deployment of these new features and services, supported by digital technology, by the service providers that frequently has created problems for law enforcement agencies. As the features and services being deployed and offered by service providers have become more advanced, the communications and dialing information that law enforcement agencies attempt to intercept and acquire become less accessible in the local loop thus making it a less feasible access point, and **effective central office access has not been developed by the telephone companies.** Of course, in the near future when the many and diverse sophisticated digital-based services and features are deployed in the local loop, there will be substantially more problems.

5) You have referred to an informal survey of federal, state, and local law enforcement agencies that uncovered 91 instances where interception orders could not be executed due to technology. Please detail how the survey was conducted.

The FBI relies on a Technical Advisor (TA) within each field office to coordinate the technical efforts necessary to execute court orders and other technical aspects of investigations. These TAs maintain informal technical liaison with many federal, state, and local law enforcement agencies within their field office area. The TAs within each office were asked to collect, through their

contacts with other law enforcement agencies, information relating to recent technology-based problems that have impeded electronic surveillance/pen register/trap and trace efforts. This information was solicited and provided on a confidential basis in order to assure each agency that their ongoing investigations would not be hampered or compromised by the release of this information and in order to protect information regarding the law enforcement agencies' technical capabilities and inabilities. Additionally, this survey was not conducted in a rigorous, comprehensive, or in-depth fashion since participation was entirely voluntary and the information provided was generally limited in detail.

Nonetheless, the information obtained does clearly indicate that there are serious and widespread problems and serious implications regarding the frustration of court orders when telephone companies deploy technology without accommodating electronic surveillance requirements and without considering whether such deployment will, as a practical matter, prevent them from fully and effectively assisting law enforcement pursuant to the statutory "assistance provision" in the current law.

Not included in the tabulation were the numerous instances where court orders were not sought or had been "discouraged" due to these technological impediments. Since this survey was conducted, the FBI has become aware that technology-based problems have been encountered in many more instances.

6) In 40 instances the cellular provider could not provide called number information or had insufficient capacity. For each instance, please identify the date, the service provider involved, and whether the problem was one of capability or capacity. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please

indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

See answer #9 below

7) You have cited 29 instances in which interception orders were impeded because of custom calling features. For each instance, please identify the date, the service provider involved, and whether the problem was one of capability or capacity. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

See answer #9 below

9) You have generally referred to the nature of the problem in 69 of the 91 instances in which interception orders could not be executed due to technology. What was the problem in the remaining 22 instances? For each of those 22 instances, please identify the date, the service provider involved, and the problem. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

The survey that is the source of these numbers, as indicated above, was conducted in an informal way, as a means of trying to determine the scope of the problem that existed at that time and how it was affecting law enforcement agencies. In order to encourage law enforcement agencies to candidly share information

regarding the technological problems they were encountering, the survey was rather narrow in the scope of information sought. Hence, many of the details you have requested were not acquired in the survey. The various agencies were asked only to provide information (no level of detail specified) regarding court orders that were frustrated by technology-based problems.

Of the forty (40) instances of technological problems involving cellular providers that were identified, ten (10) instances resulted from insufficient capacity within the service providers' systems. However, the overall number of court orders that have been frustrated due to limited capacity within the cellular system is known to be much greater than this. It is known, for example, that a large number of requests for cellular-based electronic surveillance and pen register/trap and trace court orders have been discouraged in various localities because of the cellular capacity problem and were therefore never prepared for submission to a court. Although many of the cellular capacity problems have been addressed, some still remain. In addition, there remain many aspects (capability problems) where law enforcement requirements for electronic surveillance of cellular communications have yet to be addressed.

Twenty-nine (29) of the instances of technological problems reported through the survey were associated with custom calling features. Because service providers traditionally have refused law enforcement admittance to central office facilities or have discouraged law enforcement agencies from conducting interceptions from within their central office facilities, and because in the past adequate access could be obtained by law enforcement on the outside plant portion of the telecommunications network, most electronic surveillance/pen registers have been technically effected in the local loop. However, the deployment of calling features has created serious problems for law enforcement agencies and has resulted in the frustration of court orders. For example,

abbreviated dialing features have allowed the subjects of interceptions to place calls from their phones by dialing a short sequence (e.g. #2) which is translated at the central office into a full 10 digit telephone number. There is currently no means for law enforcement to obtain these translations in real-time-- **nor have service providers themselves solved this problem at this time.** Other calling features, such as call forwarding, similarly pose serious problems and frustrate court orders. Call forwarding, in many instances, is carried out by the service provider at the central office switch. The telephone companies' deployment of call forwarding permits subjects to utilize call forwarding to reroute their communications to a distant telephone number. In these cases, communications of interest to law enforcement are not accessible in the local loop. **Further, telephone companies themselves have not devised solutions, to date, to capture these communications.** Although we have not specifically tracked these problems, we know they remain, and we have no reason to believe that they have been resolved where they occurred since they were reported.

The remaining twenty-two (22) instances were in several major categories: Features (other than calling features) such as Voice Mail; central office-based digital subscriber lines (e.g. CENTREX); multiplexed digital transmission lines (e.g. T-1); service provider furnished encryption; fiber optic lines; and trap and trace inabilities on the part of the service provider. Although we have not specifically tracked these problems, we know these problems remain, and we have no reason to believe that they have been resolved where they occurred since they were reported.

One feature that was recently deployed by some service providers has already created problems for law enforcement agencies. "Voice Dialing" is a form of abbreviated dialing feature that allows a user to "dial" a phone number by speaking into the telephone. For example, a user might say "Call work" and thereby be

connected to his work phone by the service provider who has equipment capable of recognizing and decoding his voice. Law enforcement agencies utilizing a pen register to acquire the dialing tones in order to obtain dialing information cannot capture this dialing information. Unless service providers devise a method of furnishing law enforcement agencies this information, many pen register court orders for dialing information will be frustrated.

Historically, law enforcement agencies have not taken any steps to compel cooperation by the service providers through legal action for several reasons. First, due to the time-critical nature of most investigations, the length of time needed to resolve a problem through such means would not result in satisfactory solutions. Second, litigation concerning such a problem would very likely compromise not just an investigation of a particular subject and his use of a subject telephone but potentially an entire investigation of a criminal group or organization. Third, there is no clear consensus that such legal action would result in the service providers being compelled to provide necessary assistance or held in contempt under the current law, where the provider is not technically capable of doing so at the time. The prevailing attitude expressed by industry representatives has been that the current statutory "assistance" requirement does not clearly extend to modifications of existing systems or to the development of new equipment or systems to support law enforcement electronic surveillance needs. Fourth, since the working relationships between law enforcement agencies and service providers have been generally good in the past, there has been a fear of damaging these relationships and ultimately impacting many other critical investigations negatively. In particular, within the last few years (and during which time the survey was conducted), law enforcement has been attempting to have a dialogue with telephone companies to obtain a firm and comprehensive commitment to meeting law enforcement's electronic surveillance requirements within a fixed and reasonable period of time. Seeking contempt of court or

other such remedies during this time undoubtedly would have been viewed as confrontational and would have been counterproductive.

Further, companies have been reluctant to undertake greater efforts to provide assistance because they perceive that such assistance places them at a disadvantage when compared to other companies that simply refuse to expend developmental resources for law enforcement needs. The FBI has attempted to encourage service providers to voluntarily comply in different ways: e.g., in some instances purchasing a known solution for the service provider.

8. Please identify whether the FBI is aware of any technological solution(s) to provide wiretap capability for each custom calling telephone feature that impedes interception orders. What is the estimated cost per year of implementing the technological solution(s) that the FBI has identified for each custom calling feature?

The FBI, through its liaison with many foreign law enforcement agencies, has learned that a technological solution to many of the switch-based problems is under development in one of those countries. The foreign law enforcement agency in question has requested that the FBI not share the details or costs related to this effort. Aside from this constraint, further elaboration would involve classified information.

10. Under the proposal, the Attorney General would be given authority to enforce the requirements. What is the mechanism the Attorney General will use to make accurate estimates of criminal activities requiring wiretaps as an investigative technique, so that industry will be given clear capacity guidelines? Is the FBI able to predict accurately the number of wiretaps that will be employed in the future? If so, has the FBI provided the telephone companies with those estimates and discussed wiretap capacity? What has been the result of those discussions?

The Administration's legislative proposal contains a "consultation" provision (Section 3(g)) which encourages the Attorney General to consult with the FCC and the telecommunications industry to discuss details of the law enforcement requirements "related to capacity and cost-effective approaches." Pursuant to this provision, the Attorney General, through the FBI and other law enforcement representatives, will consult closely with industry so that industry will be able to develop **appropriate and flexible deployment strategies** for their solutions based, in part, upon historical interception activity as well as upon flexible components that accommodate broad "ranges of capacity." (See pages 5 and 6 of the legislative proposal's section-by-section analysis and page 47 of Director Freeh's statement for the record.) Approaches currently being discussed in the Electronic Communications Service Provider Committee, acting under the aegis of ATIS, will most likely allow for acceptable and compliant ranges of intercept/pen register capacity without the need to develop or be concerned with precise interception/pen register/trap and trace numbers.

STATEMENT
OF
LOUIS J. FREEH
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C.
MARCH 18, 1994
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW
OF THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
AND THE
SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS
OF THE COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

MR. CHAIRMEN, I APPRECIATE THE OPPORTUNITY TO APPEAR BEFORE YOUR SUBCOMMITTEES. I AM HERE TODAY NOT JUST IN MY CAPACITY AS DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION BUT ALSO AS A SPOKESMAN FOR OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE COMMUNITIES REGARDING A MATTER OF EXTREME URGENCY AND IMPORTANCE. I AM HERE ON BEHALF OF THE ADMINISTRATION TO TELL YOU THAT WE ARE CONFRONTED WITH A MAJOR THREAT TO OUR ABILITY TO PROTECT THE AMERICAN PUBLIC, SAFEGUARD THE NATIONAL SECURITY, AND EFFECTIVELY ENFORCE THE LAW. THIS THREAT RESULTS FROM VARIOUS TECHNOLOGICAL IMPEDIMENTS TO OUR ABILITY TO EXECUTE COURT ORDERS AND LAWFULLY CONDUCT ELECTRONIC SURVEILLANCE AND ACQUIRE THE ASSOCIATED DIALING INFORMATION. THESE IMPEDIMENTS ARE THE UNINTENDED SIDE EFFECTS OF ADVANCED TELECOMMUNICATIONS TECHNOLOGY WHICH HAS BEEN, AND CONTINUES TO BE, DEPLOYED WITHOUT CONSIDERATION FOR THE CRITICAL NEEDS OF OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.

I AM HERE TODAY TO STRONGLY ASSERT WHAT I AND THE ADMINISTRATION BELIEVE IS THE ONLY RATIONAL AND VIABLE MEANS OF REMOVING THIS THREAT -- THE ENACTMENT OF THE PROPOSED COMPREHENSIVE LEGISLATION TO ADDRESS THE DIGITAL TELEPHONY ISSUE. WITHOUT ITS ENACTMENT, ONE OF OUR MOST EFFECTIVE WEAPONS AGAINST NATIONAL AND INTERNATIONAL DRUG TRAFFICKING, TERRORISM, ESPIONAGE, ORGANIZED CRIME, AND SERIOUS VIOLENT CRIMES WILL BE SEVERELY AND ADVERSELY IMPACTED.

THE ADMINISTRATION WANTS TO WORK WITH THE CONGRESS TO DEVELOP SUCH COMPREHENSIVE LEGISLATION. I WILL DESCRIBE IN THIS

TESTIMONY A DRAFT LEGISLATIVE PROPOSAL THAT HAS BEEN SHARED WITH YOU.

QUITE SIMPLY, THE PURPOSE OF THIS LEGISLATION (DRAFT) IS TO MAINTAIN TECHNOLOGICAL CAPABILITIES COMMENSURATE WITH EXISTING STATUTORY AUTHORITY -- THAT IS, TO PREVENT ADVANCED TELECOMMUNICATIONS TECHNOLOGY FROM REPEALING DE FACTO THE STATUTORY AUTHORITY ALREADY CONFERRED BY THE CONGRESS. THE PROPOSED LEGISLATION EXPLICITLY STATES THAT THE LEGISLATION DOES NOT ENLARGE OR REDUCE THE GOVERNMENT'S AUTHORITY TO LAWFULLY CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE AND INSTALL OR USE COURT-ORDERED PEN REGISTER OR TRAP AND TRACE DEVICES. THE ESSENCE OF THE DRAFT LEGISLATION IS TO CLARIFY AND MORE FULLY DEFINE THE NATURE AND EXTENT OF THE TELECOMMUNICATIONS SERVICE PROVIDER'S "ASSISTANCE" REQUIREMENT THAT WAS ENACTED BY CONGRESS IN 1970. THAT REQUIREMENT EVIDENCED CONGRESS' CLEAR INTENT THAT LAWFUL COURT ORDERS SHOULD NOT BE FRUSTRATED DUE TO A SERVICE PROVIDER'S FAILURE TO PROVIDE NEEDED TECHNOLOGICAL ASSISTANCE AND FACILITIES. THE PROPOSED LEGISLATION RELATES SOLELY TO ADVANCED TECHNOLOGY, NOT LEGAL AUTHORITY OR PRIVACY.

WE DID NOT COME TO SEEK LEGISLATION BLITHELY. FOR NEARLY FOUR YEARS, THE FBI HAS EXPENDED EVERY REASONABLE EFFORT TO ADDRESS THIS THREAT THROUGH NUMEROUS AND ONGOING MEETINGS WITH THE TELECOMMUNICATIONS INDUSTRY. HOWEVER, IT IS MY CONSIDERED JUDGEMENT, AND THAT OF THE ADMINISTRATION, THAT DIALOGUE ALONE, NO MATTER HOW WELL INTENDED, WILL NOT SOLVE THIS SERIOUS THREAT TO PUBLIC SAFETY. NONETHELESS, WE HAVE LISTENED AND LEARNED, AND

THE LEGISLATIVE PROPOSAL BEFORE YOU REPRESENTS, IN OUR ESTIMATION, THE ONLY PROPER APPROACH. ON THE ONE HAND, IT DEALS WITH THE ADVANCED TELEPHONY PROBLEM IN AN APPROPRIATELY COMPREHENSIVE FASHION -- IT DOES NOT SIMPLY "BAND-AID-OVER" PAST PROBLEMS, IT ALSO RESPONSIBLY DEALS WITH NEW SERVICES AND TECHNOLOGIES (SUCH AS PERSONAL COMMUNICATIONS SERVICES) THAT LIKELY WILL EMERGE IN THE NEXT FEW YEARS. ON THE OTHER HAND, THE DRAFT LEGISLATION IS NARROWLY FOCUSED AND COVERS ON ONLY THOSE SEGMENTS OF THE TELECOMMUNICATIONS INDUSTRY WHERE THE VAST MAJORITY OF THE PROBLEMS EXIST -- THAT IS, ON COMMON CARRIERS, A SEGMENT OF THE INDUSTRY WHICH HISTORICALLY HAS BEEN SUBJECT TO REGULATION. WE BELIEVE THE PROVISIONS OF THE ADMINISTRATION'S PROPOSAL ADDRESS THE PROBLEM IN A VERY RATIONAL FASHION. THEY INCLUDE CLEARLY STATED LAW ENFORCEMENT ELECTRONIC SURVEILLANCE REQUIREMENTS, SYSTEMS SECURITY PROVISIONS, A REASONABLE DEADLINE FOR COMPLIANCE, REQUIREMENTS FOR EQUIPMENT MANUFACTURER AND SUPPORT SERVICE PROVIDER COOPERATION, PROPER ENFORCEMENT AND PENALTY PROVISIONS, ONGOING GOVERNMENT CONSULTATION WITH COMMON CARRIERS TO FACILITATE COMPLIANCE, AND, IMPORTANTLY, A COMMITMENT ON THE PART OF THE FEDERAL GOVERNMENT TO PAY COMMON CARRIERS FOR REASONABLE CHARGES ASSOCIATED WITH ACHIEVING COMPLIANCE.

IMPORTANCE OF ELECTRONIC SURVEILLANCE

AS THE PROPOSED LEGISLATION IS CONSIDERED, IT IS ABSOLUTELY ESSENTIAL THAT CONGRESS UNDERSTAND THE IMPORTANCE OF ELECTRONIC SURVEILLANCE, AS WELL AS THE SEVERE HARM THAT WILL

OCCUR IF THIS CRITICAL LAW ENFORCEMENT TOOL IS LOST OR DIMINISHED.

THE NATION'S TELECOMMUNICATIONS NETWORKS ARE ROUTINELY USED IN THE COMMISSION OF SERIOUS CRIMINAL ACTIVITIES, INCLUDING TERRORISM AND ESPIONAGE. ORGANIZED CRIME GROUPS AND DRUG TRAFFICKING ORGANIZATIONS, WHICH ARE OFTEN HIGHLY STRUCTURED, RELY HEAVILY UPON TELECOMMUNICATIONS TO PLAN AND EXECUTE THEIR CRIMINAL ACTIVITIES AND HIDE THEIR ILLEGAL PROCEEDS. SIMILARLY, FOREIGN INTELLIGENCE SERVICE OFFICERS AND THEIR AGENTS CARRY OUT THEIR SPY AND OTHER CLANDESTINE MISSIONS THROUGH THESE NETWORKS.

CONGRESS RECOGNIZED THIS FACT A LITTLE OVER 25 YEARS AGO, WHEN IT PASSED THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968. TITLE III OF THAT ACT CONTAINED THE FIRST COMPREHENSIVE FEDERAL LEGISLATIVE REGIMEN REGARDING ELECTRONIC SURVEILLANCE FOR USE IN CRIMINAL INVESTIGATIONS. THE TITLE III LEGISLATION ESTABLISHED STRICT PROCEDURES FOR THE CONDUCT OF ELECTRONIC SURVEILLANCE BY FEDERAL, STATE AND LOCAL LAW ENFORCEMENT AUTHORITIES. THESE PROCEDURES ARE CAREFULLY ADHERED TO BY LAW ENFORCEMENT AND ARE RIGOROUSLY ENFORCED BY THE COURTS. TO DATE, THIRTY-SEVEN (37) STATES, PUERTO RICO, THE U.S. VIRGIN ISLANDS, AND THE DISTRICT OF COLUMBIA ALSO HAVE ENACTED ELECTRONIC SURVEILLANCE STATUTES. IN 1992, A TOTAL OF 919 TITLE III ORDERS, AS WELL AS AN ESTIMATED 9,000 PEN REGISTER ORDERS, WERE AUTHORIZED FOR ALL FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT AGENCIES. ON AVERAGE, APPROXIMATELY TWO-THIRDS OF THE CRIMINAL-RELATED ELECTRONIC SURVEILLANCE CONDUCTED IN THE UNITED STATES IS

CARRIED OUT BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES. AS MANDATED IN THE TITLE III LEGISLATION, ELECTRONIC SURVEILLANCE MAY BE USED ONLY IN THE INVESTIGATION OF SERIOUS FELONY OFFENSES AND ONLY WHEN OTHER INVESTIGATIVE TECHNIQUES WILL NOT WORK OR ARE TOO DANGEROUS.

IN 1978, CONGRESS ESTABLISHED AN ANALOGOUS FEDERAL ELECTRONIC SURVEILLANCE REGIMEN FOR USE IN COUNTER-INTELLIGENCE, COUNTER-TERRORISM, AND COUNTER-ESPIONAGE INVESTIGATIONS, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA). PURSUANT TO FISA, THE U. S. GOVERNMENT IS AUTHORIZED TO INTERCEPT COMMUNICATIONS OF INDIVIDUALS WHO POSE A THREAT TO THE NATIONAL SECURITY, AND INCLUDE THOSE IN FURTHERANCE OF ESPIONAGE AND TERRORISM.

SINCE THE PASSAGE OF TITLE III, LAW ENFORCEMENT HAS FOUND ELECTRONIC SURVEILLANCE TO BE ONE OF ITS MOST IMPORTANT INVESTIGATIVE TECHNIQUES -- IF NOT THE MOST IMPORTANT. USE OF THE TECHNIQUE HAS BEEN CRITICAL IN FIGHTING ORGANIZED CRIME, DRUG TRAFFICKING, PUBLIC CORRUPTION, FRAUD, TERRORISM, AND VIOLENT CRIME, AND IN SAVING NUMEROUS INNOCENT LIVES. IN MANY OF THESE CASES, THE CRIMINAL ACTIVITY UNDER INVESTIGATION COULD NEVER HAVE BEEN FULLY DETECTED, PREVENTED, ADEQUATELY INVESTIGATED, OR SUCCESSFULLY PROSECUTED WITHOUT THE USE OF EVIDENCE DERIVED FROM COURT-ORDERED ELECTRONIC SURVEILLANCE. SIMILARLY, FISA-BASED INTELLIGENCE INFORMATION MAKES A SIGNIFICANT AND IMPORTANT CONTRIBUTION TO U. S. COUNTER-INTELLIGENCE, COUNTER-TERRORISM, AND COUNTER-ESPIONAGE EFFORTS.

AS YOU ARE AWARE, ELECTRONIC SURVEILLANCE IS A CRITICAL TOOL USED TO DETECT AND OBTAIN EVIDENCE OF, AND OFTEN PREVENT, THE MOST SERIOUS, AND OFTEN MOST VIOLENT, CRIMINAL ACTIVITY CONFRONTING OUR SOCIETY. AS SHOWN IN THE ATTACHED EXHIBIT, ALTHOUGH USED SPARINGLY, ELECTRONIC SURVEILLANCE HAS PROVED TO BE AN EXTREMELY EFFECTIVE INVESTIGATIVE TECHNIQUE FOR LAW ENFORCEMENT AND HAS LED TO THE CONVICTIONS OF THOUSANDS OF DANGEROUS PERSONS INVOLVED IN DRUG TRAFFICKING, ORGANIZED CRIME, VIOLENT CRIME, KIDNAPING, CRIMES AGAINST CHILDREN, AND PUBLIC CORRUPTION. BECAUSE A SUBSTANTIAL NUMBER OF PROSECUTIONS ARE ONGOING, THE EXACT NUMBER OF CONVICTIONS RESULTING FROM THESE WIRETAPS INCREASES ALMOST DAILY; HOWEVER, THIS KEY INVESTIGATIVE TECHNIQUE HAS PROVEN TO BE INCOMPARABLY EFFECTIVE, WITH THE RESULTING EVIDENCE SECURING THE CONVICTION OF OVER 22,000 DANGEROUS FELONS OVER THE PAST DECADE.

PUBLIC SAFETY: PREVENTING CRIMES AND SAVING HUMAN LIVES

ALTHOUGH ELECTRONIC SURVEILLANCE IS EXTREMELY IMPORTANT AS AN INVESTIGATIVE TOOL TO ACQUIRE EVIDENCE, FREQUENTLY IT HAS BEEN ESSENTIAL IN PREVENTING CRIMES FROM OCCURRING AND IN SAVING HUMAN LIFE. ELECTRONIC SURVEILLANCE HAS BEEN ESSENTIAL IN PREVENTING MURDERS; IN SAVING HUMAN LIFE PUT AT RISK THROUGH PLANNED TERRORIST ATTACKS; IN DISMANTLING ENTRENCHED ORGANIZED CRIME GROUPS WHICH SEVERELY HARM THE ECONOMY THROUGH EXTORTION, FRAUD, AND CORRUPTION; AND IN ATTACKING THE MAJOR NATIONAL AND INTERNATIONAL DRUG IMPORTATION AND DISTRIBUTION CARTELS AND

NETWORKS WHOSE ACTIVITIES RAVAGE SOCIETY AND CAUSE INCALCULABLE PERSONAL AND ECONOMIC INJURY IN THE UNITED STATES.

ORGANIZED CRIME INVESTIGATIONS

THE ACTIVITIES OF ORGANIZED CRIME ARE EXTREMELY HARMFUL TO AMERICAN BUSINESS AND INDUSTRY, LABOR UNIONS, AND INDIVIDUALS IN OUR SOCIETY. ELECTRONIC SURVEILLANCE IS INDISPENSABLE IN COMBATTING ORGANIZED CRIME. INDEED, THE FBI'S ORGANIZED CRIME/DRUGS SECTION REPORTS THAT EVERY MAJOR FBI ORGANIZED CRIME INVESTIGATION HAS RELIED UPON ELECTRONIC SURVEILLANCE. IN APRIL, 1988, THE IMPORTANCE OF THE ELECTRONIC SURVEILLANCE TECHNIQUE WAS FORMALLY RECOGNIZED IN HEARING TESTIMONY BEFORE THE U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, GOVERNMENTAL AFFAIRS COMMITTEE, ON ORGANIZED CRIME: "25 YEARS AFTER VALACHI." IN PARTICULAR, DAVID C. WILLIAMS, OFFICE OF SPECIAL INVESTIGATIONS, GENERAL ACCOUNTING OFFICE, TESTIFIED THAT "ELECTRONIC SURVEILLANCE IS ANOTHER TOOL THAT HAS BEEN OF GREAT VALUE TO THE LAW ENFORCEMENT COMMUNITY TO COMBAT THE LA COSA NOSTRA (LCN) [ORGANIZED CRIME FAMILIES]. EVIDENCE GATHERED THROUGH ELECTRONIC SURVEILLANCE ... HAS HAD A DEVASTATING IMPACT ON ORGANIZED CRIME." (EMPHASIS ADDED)

LEFT UNCHECKED, ORGANIZED CRIME EXERTS A CHOKE HOLD ON SOCIETY, AND THE SUBSEQUENT COST TO BUSINESS AND INDUSTRY IS DRAMATIC. GREATER DETAIL CONCERNING AREAS OF ORGANIZED CRIME'S PENETRATION IN BUSINESS AND LABOR UNIONS AND EXAMPLES OF THE SUCCESSFUL USE OF ELECTRONIC SURVEILLANCE TO EFFECTIVELY COMBAT

THE ADVERSE IMPACT OF ORGANIZED CRIME UPON THE ECONOMY AND SOCIETY IS SET FORTH IN THE ATTACHED APPENDIX.

IN THE 1986 REPORT, THE IMPACT: ORGANIZED CRIME TODAY, THE PRESIDENT'S COMMISSION ON ORGANIZED CRIME UTILIZED THE WHARTON BUSINESS SCHOOL'S LONG-TERM MODEL OF THE UNITED STATES ECONOMY TO ESTIMATE THE COST OF ORGANIZED CRIME ON THE ECONOMY, IN TERMS OF SUSTAINED HIGHER PRICES AND THE CONTINUED UNDERPAYMENT OF TAXES TO THE FEDERAL GOVERNMENT. THE COMMISSION CONCLUDED THAT THE ESTIMATED ECONOMY-WIDE IMPACT OF ORGANIZED CRIME, EXCLUDING DRUG TRAFFICKING ORGANIZATIONS, WAS AS FOLLOWS:

- O U. S. OUTPUT WAS REDUCED BY \$18.2 BILLION IN 1986 DOLLARS.
- O U. S. EMPLOYMENT WAS REDUCED BY 414,000 JOBS.
- O CONSUMER PRICES WERE HIGHER BY 0.3 PERCENT; AND,
- O PER CAPITA PERSONAL INCOME WAS LOWER BY \$77.22, MEASURED IN 1986 DOLLARS.

FBI ORGANIZED CRIME PROGRAM MANAGERS STATE: "THE LOSS OR IMPAIRMENT OF THE CAPABILITY TO CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE WOULD CATASTROPHICALLY IMPAIR FEDERAL AND STATE LAW ENFORCEMENT AGENCIES' ABILITY TO EFFECTIVELY INVESTIGATE ORGANIZED CRIMINAL GROUPS." (EMPHASIS ADDED)

ALTHOUGH NO STUDIES HAVE BEEN CONDUCTED TO MEASURE THE PRECISE ECONOMIC AND SOCIETAL BENEFITS DERIVED FROM THE SUCCESSES OF FEDERAL AND STATE CRIMINAL LAW ENFORCEMENT AGENCIES AGAINST ORGANIZED CRIME, IT IS EVIDENT THAT AN ABATEMENT IN SUCCESSFUL ORGANIZED CRIME INVESTIGATIONS, DUE TO THE LOSS OR IMPAIRMENT OF ONE OF LAW ENFORCEMENT'S MOST IMPORTANT TOOLS -- THE COURT-

ORDERED ELECTRONIC SURVEILLANCE TECHNIQUE -- WOULD ALLOW ORGANIZED CRIME'S DAMAGE TO THE U.S. ECONOMY TO BECOME SUBSTANTIALLY GREATER.

NARCOTICS AND DANGEROUS DRUGS

THE GREATEST USE OF ELECTRONIC SURVEILLANCE BY LAW ENFORCEMENT RELATES TO THE FEDERAL AND STATE GOVERNMENTS' "WAR ON DRUGS." INFORMATION REPORTED IN THE FEDERAL WIRETAP REPORT BY THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS INDICATES THAT ALMOST TWO THIRDS (62%) OF ALL TITLE III GOVERNMENTAL ELECTRONIC SURVEILLANCE IS DEVOTED TO THIS CRITICAL NATIONAL PROBLEM. THE MAJOR DRUG TRAFFICKING ORGANIZATIONS WHICH IMPORT AND DISTRIBUTE DRUGS, LIKE ANY BUSINESS OR ORGANIZATION, RELY HEAVILY ON TELECOMMUNICATIONS TO COORDINATE AND CARRY OUT THESE CRIMINAL ACTIVITIES AND TO "LAUNDER" THE BILLIONS OF DOLLARS IN ILLEGAL DRUG PROCEEDS. ACCORDINGLY, FEDERAL AND STATE LAW ENFORCEMENT MAXIMIZE THEIR LIMITED RESOURCES AND FOCUS ELECTRONIC SURVEILLANCE EFFORTS ON THE MAIN DRUG IMPORTATION AND DISTRIBUTION NETWORKS.

ALTHOUGH FIGURES ABOUND WITH REGARD TO THE BILLIONS OF DOLLARS IN FEDERAL, STATE, AND LOCAL SEIZURES OF DRUGS, ILLEGAL DRUG PROCEEDS (CASH AND OTHER ASSETS), ETC., THE FUNDAMENTAL HARM TO SOCIETY IS INCALCULABLE. IT IS IMPOSSIBLE TO FULLY IDENTIFY THE HUMAN, ECONOMIC, AND OTHER SOCIETAL HARM BROUGHT ABOUT BY DRUG DEPENDENCY AND ADDICTION. IN ONE ATTEMPT TO QUANTIFY CERTAIN FACETS OF THIS HARM, THE U. S. PUBLIC HEALTH SERVICE HAS

ESTIMATED THE HEALTH, LABOR, AND CRIME COSTS OF DRUG ABUSE AT \$58.3 BILLION IN 1988, EXCLUSIVE OF THE VALUE OF THE DRUGS THEMSELVES. D. RICE, ET AL., U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, THE ECONOMIC COST OF ALCOHOL AND DRUG ABUSE AND MENTAL ILLNESS: 1985, TABLE 1, PAGE 2 (1990). A 1992 U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES' STUDY ESTIMATES THE 1992 COSTS OF DRUG ABUSE IN THE UNITED STATES TO BE \$168 BILLION OR \$675 PER PERSON. APPROXIMATELY \$40 BILLION DOLLARS A YEAR ARE SPENT BY USERS TO PROCURE THESE DRUGS.

ULTIMATELY, THE ECONOMIC, SOCIETAL, AND PERSONAL HARM OF DRUG TRAFFICKING IS ALSO MEASURED IN DAILY "DRIVE-BY SHOOTINGS" IN NEIGHBORHOOD STREETS (WHERE THE BLOOD OF INNOCENT CHILDREN IS SPILLED NEXT TO THAT OF NEIGHBORHOOD DRUG LIEUTENANTS); SUBSTANTIALLY INCREASED CRIME SUCH AS THEFTS, ROBBERIES, AND MURDERS BROUGHT ABOUT BY DRUG USE; VIOLENT "TURF BATTLES" TO CONTROL DRUG DISTRIBUTION; LOST PRODUCTIVITY; EMPLOYEE ABSENCE; EXTENSIVE AND EXPENSIVE HEALTH CARE WITH DRUG CASUALTIES THAT CLOG OUR HOSPITAL EMERGENCY ROOMS; AS WELL AS THE SAD OCCURRENCE OF A GENERATION OF DRUG-DEPENDANT BABIES.

THE DRUGS WHICH ARE MOST RESPONSIBLE FOR THIS PROBLEM ARE ESSENTIALLY THOSE (SUCH AS COCAINE AND HEROIN) WHICH MUST BE IMPORTED INTO THE UNITED STATES, GENERALLY BY HIGHLY ORGANIZED CRIMINAL GROUPS, DRUG TRAFFICKING CARTELS AND OTHER SYNDICATES, AND THEREAFTER TRANSPORTED OVER VAST DISTANCES AND DISTRIBUTED WIDELY WITHIN THE UNITED STATES. THESE CARTELS AND ORGANIZATIONS RELY HEAVILY ON TELECOMMUNICATIONS TO CARRY OUT THEIR ILLEGAL

ACTIVITIES. THE UNITED STATES GOVERNMENT ESTIMATES THAT EVERY YEAR OVER 400 METRIC TONS OF COCAINE AND APPROXIMATELY 18 TO 22 METRIC TONS OF HEROIN ARE SMUGGLED INTO THE UNITED STATES.

ELECTRONIC SURVEILLANCE IS CRITICAL IN THE MONITORING OF THE DRUG TRAFFICKERS' "COMMUNICATIONS NETWORKS," PROVIDING LAW ENFORCEMENT WITH THE ABILITY TO IDENTIFY ALL OF THE ORGANIZATION'S DRUG TRAFFICKERS AND THEIR ILLEGAL PROCEEDS, AS WELL AS ULTIMATELY IN DISMANTLING THOSE NATIONAL AND INTERNATIONAL DRUG TRAFFICKING ORGANIZATIONS. SINCE NATIONAL AND INTERNATIONAL DRUG CHIEFTAINS AND LOCAL DRUG "KINGPINS" DO NOT APPEAR AT DRUG BUYS OR SHIPMENTS, ELECTRONIC SURVEILLANCE ORDINARILY PROVIDES THE ONLY RELIABLE METHOD OF LINKING THE DRUG ORGANIZATIONS' LEADERS WITH THE ENTERPRISE, AND FREQUENTLY PROVIDES THE ONLY DIRECT AND PERSUASIVE EVIDENCE THAT WILL SUPPORT A CRIMINAL CONVICTION. CONSEQUENTLY, INFORMATION DERIVED FROM ELECTRONIC SURVEILLANCE IS ESSENTIAL IN SUCCESSFULLY PROSECUTING THOSE AT THE EXECUTIVE LEVEL OF THE DRUG TRADE.

RECENT EXAMPLES OF THE CRITICAL ROLE OF ELECTRONIC SURVEILLANCE IN DRUG INVESTIGATIONS ARE:

- IN A NEW YORK CITY-BASED DRUG TRAFFICKING INVESTIGATION, AN FBI-LED TASK FORCE CONDUCTED OVER 55 SEPARATE ELECTRONIC SURVEILLANCES (WITH NUMEROUS EXTENSIONS). AS OF MARCH 1993, THIS INVESTIGATION HAS RESULTED IN 222 ARRESTS; 167 CONVICTIONS; THE DISMANTLING OF 15 MAJOR DRUG TRAFFICKING ORGANIZATIONS/GANGS, AND THE IDENTIFICATION OF 30

OTHERS; THE RESOLUTION OF SOME 40 NEW YORK AREA HOMICIDES, INCLUDING THE ASSASSINATION OF A NYCPD POLICE OFFICER AND A NEW YORK STATE PAROLE OFFICER. SUBSTANTIAL QUANTITIES OF DRUGS HAVE BEEN SEIZED AND OVER \$8 MILLION IN ASSETS HAVE BEEN SEIZED. THESE EFFORTS HAVE RESULTED IN A SUBSTANTIAL REDUCTION IN DRUG-RELATED HOMICIDES.

- THE APRIL, 1992, DRUG RAID IN MIAMI THAT NETTED 15,000 POUNDS OF COCAINE WHICH WAS BASED ON INFORMATION DEVELOPED THROUGH ELECTRONIC SURVEILLANCE. EVIDENCE DERIVED FROM ELECTRONIC SURVEILLANCE WAS INSTRUMENTAL IN IDENTIFYING THE NETWORK'S LEADER AMONG THE 22 DEFENDANTS ARRESTED;
- THE 1991 DEA HERRERA DRUG INVESTIGATION IN NEW YORK CITY RESULTING IN THE SUCCESSFUL PROSECUTION OF 51 DEFENDANTS, INCLUDING KEY INDIVIDUALS LINKED TO THE CALI DRUG CARTEL, RELIED UPON ELECTRONIC SURVEILLANCE.

WITHOUT THE USE OF ONE OF FEDERAL AND STATE LAW ENFORCEMENT'S MOST IMPORTANT ENFORCEMENT TOOLS -- ELECTRONIC SURVEILLANCE -- THE VOLUME OF DRUGS WOULD DRAMATICALLY INCREASE AND THE EASE AND MEANS OF DRUG IMPORTATION AND DISTRIBUTION WOULD BE DRAMATICALLY ENHANCED THROUGH THE DRUG TRAFFICKERS' UNFETTERED USE OF THEIR DRUG "COMMUNICATIONS NETWORKS."

PUBLIC CORRUPTION AND GOVERNMENTAL FRAUD

INTEGRITY IN GOVERNMENT IS A KEYSTONE IN ANY DEMOCRACY. CORRUPTION AND FRAUD UNDERMINE THE PUBLIC'S RESPECT AND CONFIDENCE IN GOVERNMENTAL INSTITUTIONS AND IN THE RULE OF LAW. BY THEIR NATURE, CORRUPTION AND FRAUD CAN ONLY FLOURISH IN SECRECY, HIDDEN FROM PUBLIC VIEW. AS A RESULT, NORMAL, OVERT INVESTIGATIVE TECHNIQUES ARE IN MOST CASES TOTALLY UNAVAILING. HENCE, AS A GENERAL PROPOSITION, LAW ENFORCEMENT HAS FOUND THAT ELECTRONIC SURVEILLANCE AND UNDERCOVER OPERATIONS ARE CRITICAL MEANS TO EFFECTIVELY DETECT, INVESTIGATE, AND PROSECUTE THESE INSIDIOUS CRIME PROBLEMS.

IN SEVERAL RECENT JUDICIAL CORRUPTION INVESTIGATIONS, ELECTRONIC SURVEILLANCE EVIDENCE HAS DIRECTLY LED TO THE CONVICTION OF TWO FEDERAL DISTRICT COURT JUDGES AND, IN ANOTHER CASE, TO THE INDICTMENT OR PLEA OF SIX CURRENT OF FORMER DADE COUNTY, FLORIDA, STATE JUDGES (FOUR CONVICTED, ONE ACQUITTED, AND ONE TO BE RETRIED) AND FIVE ATTORNEYS (ALL CONVICTED) FOR EXTORTION AND CASE FIXING. WITHIN THE RECENT PAST, ELECTRONIC SURVEILLANCE HELPED BUILD A CORRUPTION CASE INVOLVING THE POLICE FORCE OF A LARGE MIDWESTERN CITY WHICH INCLUDED EXTORTION AND PROTECTION FOR GAMBLING AND NARCOTICS DISTRIBUTION. THIRTY POLICE OFFICERS AND 17 OTHERS WERE INDICTED, AND 46 OF THE 47 EITHER PLED OR HAVE BEEN FOUND GUILTY.

ELECTRONIC SURVEILLANCE HAS PLAYED AN INDISPENSABLE ROLE IN COUNTERING GOVERNMENTAL FRAUD. FOR EXAMPLE, THE "ILL-WIND" INVESTIGATION (WHICH WAS LARGELY BASED UPON 36 SEPARATE

COURT-ORDERED ELECTRONIC SURVEILLANCES CONDUCTED ACROSS THE UNITED STATES) HAS HAD A TREMENDOUS IMPACT UPON FRAUD AND ABUSE BOTH WITHIN THE GOVERNMENT AND WITHIN THE INDUSTRIES THAT CONTRACT WITH THE GOVERNMENT. TO DATE, THE "ILL-WIND" INVESTIGATION HAS RESULTED IN 65 CONVICTIONS (INCLUDING HIGH-LEVEL DEPARTMENT OF DEFENSE OFFICIALS AND EIGHT CORPORATIONS), SANCTIONS AGAINST CONTRACTORS, AND OVER A QUARTER OF A BILLION DOLLARS (\$271,000,000) IN FINES, RESTITUTIONS, AND RECOVERIES ORDERED. EVIDENCE NECESSARY TO OBTAIN THESE CONVICTIONS, FINES, RECOVERIES, ETC., WOULD HAVE BEEN IMPOSSIBLE TO OBTAIN WITHOUT ELECTRONIC SURVEILLANCE.

THE HIGH COST OF HEALTH CARE IN THE UNITED STATES IS A PROBLEM OF TREMENDOUS IMPORTANCE TO OUR SOCIETY. UNFORTUNATELY, BILLIONS OF HEALTH CARE DOLLARS ARE WASTED THROUGH FRAUD. WITH REGARD TO HEALTH CARE FRAUD, ELECTRONIC SURVEILLANCE HAS BEEN EXTREMELY IMPORTANT. IN 1993, IN NEW YORK, ELECTRONIC SURVEILLANCE OF HARDWIRED (FIXED) AND CELLULAR (MOBILE) TELEPHONES PRODUCED CRITICAL EVIDENCE IN A CASE INVOLVING WIDESPREAD MEDICARE/MEDICAID FRAUD CARRIED OUT BY NUMEROUS PHARMACIES AND PHARMACISTS. SEVENTY-NINE (79) INDIVIDUALS, INCLUDING 38 PHARMACISTS, WERE INDICTED. TO DATE, 79 INDIVIDUALS HAVE BEEN CONVICTED OR PLED GUILTY AND \$6.6 MILLION IN ASSETS ARE SUBJECT TO SEIZURE AND FORFEITURE. SIMILARLY, IN 1993, IN DETROIT, ELECTRONIC SURVEILLANCE WAS INSTRUMENTAL IN INVESTIGATING AND PROSECUTING A WIDE-SPREAD MEDICARE/MEDICAID FRAUD PERPETRATED BY NUMEROUS PHARMACIES AND PHARMACISTS.

THIRTY-TWO (32) PHARMACIES/PHARMACISTS WERE PROSECUTED, AND \$4 MILLION IN CRIMINAL FORFEITURES ARE EXPECTED TO FOLLOW. THE FBI ESTIMATES THAT THE HEALTH CARE FRAUD IN EACH OF THE FOREGOING CASES ALONE RANGED IN THE TENS OF MILLIONS OF DOLLARS.

RECENTLY, A MAJOR GOVERNMENTAL FRAUD CASE INVOLVING RUSSIAN EMIGRE ORGANIZED CRIME AND THE GAMBINO LCN ORGANIZED CRIME FAMILY WAS SUCCESSFULLY INVESTIGATED THROUGH THE USE OF AN UNDERCOVER OPERATION AND THE SUBSTANTIAL USE OF ELECTRONIC SURVEILLANCE TO INTERCEPT A NUMBER OF CELLULAR TELEPHONES. THE CRIMINAL SCHEME INVOLVED DEFRAUDING THE FEDERAL GOVERNMENT AND STATE GOVERNMENTS OF MOTOR FUEL TAXES. THE DEPARTMENT OF JUSTICE ESTIMATES THAT MORE THAN \$1 BILLION IN FEDERAL EXCISE TAX, FUNDS THAT ARE EARMARKED FOR THE HIGHWAY TRUST FUND FOR USE IN MAINTAINING THE NATION'S HIGHWAY INFRASTRUCTURE, IS ILLEGALLY "SKIMMED" EACH YEAR. AN INDICTMENT IN THE FOREGOING CASE HAS BEEN RETURNED IN NEWARK, CHARGING 14 INDIVIDUALS WITH DEFRAUDING THE FEDERAL GOVERNMENT AND THE STATE OF NEW JERSEY OUT OF MORE THAN \$60 MILLION IN TAX REVENUES AND WITH LAUNDERING \$66.2 MILLION RESULTING IN 4 CONVICTIONS TO DATE. A NUMBER OF THE SUBJECTS IN THIS INVESTIGATION UTILIZED CELLULAR TELEPHONES AND FREQUENTLY CHANGED CELLULAR TELEPHONES IN AN EFFORT TO THWART ELECTRONIC SURVEILLANCE. THE INTERCEPTED TELEPHONE CONVERSATIONS WERE CRITICAL TO PROVING THE INVOLVEMENT OF THE LCN IN THIS RUSSIAN ORGANIZED CRIME FRAUD AGAINST FEDERAL AND STATE GOVERNMENTS.

TERRORISM

A SIGNIFICANT NUMBER OF TERRORIST ACTS, INCLUDING BOMBINGS AND MURDERS, HAVE BEEN PREVENTED THROUGH THE EFFECTIVE USE OF ELECTRONIC SURVEILLANCE. MANY OF THESE TERRORIST ACTS, IF NOT PREVENTED, LIKELY WOULD HAVE HAD SUBSTANTIAL NATIONAL AND/OR INTERNATIONAL IMPLICATIONS. IN ONE CASE, THE BOMBING OF A FOREIGN CONSULATE IN THE UNITED STATES WAS PREVENTED, AND THE ELECTRONIC SURVEILLANCE EVIDENCE WAS USED IN THE SUBSEQUENT CONVICTION OF THE PRINCIPALS. IN ANOTHER CASE, A TERRORIST ROCKET ATTACK AGAINST A UNITED STATES ALLY BY A FOREIGN-BASED TERRORIST GROUP WAS THWARTED, AND THE ELECTRONIC SURVEILLANCE-BASED INVESTIGATION LED TO THE ARREST OF THE PRINCIPALS AND THE PREVENTION OF THE LOSS OF LIFE OF SCORES OF PERSONS.

IN 1986, THE EFFORTS OF THE VIOLENT EL RUKN CHICAGO STREET GANG TO SHOOT DOWN A COMMERCIAL AIRLINER WITHIN THE UNITED STATES WITH A STOLEN MILITARY WEAPON SYSTEM WAS THWARTED THROUGH ELECTRONIC SURVEILLANCE. THE FBI'S PREVENTION OF THIS ACT OF STATE-SPONSORED TERRORISM, FINANCED BY LIBYA, WHICH WOULD HAVE COST SEVERAL HUNDRED U.S. LIVES, WAS SINGULARLY ATTRIBUTABLE TO THE USE OF ELECTRONIC SURVEILLANCE -- BUT FOR THE AVAILABILITY OF THIS TECHNIQUE, ANOTHER PAN AM 103 DISASTER COULD HAVE OCCURRED ON AMERICAN SOIL.

MORE RECENTLY, IN 1993, ELECTRONIC SURVEILLANCE CONTRIBUTED TO THE INDICTMENT OF INDIVIDUALS IN THE ST. LOUIS-BASED CELL OF THE ABU NIDAL ORGANIZATION ON RICO CHARGES OF MURDER, CONSPIRACY TO COMMIT MURDER, AND CONSPIRACY TO BOMB THE

ISRAELI EMBASSY IN WASHINGTON, D.C. IN 1990, FOREIGN-BASED TERRORISTS WERE PREVENTED FROM ACQUIRING A STINGER SURFACE-TO-AIR MISSILE WHICH WAS TO BE EMPLOYED IN A TERRORIST ACT WHEREIN NUMEROUS PEOPLE WOULD UNDOUBTEDLY HAVE BEEN KILLED. ALSO, IN 1989, AS A DIRECT RESULT OF COURT-ORDERED ELECTRONIC SURVEILLANCE IN A TERRORIST-RELATED MATTER, INFORMATION WAS OBTAINED WHICH RESULTED IN THE CONVICTION OF TWO INDIVIDUALS FOR THE BRUTAL HOMICIDE OF THEIR 16-YEAR OLD DAUGHTER.

BEYOND THE FOREGOING INSTANCES, OVER THE LAST DECADE NUMEROUS OTHER TERRORIST-RELATED INVESTIGATIONS HAVE UTILIZED ELECTRONIC SURVEILLANCE TO: PREVENT A ROCKET ATTACK AGAINST AN FBI FIELD OFFICE; PREVENT AN ATTACK ON A NUCLEAR POWER FACILITY; SOLVE SEVERAL MURDERS; IDENTIFY THE PERPETRATORS OF A \$7,000,000 ARMED ROBBERY; AND SOLVE AND PREVENT SEVERAL BOMBINGS BY ANTI-CASTRO GROUPS IN MIAMI, FLORIDA.

VIOLENT CRIME

MANY VIOLENT CRIMES, INCLUDING MURDER, HAVE BEEN SOLVED AND A SIGNIFICANT NUMBER PREVENTED BY LAW ENFORCEMENT'S "REAL TIME" RESPONSE TO, AND PREVENTIVE ACTIONS TAKEN AS A RESULT OF CONVERSATIONS INTERCEPTED THROUGH ELECTRONIC SURVEILLANCE. ELECTRONIC SURVEILLANCE HAS BEEN USED IN COMBATTING AND SOLVING VIOLENT CRIMES PERPETRATED BY BOTH ORGANIZED CRIMINAL GROUPS AND BY INDIVIDUALS. THE FOLLOWING ARE RECENT EXAMPLES OF CASES IN WHICH ELECTRONIC SURVEILLANCE HAS BEEN CRUCIAL IN SAVING LIVES OR PREVENTING VIOLENT ACTS FROM OCCURRING:

- CONVERSATIONS OF MEMBERS OF THE NEW ENGLAND LCN FAMILY WERE INTERCEPTED WHEREIN THE MURDERS OF THREE INDIVIDUALS WERE PLANNED, AND DETAILS CONCERNING SIX PRIOR MURDERS WERE DISCUSSED. OF THE THREE PLANNED MURDERS, TWO WERE PREVENTED BY THE FBI; THE THIRD COULD NOT BE PREVENTED BECAUSE OF AN INABILITY TO LOCATE THE VICTIM PRIOR TO HIS MURDER.
- ONE OF THE MOST VIOLENT ASIAN ORGANIZED CRIME GANGS ACTIVE IN THE NEW YORK CITY AREA IS THE GREEN DRAGONS, WHICH, AS OF 1990, WAS DIRECTED TELEPHONICALLY BY KIN FEI WONG FROM THE PEOPLE'S REPUBLIC OF CHINA. THE GREEN DRAGONS GANG PERPETRATED MURDER, ARMED ROBBERIES, HOME INVASIONS, EXTORTION, DRUG TRAFFICKING, AND WERE INVOLVED IN THE OBSTRUCTION OF JUSTICE. COURT-ORDERED ELECTRONIC SURVEILLANCE PROVIDED EVIDENCE OF THESE CRIMES AND ALSO DISCLOSED THAT THE GREEN DRAGONS WERE ABOUT TO ENGAGE IN A "SHOOT OUT" WITH A RIVAL ASIAN GANG. IMMEDIATELY ACTING UPON THIS INFORMATION, 16 MEMBERS OF THE GROUP WERE ARRESTED BY FBI AGENTS AND POLICE OFFICERS AND AN IMMINENT VIOLENT CONFRONTATION AND LOSS OF LIFE WERE PREVENTED. BASED PARTLY UPON EVIDENCE DERIVED FROM ELECTRONIC SURVEILLANCE, ALL DEFENDANTS WERE FOUND GUILTY OF RACKETEERING, RACKETEERING CONSPIRACY, AND NUMEROUS SUBSTANTIVE COUNTS WHICH INCLUDED MURDER, KIDNAPPING, HOME

INVASIONS, ARMED ROBBERY, EXTORTION AND BRIBERY OF A PUBLIC OFFICIAL.

- IN 1991, THE MURDER OF A UNITED STATES COURT OF APPEALS JUDGE WAS SOLVED AND A CONVICTION OBTAINED BASED IN PART UPON ELECTRONIC SURVEILLANCE INFORMATION.
- IN A NOTABLE 1990 "SEXUAL EXPLOITATION" OF CHILDREN CASE WHICH RELIED HEAVILY UPON ELECTRONIC SURVEILLANCE, THE FBI THWARTED TWO INDIVIDUALS WHO WERE CONSPIRING TO ABDUCT, TORTURE, AND KILL A TEENAGE BOY FOR THE PURPOSE OF MAKING A "SNUFF MURDER" FILM.
- IN 1993, IN GREENE COUNTY, OHIO, A 10-YEAR OLD TRIPLE HOMICIDE WAS FINALLY SOLVED, AND EVIDENCE CRITICAL FOR SUCCESSFUL PROSECUTION WAS OBTAINED THROUGH THE USE OF ELECTRONIC SURVEILLANCE. THE VICTIMS, TWO MEN AND A PREGNANT WOMAN, HAD BEEN SHOT EXECUTION-STYLE, AND SUBSEQUENTLY THEIR THROATS HAD BEEN SLIT AND THEIR SKULLS HAD BEEN CRUSHED BY THE MURDERERS.

FOREIGN COUNTERINTELLIGENCE (FCI)

BECAUSE ANY DISCUSSION OF THE IMPORTANCE OF FISA-BASED ELECTRONIC SURVEILLANCE WOULD INVOLVE HIGHLY SENSITIVE MATTERS AND HIGHLY CLASSIFIED INFORMATION, SUFFICE IT TO SAY THAT INFORMATION DERIVED FROM FISA ELECTRONIC SURVEILLANCE IS CRITICAL TO THE PRESIDENT OF THE UNITED STATES, THE NATIONAL SECURITY COUNCIL, THE INTELLIGENCE COMMUNITY, THE DEPARTMENT OF DEFENSE, AND THE STATE DEPARTMENT. SUCH INFORMATION IS OF GREAT

IMPORTANCE AS OUR NATION'S LEADERS ESTABLISH POLICY AND SAFEGUARD THE NATION'S DEFENSE AND NATIONAL SECURITY.

CONSEQUENCES OF THE LOSS OF ELECTRONIC SURVEILLANCE

AS INDICATED ABOVE, SOCIETY'S MOST DANGEROUS CRIMINAL ORGANIZATIONS AND GROUPS RELY HEAVILY UPON THE USE OF TELECOMMUNICATIONS. ADDITIONALLY, SUCH ORGANIZATIONS TEND TO TAKE ADVANTAGE OF ADVANCED TELECOMMUNICATIONS AND SERVICES TO CONDUCT AND CARRY OUT THEIR ILLEGAL ACTIVITIES. EVIDENCE IS DEVELOPING THAT INDICATES CRIMINAL ORGANIZATIONS ARE ALSO INCREASINGLY LOOKING FOR WAYS TO AVOID LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE BY FREQUENTLY CHANGING THEIR TELECOMMUNICATIONS DEVICES AND TELEPHONE NUMBERS, MODIFYING AND REPROGRAMMING THEIR CELLULAR TELEPHONE IDENTIFICATION NUMBERS AND CODES, AND UTILIZING CALL-FORWARDING FEATURES, ETC. INCREASED USE OF CELLULAR TELEPHONES, CALL-FORWARDING FEATURES, AND EVASIVE EFFORTS HAVE ALREADY HAD A NEGATIVE IMPACT UPON ELECTRONIC SURVEILLANCE AND LAW ENFORCEMENT'S ABILITY TO PROTECT THE PUBLIC AND EFFECTIVELY ENFORCE THE LAW. THE FOREGOING CASES DIRECTLY DEMONSTRATE THE PUBLIC SAFETY AND LAW ENFORCEMENT BENEFITS DIRECTLY ATTRIBUTABLE TO THE USE OF ELECTRONIC SURVEILLANCE. THEY ALSO INDICATE THE KIND OF NEGATIVE IMPACTS AND SOCIETAL HARMS THAT WOULD RESULT IF THERE WERE A LOSS OR DIMINISHMENT OF THE ELECTRONIC SURVEILLANCE TECHNIQUE. INDEED, LOSS OF A VIABLE, EFFECTIVE ELECTRONIC SURVEILLANCE TECHNIQUE WOULD RESULT IN:

- A SUBSTANTIAL LOSS OF LIFE, ATTRIBUTABLE TO THE INABILITY OF LAW ENFORCEMENT TO PREVENT PLANNED TERRORIST ACTS AND MURDERS.
- A SUBSTANTIAL INCREASE IN ECONOMIC HARM (IN THE BILLIONS OF DOLLARS) TO BUSINESS, INDUSTRY, LABOR UNIONS, AND SOCIETY GENERALLY CAUSED BY THE GROWTH/EMERGENCE OF ORGANIZED CRIME GROUPS AND ACTIVITIES;
- A SUBSTANTIAL INCREASE IN THE CORRUPTION OF LEGITIMATE BUSINESS, INDUSTRY, AND LABOR UNIONS CAUSED BY THE GROWTH/EMERGENCE OF ORGANIZED CRIME GROUPS;
- A SUBSTANTIAL INCREASE IN THE AVAILABILITY AND REDUCED COST OF NARCOTICS AND ILLEGAL DRUGS, AS WELL AS THE ATTENDANT PERSONAL, SOCIETAL, AND ECONOMIC HARM (NUMEROUS DEATHS, RAVAGED LIVES, AND INCREASED ECONOMIC HARM IN THE BILLIONS OF DOLLARS);
- A SUBSTANTIAL INCREASE IN UNDETECTED AND UNPROSECUTED PUBLIC CORRUPTION AND FRAUD AGAINST THE GOVERNMENT (IN THE BILLIONS OF DOLLARS) AND A RESULTING LOST TRUST IN GOVERNMENT;
- A SUBSTANTIAL INCREASE IN UNDETECTED AND UNPROSECUTED TERRORIST BOMBINGS, MURDERS, AND OTHER ACTS WITH THE ATTENDANT LOSS OF NUMEROUS LIVES AND BILLIONS OF DOLLARS IN ECONOMIC HARM;
- A SUBSTANTIAL INCREASE IN UNPROSECUTED CRIMINAL CASES OF ALL KINDS AND THE POTENTIAL FOR A SUBSTANTIAL

INCREASE IN ACQUITTALS AND HUNG JURIES OCCASIONED BY
THE LACK OF DIRECT AND PERSUASIVE ELECTRONIC
SURVEILLANCE EVIDENCE.

ELECTRONIC SURVEILLANCE: SURGICAL USE WITHOUT ABUSE

IN PASSING THE TITLE III LEGISLATION, CODIFIED AT
18 U.S.C. 2510-21, CONGRESS ENACTED A COMPREHENSIVE ELECTRONIC
SURVEILLANCE REGIMEN THAT CAREFULLY BALANCED THE COMMUNICATIONS
SECURITY NEEDS AND PRIVACY RIGHTS OF INDIVIDUALS WITH THE
LEGITIMATE NEEDS OF LAW ENFORCEMENT TO PROTECT THE PUBLIC AND
EFFECTIVELY ENFORCE THE LAW. ABOVE AND BEYOND THE TRADITIONAL
REQUIREMENTS OF THE FOURTH AMENDMENT COMPLIANCE (SUCH AS PROBABLE
CAUSE, THE NEED FOR IMPARTIAL JUDICIAL REVIEW AND A WARRANT,
PARTICULARITY AS TO THE OBJECT OF THE SEARCH, PROMPT EXECUTION OF
THE ELECTRONIC SEARCH, ETC.), CONGRESS ALSO SPECIFIED THAT
ELECTRONIC SURVEILLANCE COULD BE USED, GENERALLY SPEAKING, ONLY
AS A LAST RESORT (WHEN OTHER INVESTIGATIVE TECHNIQUES FAILED OR
WERE TOO DANGEROUS); ONLY FOR SERIOUS FELONY OFFENSES; AND ONLY
FOR SPECIFIC CRIMINAL COMMUNICATIONS. THE ACQUISITION OF NON-
CRIMINAL, NON-RELEVANT COMMUNICATIONS IS FORBIDDEN AND SUCH
COMMUNICATIONS MUST BE CAREFULLY MINIMIZED.

CONGRESS HAS ALSO ENACTED AN ELECTRONIC SURVEILLANCE
REGIMEN FOR USE IN INTELLIGENCE BASED INVESTIGATIONS, THE FOREIGN
INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA), CODIFIED AT 50
U.S.C. 1801-1811. CONTRARY TO THE ASSERTIONS OF SOME, ELECTRONIC
SURVEILLANCE CONDUCTED PURSUANT TO TITLE III OR FISA MAY NOT BE

(AND ARE NOT) EMPLOYED AGAINST INDIVIDUALS EXERCISING THEIR FIRST AMENDMENT RIGHTS, SUCH AS BY ENGAGING IN UNPOPULAR, POLITICAL, OR ANTI-GOVERNMENTAL DISCOURSE.

AN OBJECTIVE REVIEW AND ASSESSMENT OF THE TITLE III AND FISA STATUTES, AND OF THE CONDUCT OF ELECTRONIC SURVEILLANCE BY LAW ENFORCEMENT PURSUANT TO THESE STATUTES, INDICATE THAT ELECTRONIC SURVEILLANCE HAS BEEN CONDUCTED SPARINGLY, JUDICIOUSLY, AND IN COMPLIANCE WITH THE LETTER OF THE LAW AND THE SPIRIT OF CONGRESS' INTENT. AS DEMONSTRATED BY THE LIVES SAVED AND IMPORTANT INVESTIGATIONS AND PROSECUTIONS SUCCESSFULLY COMPLETED, THE TITLE III STATUTORY REGIMEN HAS SERVED BOTH SOCIETY AND LAW ENFORCEMENT EXTREMELY WELL. MOREOVER, AFTER 25 YEARS OF USAGE, THERE IS NO EVIDENCE OF SIGNIFICANT ABUSE. STATISTICS COMPILED BY THE FBI, WHICH IS CHARGED WITH INVESTIGATING VIOLATIONS OF THE FEDERAL "WIRETAP" STATUTE BASED UPON ACTS OF ILLEGAL ELECTRONIC SURVEILLANCE AND WIRETAPPING, INDICATE THAT INSTANCES OF ILLEGAL WIRETAPPING ARE VERY, VERY RARE.

ELECTRONIC SURVEILLANCE TECHNICAL ASSISTANCE

WHEN THE TITLE III LEGISLATION WAS ENACTED BY CONGRESS IN 1968, THERE WAS NO SPECIFIC PROVISION FOR TECHNICAL OR OTHER ASSISTANCE TO LAW ENFORCEMENT. WITH REGARD TO WIRE COMMUNICATIONS, LAW ENFORCEMENT NECESSARILY RELIES UPON THE TELECOMMUNICATION SERVICE PROVIDER'S ASSISTANCE IN IDENTIFYING THE TARGET'S WIRE PAIRS AND THEIR LINE "APPEARANCES," AND UPON THE SERVICE PROVIDER'S FURNISHING OF LEASED LINES TO ENABLE THE INTERCEPTED

COMMUNICATIONS TO BE TRANSMITTED TO A SECURE, LAW ENFORCEMENT MONITORING FACILITY.

ALTHOUGH THE SERVICE PROVIDER ASSISTANCE REQUIREMENT WAS THOUGHT TO BE SELF-EVIDENT AND IMPLICIT IN THE TITLE III LEGISLATION, CERTAIN SERVICE PROVIDERS INITIALLY RESISTED PROVIDING LAW ENFORCEMENT WITH NEEDED ASSISTANCE, EVEN WHEN DIRECTED TO DO SO BY COURT ORDER. SEE, E.G., APPLICATION OF UNITED STATES, 427 F.2D 639 (9TH CIR. 1970). AS A RESULT, CONGRESS WAS COMPELLED TO AMEND THE TITLE III STATUTE IN 1970 AND EXPRESSLY FIX THE ASSISTANCE RESPONSIBILITY THEREIN. THE ASSISTANCE PROVISION, AS AMENDED, AND CODIFIED AT 18 U.S.C 2518(4), STATES:

"AN ORDER AUTHORIZING THE INTERCEPTION OF A WIRE, ORAL, OR ELECTRONIC COMMUNICATION UNDER THIS CHAPTER SHALL, UPON REQUEST OF THE APPLICANT, DIRECT THAT A PROVIDER OF WIRE OR ELECTRONIC COMMUNICATION SERVICE, LANDLORD, CUSTODIAN OR OTHER PERSON SHALL FURNISH THE APPLICANT FORTHWITH ALL INFORMATION, FACILITIES, AND TECHNICAL ASSISTANCE NECESSARY TO ACCOMPLISH THE INTERCEPTION UNOBTRUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH THE SERVICES THAT SUCH SERVICE PROVIDER, LANDLORD, CUSTODIAN, OR PERSON IS ACCORDING THE PERSON WHOSE COMMUNICATIONS ARE TO BE INTERCEPTED. ANY PROVIDER OF WIRE OR ELECTRONIC COMMUNICATION SERVICE, LANDLORD, CUSTODIAN OR OTHER PERSON FURNISHING SUCH FACILITIES OR TECHNICAL ASSISTANCE SHALL BE COMPENSATED THEREFORE BY THE APPLICANT FOR REASONABLE EXPENSES INCURRED IN PROVIDING SUCH FACILITIES OR ASSISTANCE." (EMPHASIS ADDED)

THE FISA STATUTE, ENACTED IN 1978, CONTAINS A SIMILAR ASSISTANCE PROVISION, CODIFIED AT 50 U.S.C 1805 (B)(2). SO ALSO DO THE PEN REGISTER AND TRAP AND TRACE STATUTES. SEE 18 U.S.C. 3124(a)(b).

IT IS VERY IMPORTANT TO UNDERSTAND THAT TELEPHONE COMPANIES HISTORICALLY HAVE BEEN EXTREMELY CONSERVATIVE, AND OFTEN HAVE DECLINED TO PROVIDE LAW ENFORCEMENT WITH NECESSARY TECHNICAL ASSISTANCE, EVEN WHEN SERVED WITH COURT ORDERS. FOR EXAMPLE, SOME TELEPHONE COMPANIES INITIALLY RESISTED PROVIDING LAW ENFORCEMENT WITH EVEN MINOR "LEASED LINE" ASSISTANCE TO ALLOW LAW ENFORCEMENT TO CARRY OUT A PEN REGISTER INVESTIGATION, ALTHOUGH SERVED WITH A FEDERAL SEARCH WARRANT. THIS RESISTANCE TO PEN REGISTER ASSISTANCE WAS REMOVED BY THE SUPREME COURT IN UNITED STATES V. NEW YORK TELEPHONE CO., 434 U.S. 159 (1977). SOME TELEPHONE COMPANIES ALSO RESISTED PROVIDING RELATIVELY MINOR ASSISTANCE TO EFFECT A TRAP AND TRACE OF DIALED NUMBER INFORMATION WHEN SERVED WITH A FEDERAL COURT ORDER. FEDERAL COURT OF APPEALS ACTION WAS REQUIRED TO OBTAIN SUCH TRAP AND TRACE ASSISTANCE TO TRACE DIALED NUMBER INFORMATION. UNITED STATES V. MOUNTAIN STATES TELEPHONE AND TELEGRAPH COMPANY, 616 F.2D 1122 (9TH CIR. 1980); IN RE APPLICATION OF UNITED STATES, 610 F.2D 1148 (3RD CIR. 1979); MICHIGAN BELL TELEPHONE COMPANY V. UNITED STATES, 565 F.2D 385 (6TH CIR. 1977). THE LESSON FROM SUCH INCIDENTS IS CLEAR: SOME TELECOMMUNICATIONS COMPANIES, INCLUDING COMMON CARRIERS, WHO ARE CONCERNED WITH THEIR LEGAL LIABILITIES WILL ACT ONLY WHEN THE LAW IS CLEAR AS TO THEIR RESPONSIBILITIES AND WHEN PRESENTED WITH A COURT ORDER.

IN THE AREAS OF PEN REGISTERS AND TRAP AND TRACE DEVICES, COURTS HAVE REQUIRED TELECOMMUNICATION SERVICE PROVIDERS TO EXTEND TECHNICAL AND PHYSICAL ASSISTANCE TO LAW ENFORCEMENT, IN ORDER TO EFFECTUATE COURT ORDERS. THERE ARE, HOWEVER, NO FEDERAL CASES CONSTRUING THE TITLE III OR FISA STATUTORY "ASSISTANCE" PROVISIONS. ATTORNEYS WHO HAVE ANALYZED THESE ASSISTANCE PROVISIONS BELIEVE THAT THEIR CURRENT LANGUAGE DOES NOT CLEARLY MANDATE THAT SERVICE PROVIDERS AFFIRMATIVE MUST TAKE ANY STEPS OR DEVELOP ANY TECHNICAL SOLUTIONS TO ACCOMMODATE OR EFFECTUATE A COURT'S ELECTRONIC SURVEILLANCE ORDER. THUS, THE ISSUE AS TO THE NATURE AND EXTENT OF SERVICE PROVIDER ASSISTANCE REMAINS AN OPEN, AND OFTEN HOTLY DEBATED, QUESTION.

THE QUESTION HAS BEEN RAISED BY SOME IF REQUESTING OR REQUIRING GREATER ELECTRONIC SURVEILLANCE TECHNICAL ASSISTANCE OF SERVICE PROVIDERS TO CARRY OUT A COURT ORDER THROUGH EITHER HARDWARE- OR SOFTWARE-BASED MODIFICATIONS OR DEVELOPMENTS EXTENDS LAW ENFORCEMENT'S AUTHORITY. THERE APPEARS TO BE GENERAL AGREEMENT WITHIN THE GOVERNMENT AND INDUSTRY THAT THIS WOULD NOT EXTEND LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE AUTHORITY. THIS AGREEMENT EXTENDS TO LAW ENFORCEMENT'S LEGAL AUTHORITY OR ENTITLEMENT TO OBTAIN THE CONTENT OF A CRIMINAL TARGET'S COMMUNICATIONS OR DIALED NUMBER INFORMATION TRANSMITTED VIA A TELECOMMUNICATIONS NETWORK.

SOME HAVE STATED THAT REQUIRING TELECOMMUNICATION SERVICE PROVIDERS TO EXPEND ADDITIONAL TECHNICAL OR MONETARY RESOURCES, EVEN PURSUANT TO COURT ORDER, TO HELP LAW ENFORCEMENT EFFECT ELECTRONIC SURVEILLANCE IS UNWARRANTED OR UNPRECEDENTED.

HOWEVER, HISTORICALLY TELECOMMUNICATION SERVICE PROVIDERS HAVE BEEN REQUIRED TO ALTER THEIR OPERATIONS AND ACTIVITIES TO MEET LAW ENFORCEMENT REQUIREMENTS. FOR EXAMPLE, SERVICE PROVIDERS HAVE BEEN REQUIRED BY REGULATION TO MAINTAIN TELEPHONE TOLL RECORDS LONGER THAN OPERATIONALLY NECESSARY, AND GENERALLY THEY DEDICATE TIME, HUMAN RESOURCES, AND HENCE MONEY, TO PROVIDE LAW ENFORCEMENT AGENCIES WITH SUCH SUBSCRIBER INFORMATION. FURTHER, BY WAY OF PRECEDENT, CONGRESS HAS ENACTED PUBLIC SAFETY/PUBLIC WELFARE LEGISLATION CONCERNING TELECOMMUNICATION SERVICE PROVIDERS IN THE AREA OF INTEROPERABLE EQUIPMENT TO ASSIST THE HEARING-IMPAIRED AND IN THE AREA OF TELEPHONICALLY TRANSMITTED PORNOGRAPHIC COMMUNICATIONS (SO CALLED "DIAL-A-PORN"). ALSO, MANY LOCALITIES REQUIRE BY LAW THAT THE TELECOMMUNICATION LOCAL EXCHANGE CARRIERS PROVIDE "911" EMERGENCY SERVICE, THE COST OF WHICH IS PASSED ON TO ALL SUBSCRIBERS.

WITHIN THE UNITED STATES, THERE ARE NUMEROUS OTHER PUBLIC SAFETY/PUBLIC WELFARE LAWS AND REGULATIONS WHICH AFFECT A NUMBER OF INDUSTRIES AND BUSINESSES AND MANDATE TECHNICAL EFFORTS AND MONETARY EXPENSES (E.G., REQUIRED SPRINKLER SYSTEMS, SMOKE DETECTORS, FIRE ALARMS, FIRE ESCAPES, ETC., IN OFFICES, FACTORIES, APARTMENT COMPLEXES, ETC.; SAFETY BELTS, "AIR BAGS," CATALYTIC CONVERTERS, AND EMISSION CONTROL DEVICES IN VEHICLES). ON BALANCE, WHEN LAW ENFORCEMENT'S COURT-ORDERED USE OF ELECTRONIC SURVEILLANCE IS VIEWED IN TERMS OF ITS IMPORTANT, AND EVEN CRITICAL, UTILITY IN PREVENTING AND SOLVING CRIMES, AND AS A PUBLIC SAFETY REQUIREMENT, THERE CAN BE NO SERIOUS DOUBT THAT A

POLICY DECISION REQUIRING SUCH TECHNICAL ASSISTANCE BY LAW IS CONSISTENT WITH PAST SOCIETAL AND GOVERNMENTAL PRACTICES.

SUMMARY OF TECHNOLOGICAL IMPEDIMENTS

PRIOR TO 1984, THE MAJORITY OF LOCAL AND LONG DISTANCE TELECOMMUNICATIONS WERE CARRIED BY AT&T, WHICH HELD A VIRTUAL MONOPOLY ON THESE SERVICES. THIS RESULTED IN AN HOMOGENEOUS NETWORK IN WHICH THE TECHNOLOGIES USED TO CONDUCT BUSINESS WERE THE SAME THROUGHOUT THE NETWORK. ADDITIONALLY, BECAUSE OF AN ABSENCE OF COMPETITION, NEW TECHNOLOGIES WERE INTRODUCED SLOWLY AND BY ONLY A SMALL NUMBER OF MANUFACTURERS.

SINCE THE DIVESTITURE OF AT&T IN 1984, THE NUMBER OF SERVICE PROVIDERS, AS WELL AS THE DIVERSITY OF TECHNOLOGIES, HAS GROWN RAPIDLY AND DRAMATICALLY. FOR EXAMPLE, THE NUMBER OF CARRIERS PROVIDING LOCAL TELEPHONE SERVICE IS NOW OVER 1,400. A SEPTEMBER 1992 DECISION BY THE FEDERAL COMMUNICATIONS COMMISSION IS FACILITATING EVEN GREATER COMPETITION IN THIS AREA. AS A RESULT, THE INDUSTRY WILL BEGIN TO SEE NEW PROVIDERS OF SERVICE AND ALREADY HAS BEGUN TO SEE NEW BUSINESS PARTNERSHIPS AMONG EXISTING SERVICE PROVIDERS. ALSO, THE NUMBER OF LONG DISTANCE CARRIERS HAS GROWN FROM ESSENTIALLY ONE IN 1984 TO OVER 300 TODAY. WITH THE ADVENT OF WIRELESS TECHNOLOGIES, SUCH AS CELLULAR, THE NUMBER OF SERVICE PROVIDERS GREW AGAIN. TODAY, THERE ARE OVER 160 CELLULAR SERVICE PROVIDERS. THE INTRODUCTION OF NEW TECHNOLOGIES, AS WELL AS ACTIONS TAKEN BY THE FEDERAL COURTS AND THE FEDERAL COMMUNICATIONS COMMISSION, HAVE RESULTED

IN GREATER NUMBERS AND MORE DIVERSITY AMONG SERVICE PROVIDERS. AS A RESULT, LAW ENFORCEMENT AGENCIES HAVE HAD TO WORK WITH MANY DIFFERENT SERVICE PROVIDERS TO OBTAIN THE ASSISTANCE NECESSARY TO CONDUCT WIRETAPS. NUMEROUS SITUATIONS HAVE ARISEN WHERE SERVICE PROVIDERS WHO WERE INEXPERIENCED WITH COURT AUTHORIZED WIRETAPS HAVE BEEN UNABLE TO PROVIDE ASSISTANCE TO LAW ENFORCEMENT AGENCIES BECAUSE OF A LACK OF UNDERSTANDING OF THE LEGITIMATE REQUIREMENTS OF LAW ENFORCEMENT.

TRADITIONALLY, COMMON CARRIERS HAVE OFFERED ESSENTIALLY "FIXED POINT" TELECOMMUNICATIONS: THAT IS TO SAY, COMMUNICATIONS GENERATED BY, OR INTENDED FOR, A CUSTOMER AND TRANSMITTED TO A FIXED LOCATION CORRESPONDING TO A SPECIFIC TELEPHONE NUMBER. HISTORICALLY, THESE COMMUNICATIONS HAVE BEEN TRANSMITTED OVER COMMON CARRIER FACILITIES, SUCH AS TELEPHONE WIRES THAT WERE DEDICATED TO A CUSTOMER'S SPECIFIC TELEPHONE NUMBER (OFTEN REFERRED TO AS A SUBSCRIBER'S "LOOP"). IN THE PAST, WHEN LAW ENFORCEMENT AGENCIES CONDUCTED COURT-AUTHORIZED ELECTRONIC SURVEILLANCE OR "WIRETAPS" ON A SUBJECT'S TRADITIONAL "LOCAL LOOP," THEY WERE VIRTUALLY ASSURED OF INTERCEPTING THE CONTENT OF ALL COMMUNICATIONS (AS WELL AS THE RELATED DIALING INFORMATION) ASSOCIATED WITH THE SUBJECT'S TELEPHONE NUMBER SET FORTH IN THE COURT ORDER.

OVER RECENT YEARS, ADVANCES IN TELECOMMUNICATIONS TECHNOLOGIES, AS WELL AS THE INCREASING NUMBER OF COMMON CARRIERS (APPROXIMATELY 2,000) ENTERING THE TELECOMMUNICATIONS MARKETPLACE, HAVE INTRODUCED NEW SOPHISTICATED SERVICES AND

FEATURES THAT ALLOW FOR THE EFFICIENT TRANSMISSION OF MULTIPLE, SIMULTANEOUS COMMUNICATIONS OF MULTIPLE SUBSCRIBERS. SUCH COMMUNICATIONS ARE TRANSMITTED OVER FIBER OPTIC LINES AND WIRE FACILITIES THAT PREVIOUSLY WERE DEDICATED TO A SINGLE COMMUNICATION AND A SINGLE SUBSCRIBER. OTHER ADVANCED COMMUNICATIONS SERVICES (SUCH AS CELLULAR TELEPHONES) AND FEATURES (SUCH AS CALL FORWARDING WHICH PERMITS CUSTOMERS TO REDIRECT CALLS INTENDED FOR THEM) UNDERMINE THE NECESSITY FOR COMMUNICATIONS TO BE TRANSMITTED ALWAYS TO THE SAME SPECIFIC LOCATION OR THROUGH THE SAME WIRELINE LOOP. LIKEWISE, "FOLLOW-ME" FEATURES AND SERVICES EXPAND THE NOTION OF CALL FORWARDING TO NATIONAL PROPORTIONS. FURTHER, COMMON CARRIERS' DEPLOYMENT OF THE PERSONAL COMMUNICATIONS SERVICES (PCS) IN THE NEAR FUTURE WILL ENABLE USERS TO DEFINE THEIR OWN SET OF SUBSCRIBED SERVICES, USE ANY FIXED OR MOBILE TERMINAL OR TELEPHONE INSTRUMENT, AND INITIATE AND RECEIVE CALLS ACROSS MULTIPLE NETWORKS WITHOUT REGARD TO THEIR GEOGRAPHIC LOCATION. ALL OF THESE "FOLLOW-ME-TYPE" SERVICES, IN EFFECT, DISASSOCIATE A SUBSCRIBER'S NUMBER FROM A FIXED LOCAL LOOP. THUS, LAW ENFORCEMENT'S ABILITY TO CONDUCT SUCCESSFULLY COURT-ORDERED ELECTRONIC SURVEILLANCE IS GREATLY HAMPERED.

AS A RESULT OF THESE AND OTHER NEW AND ADVANCED TECHNOLOGIES, COMMON CARRIERS ARE NO LONGER ABLE TO ENSURE THEIR ABILITY TO ISOLATE SPECIFIC COMMUNICATIONS (AND DIALING INFORMATION) ASSOCIATED WITH THE SUBJECTS OF COURT-ORDERED SURVEILLANCE, TO THE EXCLUSION OF ALL OTHER SUBSCRIBERS'

COMMUNICATIONS AND DIALING INFORMATION. INDUSTRY REPRESENTATIVES HAVE BLUNTLY TOLD LAW ENFORCEMENT THAT THE EXISTING TELECOMMUNICATIONS SYSTEMS AND NETWORKS WILL THWART COURT AUTHORIZED INTERCEPTS. THE ABOVE-DESCRIBED SERVICES AND FEATURES AND THE NEW TELECOMMUNICATION SYSTEMS PLANNED FOR FUTURE IMPLEMENTATION, BOTH IN THEIR CURRENT AND PLANNED CONFIGURATIONS, OFTEN PREVENT, AND WILL CONTINUE TO PREVENT COMMON CARRIERS FROM PROVIDING LAW ENFORCEMENT WITH ACCESS TO ALL OF THE COMMUNICATIONS AND DIALING INFORMATION THAT ARE THE SUBJECT OF ELECTRONIC SURVEILLANCE AND PEN REGISTER COURT ORDERS.

THE ATTACHED CHARTS (PAST OPERATING ENVIRONMENT, PRESENT OPERATING ENVIRONMENT, AND FUTURE OPERATING ENVIRONMENT) DEPICT THE INCREASINGLY COMPLEX TELECOMMUNICATIONS ENVIRONMENT IN WHICH LAW ENFORCEMENT HAS OPERATED AND WILL CONTINUE TO OPERATE WHEN ATTEMPTING TO EXECUTE COURT-AUTHORIZED ELECTRONIC SURVEILLANCES.

OVER THE LAST DECADE, IT IS CONSERVATIVELY ESTIMATED THAT SEVERAL HUNDRED ELECTRONIC SURVEILLANCE AND PEN REGISTER AND TRAP AND TRACE COURT ORDERS HAVE BEEN FRUSTRATED, IN WHOLE OR IN PART, BY VARIOUS TECHNOLOGICAL IMPEDIMENTS. DURING 1993, THE FBI, THROUGH AN INFORMAL SURVEY OF FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT, COLLECTED INFORMATION REGARDING THE EXECUTION OF RECENT ELECTRONIC SURVEILLANCE COURT ORDERS (INCLUDING AUTHORIZATIONS FOR CALL CONTENT, PEN REGISTER, AND TRAP AND TRACE) IN ORDER TO GAUGE HOW MANY COURT ORDERS HAVE BEEN FRUSTRATED OR DELAYED DUE TO TECHNOLOGY-BASED PROBLEMS. THE

SURVEY REVEALED 91 INSTANCES IN WHICH LAW ENFORCEMENT AGENCIES PARTICIPATING IN THE SURVEY WERE PRECLUDED FROM IMPLEMENTING OR FULLY IMPLEMENTING COURT ORDERS FOR ELECTRONIC SURVEILLANCE DUE TO VARIOUS TECHNOLOGICAL IMPEDIMENTS. THE MAJORITY OF THE PROBLEMS WERE ENCOUNTERED DURING ATTEMPTS TO EXECUTE ORDERS REGARDING ELECTRONIC SURVEILLANCE ACTIVITIES RELATING TO CELLULAR TELEPHONE SYSTEMS (33%) AND "FIXED" OR WIRELINE COMMUNICATIONS THAT EMPLOYED CUSTOM CALLING FEATURES (32%). WITH RESPECT TO CELLULAR SYSTEMS, PROBLEMS HAVE RANGED FROM A TECHNICAL INABILITY ON THE PART OF THE CELLULAR COMMON CARRIER TO ASSIST LAW ENFORCEMENT, TO CELLULAR SYSTEMS THAT WERE NOT CAPABLE OF ISOLATING AND COLLECTING COMMUNICATIONS AND/OR PEN REGISTER INFORMATION (DIALED NUMBERS) ASSOCIATED WITH SUBJECT'S TELEPHONE COMMUNICATIONS. A SEPARATE CATEGORY OF TECHNICAL PROBLEMS ASSOCIATED WITH CELLULAR SYSTEMS RELATES TO THE INABILITY OF SOME CELLULAR CARRIERS TO COMPLY WITH COURT ORDERS DUE TO A LIMITED CAPACITY ASSOCIATED WITH THE CARRIER'S PARTICULAR SYSTEM (11%). THE FOLLOWING ARE EXAMPLES TO ILLUSTRATE SOME OF THE IMPEDIMENTS ENCOUNTERED:

1. A FEDERAL INVESTIGATION OF A MAJOR NARCOTICS ORGANIZATION OPERATING IN THE NORTHEASTERN UNITED STATES WAS HAMPERED WHEN THE CELLULAR TELEPHONE SERVICE PROVIDER WAS UNABLE TO FULFILL REQUESTS FOR COURT-ORDERED WIRETAPS DUE TO THE PROVIDER'S TECHNICAL LIMITATIONS.

2. AN ORGANIZED CRIME AND DRUG TRAFFICKING TASK FORCE INVESTIGATION IN THE SOUTHEASTERN U. S. WAS UNABLE TO CONDUCT A COURT-ORDERED WIRETAP AS THE CELLULAR TELEPHONE SERVICE PROVIDER WAS UNABLE TO PROVIDE LAW ENFORCEMENT WITH ACCESS TO THE SUBJECT'S LONG DISTANCE COMMUNICATIONS MADE THROUGH THE PROVIDERS CELLULAR SERVICE.
3. TWO DIFFERENT CELLULAR SERVICE PROVIDERS IN THE MID-WESTERN U.S. WERE UNABLE TO COMPLY WITH SEPARATE FEDERAL COURT-ORDERS REQUESTING PEN REGISTER OR DIALED NUMBER INFORMATION FROM A SUSPECTED DRUG TRAFFICKER'S CELLULAR TELEPHONE.
4. A REGIONAL TELEPHONE COMPANY IN THE MID-WESTERN U.S. WAS UNABLE TO PROVIDE A FEDERAL LAW ENFORCEMENT AGENCY WITH THE CONTENT AND DIALED NUMBER INFORMATION FROM A SUSPECTED DRUG TRAFFICKERS TELEPHONE AS A RESULT OF THE SUBJECTS USE OF CUSTOM CALLING FEATURES.
5. A CELLULAR SERVICE PROVIDER IN THE SOUTH WAS UNABLE TO COMPLY WITH A FEDERAL COURT-ORDER FOR DIALED NUMBER INFORMATION CONCERNING A FEDERAL PUBLIC CORRUPTION INVESTIGATION DUE TO TECHNICAL LIMITATIONS.

IT IS IMPORTANT TO NOTE THAT THERE HAVE BEEN MANY INSTANCES WHERE COURT ORDERS HAVE NOT BEEN SOUGHT OR SERVED ON CARRIERS DUE TO LAW ENFORCEMENT'S AWARENESS OF THESE PRE-EXISTING IMPEDIMENTS, AND THEREFORE THEY WERE NOT TABULATED IN CONNECTION WITH THIS SURVEY. INCLUDED IN A RECENT LETTER FROM THE DIRECTOR

OF A HIGH INTENSITY DRUG TRAFFICKING AREA (HIDTA) IT WAS NOTED THAT A FEDERAL LAW ENFORCEMENT AGENCY DID NOT PURSUE TWENTY-FIVE COURT ORDERS BECAUSE OF THE KNOWN INABILITIES OF THE CELLULAR SERVICE PROVIDER TO EFFECTUATE SUCH ORDERS.

HOWEVER, IT WOULD BE A MISTAKE TO ANALYZE AND RESPOND TO THIS PROBLEM SIMPLY BY ATTEMPTING TO COUNT THE SPECIFIC NUMBER OF COURT ORDERS FRUSTRATED OR DELAYED IN THE PAST. ALTHOUGH THEY CONVEY A SENSE OF THE PROBLEM, AND IDENTIFY SOME OF THE TECHNICAL PROBLEMS THAT ARE BEING ENCOUNTERED AS A RESULT OF RECENT TELECOMMUNICATIONS TECHNOLOGY ADVANCES, FOCUSING ON THESE NUMBERS AND TECHNOLOGIES ALONE IS TERRIBLY MISLEADING. FORTUNATELY, THE NUMBER OF COURT-ORDERED INTERCEPTIONS THAT HAVE BEEN IMPEDED BY TECHNOLOGY IS STILL SOMEWHAT LIMITED. HOWEVER, THE TELECOMMUNICATIONS TECHNOLOGIES THAT ARE EMERGING WILL LIKELY HAVE A MUCH GREATER AND MORE DEVASTATING IMPACT ON LAW ENFORCEMENT'S ABILITY TO CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE IN THE FUTURE.

FBI/GOVERNMENT EFFORTS TO OBTAIN TELECOMMUNICATIONS INDUSTRY'S COOPERATION/SOLUTIONS

FOR ALMOST FOUR YEARS, THE GOVERNMENT HAS ATTEMPTED TO RESOLVE THE TECHNICAL ISSUES ASSOCIATED WITH COURT-ORDERED ELECTRONIC SURVEILLANCE BY MEETING WITH VARIOUS REPRESENTATIVES OF THE TELECOMMUNICATIONS INDUSTRY AT VIRTUALLY ALL CORPORATE LEVELS. HISTORICALLY, LAW ENFORCEMENT'S INTERFACE WITH THIS INDUSTRY HAS BEEN THROUGH THE SECURITY ORGANIZATION OF THE COMMON

CARRIER. IT IS THIS INTERFACE THAT PREVIOUSLY HAS BEEN MOST KNOWLEDGEABLE OF LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE REQUIREMENTS, AS THEY RECEIVE COURT ORDERS REQUIRING THEM TO ASSIST LAW ENFORCEMENT WITH THEIR ELECTRONIC SURVEILLANCE RESPONSIBILITIES. HOWEVER, IT WAS LEARNED IN 1990, DURING DISCUSSIONS WITH THE INDUSTRY, THAT THE SECURITY ENTITIES WITHIN THE COMMON CARRIER COMPANIES WERE NOT ROUTINELY INVOLVED IN THE INDUSTRY'S TECHNOLOGY PLANNING, DESIGN, AND DEVELOPMENT PROCESSES. AS A RESULT, LAW ENFORCEMENT'S NEEDS WERE NOT BEING INCORPORATED INTO THE CARRIERS' SYSTEM REQUIREMENTS.

IN AN ATTEMPT TO HAVE LAW ENFORCEMENT'S REQUIREMENTS CONSIDERED DURING THE INDUSTRY'S PLANNING PROCESSES, THE GOVERNMENT SYSTEMATICALLY MET WITH THE MOST SENIOR LEVELS OF THE TRADITIONAL COMMON CARRIERS AND BRIEFED THEM ABOUT THE DIFFICULTIES BEING ENCOUNTERED BY LAW ENFORCEMENT AND ABOUT OUR CONCERNS THAT FUTURE TECHNOLOGIES WOULD SEVERELY DIMINISH, IF NOT PRECLUDE, THIS CRITICAL INVESTIGATIVE TECHNIQUE. ALTHOUGH THESE EXECUTIVES APPEARED SUPPORTIVE OF LAW ENFORCEMENT'S GOALS, SEVERAL OF THEM INDICATED THAT WITHOUT SOME SORT OF MANDATE, SUCH AS LEGISLATION, THEIR COMPANIES COULD NOT UNILATERALLY INVEST TIME, MONEY, AND TECHNICAL RESOURCES IN DEVELOPING AND IMPLEMENTING SOLUTIONS, ESPECIALLY IF THERE WERE NO ASSURANCE THAT THEIR COMPETITORS WOULD DO SO.

ON JANUARY 15, 1992, THEN PRESIDENT BUSH AUTHORIZED THE JUSTICE DEPARTMENT TO PROCEED WITH A LEGISLATIVE INITIATIVE. ON MARCH 6, 1992, THE DIGITAL TELEPHONY LEGISLATION WAS ANNOUNCED,

AND THE INDUSTRY RESPONSE WAS GENERALLY NEGATIVE, A POSITION THAT WAS AT VARIANCE WITH THAT EXPRESSED PREVIOUSLY BY A NUMBER OF THE REPRESENTATIVES OF THE TELECOMMUNICATIONS COMPANIES. ON MARCH 18, 1992, THEN ATTORNEY GENERAL WILLIAM BARR AND THEN FBI DIRECTOR WILLIAM S. SESSIONS SPONSORED AND CHAIRED A MEETING FOR ALL MAJOR INDUSTRY EXECUTIVES. IT WAS ATTENDED BY FOUR TELECOMMUNICATIONS EXECUTIVES, REPRESENTING THE INDUSTRY. DURING THIS MEETING, TELECOMMUNICATIONS EXECUTIVES ASSERTED THAT THE FBI HAD BEEN TALKING TO THE WRONG PEOPLE IN INDUSTRY (THE SECURITY OFFICERS, SENIOR EXECUTIVES, ETC.) AND THAT THE SOLUTION TO THESE PROBLEMS RESTED WITH THOSE UPPER/MID-LEVEL MANAGERS AND ENGINEERS WHO OVERSAW DEVELOPMENT/IMPLEMENTATION OF THE TECHNOLOGIES IN QUESTION. THE ATTORNEY GENERAL AGREED TO AN INDUSTRY REQUEST THAT A TELECOMMUNICATIONS TECHNICAL COMMITTEE CONSISTING OF THE "RIGHT INDUSTRY PEOPLE" (PICKED BY THE CEOS) BE CREATED TO IDENTIFY TECHNICAL SOLUTIONS AND TO GET THE JOB DONE. IT WAS ALSO CLEARLY UNDERSTOOD THAT THE ADMINISTRATION AND LAW ENFORCEMENT WOULD CONTINUE TO PURSUE LEGISLATION.

AS A RESULT OF THE MARCH 18, 1992, MEETING, INDUSTRY REPRESENTATIVES MET WITH THE GOVERNMENT ON MARCH 26, 1992, TO BEGIN A PROCESS OF ESTABLISHING A TECHNICAL WORKING COMMITTEE TO ADDRESS TECHNICAL IMPEDIMENTS TO ELECTRONIC SURVEILLANCE. IN MAY OF 1992, AN AD HOC TECHNICAL WORKING GROUP BEGAN. THIS GROUP WAS LATER ORGANIZED AS THE ELECTRONIC COMMUNICATION SERVICE PROVIDERS COMMITTEE UNDER AN INDUSTRY ASSOCIATION NOW KNOWN AS THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS (ATIS). THIS COMMITTEE

CONSISTS OF REPRESENTATIVES OF ELECTRONIC COMMUNICATION SERVICE PROVIDERS (E.G. COMMON CARRIERS), TELECOMMUNICATIONS EQUIPMENT MANUFACTURERS, AND LAW ENFORCEMENT OFFICIALS, WHO ATTEND VOLUNTARILY AND WITH VARYING DEGREES OF REGULARITY AND INTEREST. AS A RESULT OF THIS PROCESS, OVER THE PAST TWO YEARS THERE HAS BEEN A BETTER UNDERSTANDING BY BOTH LAW ENFORCEMENT AND INDUSTRY REPRESENTATIVES OF THE ISSUES THAT EACH FACE WITH RESPECT TO ELECTRONIC SURVEILLANCE. HOWEVER, CONTRARY TO ASSERTIONS, NEW TELECOMMUNICATIONS TECHNOLOGIES WILL JEOPARDIZE LAW ENFORCEMENT'S SURVEILLANCE ABILITIES. THE ATIS CHAIRMAN HAS STATED IN A RECENT LETTER THAT THE ENTIRE COMMITTEE, NOT JUST ONE PARTICIPANT OR ONE GROUP OF PARTICIPANTS, NOW RECOGNIZES THE PROBLEMS AND IMPEDIMENTS THAT THESE TELECOMMUNICATIONS TECHNOLOGIES ARE CREATING FOR LAW ENFORCEMENT. A COPY OF OUR CORRESPONDENCE WITH THE ATIS CHAIRMAN IS ATTACHED AS AN EXHIBIT.

I SUPPORT CONTINUED DIALOGUE BETWEEN INDUSTRY AND LAW ENFORCEMENT. HOWEVER, IT MUST BE RECOGNIZED THAT THIS COMMITTEE PROCESS IS VOLUNTARY AND, AS SUCH, ONLY THOSE COMPANIES WHO ARE COMMITTED TO ASSISTING LAW ENFORCEMENT PARTICIPATE AND SUPPORT THIS EFFORT. SECOND, ONLY A HANDFUL OF THE OVER 2,000 COMPANIES ATTEND. THIRD, NO IMPLEMENTABLE SOLUTIONS HAVE BEEN DEVELOPED SINCE DISCUSSIONS BEGAN ALMOST TWO YEARS AGO. FOURTH, COMMITTEE RESOLUTIONS ARE NON-BINDING AND IT IS NOT POSSIBLE TO SECURE A COMMITMENT FROM PARTICIPANTS TO IMPLEMENT ANY SOLUTIONS THAT MAY BE DEVELOPED IN THIS VOLUNTARY FORUM. FINALLY, AS IN ANY BUSINESS DECISION, IT IS RECOGNIZED THAT THERE WILL BE COSTS

INCURRED BY INDUSTRY TO ACCOMMODATE LAW ENFORCEMENT'S REQUIREMENTS. THE ATIS CHAIRMAN HAS ALSO INDICATED THAT ANTITRUST AND OTHER LEGAL CONSIDERATIONS PRECLUDE DISCUSSIONS AND RESOLUTIONS TO THESE COST ISSUES. IN LIGHT OF THESE LIMITATIONS, THE ADMINISTRATION AND ALL OF LAW ENFORCEMENT HAVE CONCLUDED THAT THE COMMITTEE PROCESS IS NOT, AND CANNOT BE, A SUBSTITUTE FOR A LEGISLATIVE MANDATE TO ENSURE LAW ENFORCEMENT'S CONTINUED ABILITY TO CONDUCT COURT-AUTHORIZED ELECTRONIC SURVEILLANCE.

PRESIDENTIAL REVIEW DIRECTIVE (PRD)

IN APRIL 1993, PRESIDENT CLINTON DIRECTED THAT AN INTERAGENCY WORKING GROUP BE ESTABLISHED UNDER THE AUSPICES OF THE NATIONAL SECURITY COUNCIL (NSC) TO EXAMINE ADVANCED TELEPHONY AND TO CONSIDER ITS EFFECT AND IMPACT ON THE CONDUCT OF ELECTRONIC SURVEILLANCE BY OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES. AFTER AN IN-DEPTH EIGHT MONTH STUDY, THE NSC PROVIDED A NUMBER OF POLICY OPTIONS FOR THE VICE PRESIDENT AND APPROPRIATE CABINET OFFICIALS. AS A RESULT OF THEIR REVIEW OF THE OPTIONS, IT WAS UNANIMOUSLY DECIDED THAT COMPREHENSIVE LEGISLATION WAS THE ONLY EFFECTIVE WAY TO DEAL WITH THE "DIGITAL TELEPHONY" PROBLEM. FUNDAMENTAL TO THIS DECISION WAS THE BELIEF THAT IT WOULD BE UNACCEPTABLE FOR THE SAFETY OF THE AMERICAN PUBLIC TO BE IMPERILED, THE NATIONAL SECURITY ENDANGERED, AND EFFECTIVE LAW ENFORCEMENT ERODED THROUGH THE LOSS OR DIMINISHMENT OF THIS CRITICAL AND ESSENTIAL TOOL OF OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.

PROPOSED LEGISLATION

THE PROPOSED LEGISLATION REPRESENTS, IN OUR ESTIMATION, THE ONLY RATIONAL AND VIABLE APPROACH TO SOLVING THE DIGITAL TELEPHONY PROBLEM IN A COMPREHENSIVE FASHION. ONLY THROUGH LEGISLATION CAN THE GOVERNMENT BE ASSURED THAT WITHIN A REASONABLE PERIOD OF TIME THE IMPEDIMENTS TO ELECTRONIC SURVEILLANCE WILL BE REMOVED AND OUR SOCIETY'S WINDOW OF VULNERABILITY CLOSED. WITHOUT ENACTMENT OF THE ADMINISTRATION'S PROPOSAL, ONE OF OUR MOST EFFECTIVE WEAPONS AGAINST NATIONAL AND INTERNATIONAL DRUG TRAFFICKING, TERRORISM, ESPIONAGE, ORGANIZED CRIME, AND SERIOUS VIOLENT CRIMES WILL BE SEVERELY AND ADVERSELY IMPACTED. WITHOUT ITS ENACTMENT, THE PUBLIC SAFETY, THE NATIONAL SECURITY, AND EFFECTIVE LAW ENFORCEMENT WILL BE IMPERILED.

THE PURPOSE OF THIS LEGISLATION IS TO MAINTAIN TECHNOLOGICAL CAPABILITIES COMMENSURATE WITH EXISTING STATUTORY AUTHORITY -- THAT IS, TO PREVENT ADVANCED TELECOMMUNICATIONS TECHNOLOGY FROM REPEALING DE FACTO THE STATUTORY AUTHORITY ALREADY CONFERRED BY THE CONGRESS. THE PROPOSED LEGISLATION EXPLICITLY STATES THAT THE LEGISLATION DOES NOT ENLARGE OR REDUCE THE GOVERNMENT'S AUTHORITY TO LAWFULLY INTERCEPT THE CONTENT OF COMMUNICATIONS OR INSTALL OR USE PEN REGISTER OR TRAP AND TRACE DEVICES PURSUANT TO COURT AUTHORIZATION. NEITHER DOES IT ALTER THE CURRENT DUTY OF THE SERVICE PROVIDER TO ASSIST LAW ENFORCEMENT AND RECEIVE PAYMENT FOR SUCH ASSISTANCE. NOR DOES IT ALTER EXISTING CAUSES OF ACTION, CIVIL LIABILITY, OR GOOD FAITH DEFENSES.

THE "PURPOSE" SECTION OF THE ACT INDICATES THAT THE ACT IS DESIGNED TO CLARIFY AND DEFINE THE RESPONSIBILITIES OF COMMON CARRIERS, PROVIDERS OF COMMON CARRIER SUPPORT SERVICES, AND TELECOMMUNICATIONS EQUIPMENT MANUFACTURERS. THEY WOULD BE REQUESTED TO PROVIDE THE ASSISTANCE REQUIRED TO ENSURE THAT GOVERNMENT AGENCIES CAN IMPLEMENT COURT ORDERS AND LAWFUL AUTHORIZATIONS TO INTERCEPT THE CONTENT OF WIRE AND ELECTRONIC COMMUNICATIONS AND ACQUIRE CALL SETUP INFORMATION (E.G., DIALED NUMBER INFORMATION), PURSUANT TO THE FEDERAL AND STATE ELECTRONIC SURVEILLANCE AND PEN REGISTER AND TRAP AND TRACE STATUTES. THE "ASSISTANCE" REQUIREMENT THAT IS CLARIFIED AND MORE FULLY DEFINED IS NOT A NEW ONE, BUT RATHER A LONG-STANDING ONE, DATING BACK TO 1970. IN THE ORIGINAL ASSISTANCE PROVISION, CONGRESS EVIDENCED A CLEAR INTENT THAT LAWFUL COURT ORDERS SHOULD NOT BE FRUSTRATED DUE TO A SERVICE PROVIDER'S FAILURE TO PROVIDE NEEDED TECHNOLOGICAL ASSISTANCE AND FACILITIES. THE PROPOSED LEGISLATION CLARIFIES AND DEFINES THE NATURE AND EXTENT OF THE RESPONSIBILITY WHICH ARISES FROM THE UNEQUIVOCAL MANDATE OF THE 1970 LAW.

AN ADDITIONAL PURPOSE OF THE ACT IS TO IMPROVE COMMUNICATIONS PRIVACY PROTECTION FOR USERS OF CORDLESS TELEPHONES, CERTAIN RADIO-BASED DATA COMMUNICATIONS AND NETWORKS, COMMUNICATIONS TRANSMITTED USING CERTAIN PRIVACY-ENHANCING MODULATION TECHNIQUES, AND TO CLARIFY THE LAWFULNESS OF QUALITY CONTROL AND SERVICE PROVISION MONITORING OF ELECTRONIC COMMUNICATIONS ON A PAR WITH WIRE COMMUNICATIONS.

THE LEGISLATION SETS FORTH LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE REQUIREMENTS. THE REQUIREMENTS ARE, BY DESIGN, GENERIC IN NATURE AND ARE INTENDED TO PUT COMMON CARRIERS ON NOTICE AS TO NEEDS OF LAW ENFORCEMENT. THE GOVERNMENT PURPOSELY ESCHEWED SETTING ANY TECHNICAL STANDARDS BECAUSE IT DOES NOT DESIRE TO "DICTATE" PARTICULAR TECHNOLOGICAL SOLUTIONS. IT IS THE GOVERNMENT'S POSITION THAT EACH COMMON CARRIER IS BEST POSITIONED AND QUALIFIED TO DETERMINE HOW IT WILL MEET THE REQUIREMENTS IN THE MOST COST-EFFECTIVE WAY.

THE ARTICULATION OF THESE REQUIREMENTS CONSTITUTES THE FIRST LEGISLATIVE LISTING OF LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE REQUIREMENTS. HOWEVER, MOST OF THESE REQUIREMENTS HAVE BEEN KNOWN TO THE MAJOR LOCAL EXCHANGE CARRIERS, INTEREXCHANGE CARRIERS, AND CELLULAR CARRIERS FOR QUITE SOME TIME.

IN BRIEF, THE REQUIREMENTS SPECIFY THAT COMMON CARRIERS MUST BE ABLE TO PROVIDE FORTHWITH, PURSUANT TO COURT ORDER OR LAWFUL AUTHORIZATION, THE CAPABILITY AND CAPACITY TO PERMIT THE GOVERNMENT TO CONDUCT ELECTRONIC SURVEILLANCE, PEN REGISTER, AND TRAP AND TRACE INVESTIGATIONS EFFECTIVELY. COMMON CARRIERS ARE REQUIRED TO ENSURE THAT THERE IS AN ABILITY TO EXECUTE EXPEDITIOUSLY AND SIMULTANEOUSLY ALL COURT ORDERS AND LAWFUL AUTHORIZATIONS DIRECTED TO THEM. SECOND, THEY ARE REQUIRED TO ENSURE THAT THE CONTENT OF COMMUNICATIONS AND CALL SETUP INFORMATION (DIALING INFORMATION) CAN BE INTERCEPTED, ACQUIRED, AND PROVIDED TO THE LAW ENFORCEMENT AGENCY. IT MUST BE PROVIDED

CONCURRENT WITH THE TRANSMISSION OF THE SUBJECT'S COMMUNICATION, TO THE EXCLUSION OF ANYONE ELSE'S COMMUNICATIONS OR DIALING INFORMATION, AND WITHOUT REGARD TO THE MOBILE NATURE OF THE FACILITY OR SERVICE THAT IS THE SUBJECT OF THE COURT ORDER OR LAWFUL AUTHORIZATION, REGARDLESS OF ANY FEATURES OFFERED BY THE COMMON CARRIER USED BY THE SUBSCRIBER WHO IS THE SUBJECT OF THE COURT ORDERED INTERCEPT. THIRD, THEY ARE REQUIRED TO ENSURE THAT COMMUNICATIONS CAN BE INTERCEPTED AND DIALING INFORMATION ACQUIRED UNOBTRUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH ANY SUBSCRIBER'S TELECOMMUNICATIONS SERVICE. FINALLY, THEY ARE REQUIRED TO ENSURE THAT THE CONTENT OF COMMUNICATIONS AND THE DIALING INFORMATION CAN BE TRANSMITTED TO A LOCATION IDENTIFIED BY THE GOVERNMENT DISTANT FROM THE FACILITY THAT IS THE SUBJECT OF THE INTERCEPTION, FROM THE INTERCEPTION ACCESS POINT, AND FROM THE PREMISES OF THE COMMON CARRIER.

THE BASIS FOR THESE REQUIREMENTS IS EASY TO UNDERSTAND. INASMUCH AS COMMUNICATION INTERCEPTIONS AND DIALED NUMBER ACQUISITIONS INCREASINGLY WILL BE ACTIVATED FROM WITHIN COMMON CARRIER PREMISES, INCLUDING SWITCHING OFFICES, IT IS CRITICAL THAT THERE BE SUFFICIENT CAPACITY TO ACCOMMODATE COMPLETELY THE CONCOMITANT NEEDS OF ALL LAW ENFORCEMENT AND GOVERNMENT AGENCIES.

IT IS CRITICAL FOR LAW ENFORCEMENT AGENCIES TO BE ABLE TO INTERCEPT COMMUNICATIONS AND ACQUIRE DIALING INFORMATION CONCURRENTLY, SO THEY CAN RESPOND IMMEDIATELY TO LIFE-THREATENING CIRCUMSTANCES AND REACT PROMPTLY AND EFFECTIVELY TO CRIMINAL ACTIVITY IN TERMS OF MAKING NEEDED ARRESTS, SEIZING EVIDENCE, AND

INTERDICTING CONTRABAND, SUCH AS DRUGS, ILLEGAL WEAPONS, AND BOMBS. THIS REQUIREMENT ALSO IS IMPORTANT AND CRITICAL IN HELPING LAW ENFORCEMENT AGENCIES "MINIMIZE" THE MONITORING AND RECORDING OF NONCRIMINAL COMMUNICATIONS.

THE REQUIREMENT THAT COMMON CARRIERS HAVE THE ABILITY TO ISOLATE FOR LAW ENFORCEMENT THE COMMUNICATIONS AND DIALING INFORMATION OF THE SUBJECTS OF ELECTRONIC SURVEILLANCE TO THE EXCLUSION OF THE COMMUNICATIONS AND DIALING INFORMATION OF OTHER SUBSCRIBERS IS A BASIC AND A LONG-STANDING ONE. LAW ENFORCEMENT AGENCIES DO NOT WANT TO BE FACED WITH THE PROSPECT OF HAVING TO "SORT THROUGH" A TANGLE OF COMMUNICATIONS WHICH INCLUDE THE COMMUNICATIONS OF INNOCENT INDIVIDUALS WHO HAVE THE MISFORTUNE OF HAVING THEIR COMMUNICATIONS "BUNDLED" OR OTHERWISE COMMINGLED WITH THOSE CRIMINAL CONVERSATIONS OF THE SUBJECT OF COURT-ORDERED INTERCEPTION IN THE TELECOMMUNICATIONS TRANSMISSION PROCESS. (HOWEVER, IF THE "BUNDLING" OF COMMUNICATIONS IS BEING DONE BY THE SUBSCRIBER LAW ENFORCEMENT DOES NOT EXPECT THE COMMON CARRIER TO "UNBUNDLE" THESE COMMUNICATIONS. THIS ABILITY IS BEING CHALLENGED BY THE INCREASED USE OF DIGITAL TRANSPORT, MULTIPLEXING, AND FIBER OPTICS CLOSER TO THE PREMISES OF THE INTERCEPTION SUBJECT.

THE REQUIREMENT PERTAINING TO THE MOBILE NATURE OF SERVICES AND FEATURES DIRECTLY ADDRESSES THE SIGNIFICANT IMPEDIMENTS TO ELECTRONIC SURVEILLANCE BROUGHT ABOUT BY CELLULAR, PERSONAL COMMUNICATIONS SERVICES (PCS), AND OTHER EMERGING MOBILE SERVICES, AS WELL AS FEATURES AND SERVICES WHICH PERMIT

SUBSCRIBERS TO PROGRAM OR OTHERWISE DIRECT COMMUNICATIONS TO ANY FACILITY THEY CHOOSE (E.G., "CALL FORWARDING" AND "FOLLOW ME SERVICE").

THE BASIS FOR THE REQUIREMENT THAT COMMUNICATIONS AND DIALING INFORMATION BE ACQUIRED UNOBTUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH ANY SUBSCRIBER'S SERVICE IS SELF EVIDENT. WITHOUT IT, ELECTRONIC SURVEILLANCE WOULD BE DETECTED BY THE SUBJECT OF THE INTERCEPT AND COMPROMISED.

THE REQUIREMENT THAT INTERCEPTED COMMUNICATIONS OR ACQUIRED DIALING INFORMATION BE RECEIVED AT A LOCATION IDENTIFIED BY LAW ENFORCEMENT AGENCIES DISTANT FROM THE SUBJECT'S FACILITY, FROM THE INTERCEPTION POINT, AND FROM THE PREMISES OF THE COMMON CARRIER IS LIKEWISE NOT NEW AND MAINTAINS CURRENT OPERATING PROCEDURES. THIS REQUIREMENT IS FUNDAMENTALLY IMPORTANT, SINCE WITHOUT IT THE SAFETY OF LAW ENFORCEMENT OFFICERS AND GOVERNMENT EMPLOYEES WOULD BE PUT AT RISK, THE INTERCEPTION EASILY COULD BE COMPROMISED THROUGH DETECTION, AND THE EFFECTIVE EXECUTION OF THE SURVEILLANCE WOULD BE SIGNIFICANTLY DISRUPTED.

THE LEGISLATION CONTAINS A PROVISION ENTITLED "SYSTEMS SECURITY" WHICH IS INTENDED TO MAINTAIN THE HIGHEST LEVELS OF TELECOMMUNICATIONS PRIVACY AND SYSTEMS SECURITY. SINCE COMMUNICATION INTERCEPTIONS AND DIALING INFORMATION ACQUISITIONS INCREASINGLY WILL BE FACILITATED FROM WITHIN COMMON CARRIER PREMISES, INCLUDING SWITCHING FACILITIES AND NETWORK ELEMENTS, IT IS CRITICAL THAT THESE FACILITIES REMAIN HIGHLY SECURE. CONSEQUENTLY, LAW ENFORCEMENT WILL BE REQUIRED TO NOTIFY COMMON

CARRIERS OF ANY INTERCEPTIONS THAT ARE TO BE EFFECTED WITHIN SUCH FACILITIES. FURTHER, COMMON CARRIERS WILL DESIGNATE INDIVIDUALS WHO EXCLUSIVELY WILL HAVE THE ABILITY TO ACTIVATE ALL SUCH INTERCEPTIONS FOR LAW ENFORCEMENT. LAW ENFORCEMENT AND OTHER GOVERNMENT AGENCIES ARE NOT SEEKING THE AUTHORITY OR ABILITY TO REMOTELY ACTIVATE INTERCEPTIONS WITHIN THE PREMISES OF A COMMON CARRIER IN A FASHION THAT BYPASSES PERSONNEL DESIGNATED BY COMMON CARRIER. ALL EXECUTIONS OF COURT ORDERS OR AUTHORIZATIONS WHICH REQUIRE ACCESS TO THE SWITCHING FACILITIES OR OTHER CARRIER PREMISES WILL BE MADE THROUGH THE INDIVIDUALS AUTHORIZED AND DESIGNATED BY THE COMMON CARRIER.

THE FOCUS OF COMPLIANCE IS UPON COMMON CARRIERS WITHIN WHOSE NETWORKS MOST OF THE ELECTRONIC SURVEILLANCE OCCURS AND WHERE MOST OF THE IMPEDIMENTS ARE ENCOUNTERED. COMPLIANCE IS SET FOR WITHIN THREE YEARS, A PERIOD OF TIME CONSIDERED TO BE REASONABLE FOR REMOVING THE IMPEDIMENTS. THE COVERAGE OF COMPLIANCE INCLUDES ONLY NEEDED MODIFICATIONS TO EXISTING SYSTEMS AND NETWORKS, AS WELL AS TO FUTURE SYSTEMS AND NETWORKS (THOSE FIELDDED AFTER THE THREE-YEAR COMPLIANCE PERIOD).

BECAUSE COMMON CARRIERS MUST RELY ON EQUIPMENT MANUFACTURERS AND SUPPORT SERVICE PROVIDERS, THE LEGISLATION PROVIDES THAT COMMON CARRIERS ARE TO CONSULT WITH THESE ENTITIES IN A TIMELY FASHION AND THAT THESE ENTITIES, IN TURN, SHALL MAKE AVAILABLE NEEDED EQUIPMENT AND SERVICES ON A TIMELY AND PRIORITY BASIS, AND AT A REASONABLE AND COST-EFFECTIVE CHARGE.

ENFORCEMENT OF THE LEGISLATION IS VESTED IN THE ATTORNEY GENERAL. THIS IS TO AVOID DISPARATE ENFORCEMENT ACTIONS THROUGHOUT THE COUNTRY IN WAYS THAT COULD BE BURDENSOME FOR COMMON CARRIERS. THE ATTORNEY GENERAL IS AUTHORIZED TO SEEK INJUNCTIVE RELIEF AGAINST COMMON CARRIERS, EQUIPMENT MANUFACTURERS, AND SUPPORT SERVICE PROVIDERS, AS WELL AS TO FILE CIVIL ACTIONS FOR FINES AGAINST COMMON CARRIERS. THE ATTORNEY GENERAL IS ALSO AUTHORIZED TO REQUEST ENFORCEMENT ASSISTANCE FROM THE FEDERAL COMMUNICATIONS COMMISSION. VIOLATORS ARE SUBJECT TO A CIVIL PENALTY OF \$10,000 PER DAY FOR EACH DAY IN VIOLATION. AS A PRACTICAL MATTER, IT IS NOT EXPECTED THAT THESE ENFORCEMENT REMEDIES AND ACTIONS WILL BE REQUIRED, PARTICULARLY WITH REGARD TO RESPONSIBLE COMMON CARRIERS. HOWEVER, WITH APPROXIMATELY 2,000 COMMON CARRIERS NOW IN THE TELECOMMUNICATIONS MARKETPLACE, THE PROSPECT THAT SOME WILL DISREGARD THESE REQUIREMENTS OR RESPOND TO THEM IN A DILATORY FASHION CANNOT BE DISREGARDED.

IN ORDER TO FACILITATE COMPLIANCE WITH THE PROVISIONS OF THIS LEGISLATION, THE ATTORNEY GENERAL IS ENCOURAGED TO CONSULT WITH THE FEDERAL COMMUNICATIONS COMMISSION AND COMMON CARRIER REPRESENTATIVES AND TO UTILIZE COMMON CARRIER STANDARDS BODIES, ASSOCIATIONS, OR OTHER SUCH ORGANIZATIONS TO DISCUSS DETAILS OF THE REQUIREMENTS AND COST-EFFECTIVE APPROACHES.

IN THE DEFINITION OF THE TERM "INTERCEPT," IT IS MADE CLEAR THAT THE LEGISLATION, AS A GENERAL RULE, DOES NOT MAKE COMMON CARRIERS RESPONSIBLE FOR DECIPHERING OR DECRYPTING ENCRYPTED COMMUNICATIONS. AS A GENERAL RULE, LAW ENFORCEMENT

AGENCIES ASSUME THIS RESPONSIBILITY. COMMON CARRIERS ARE REQUIRED TO PROVIDE ONLY THE PLAINTEXT OF ENCRYPTED COMMUNICATIONS WHEN THE ENCRYPTION WAS PROVIDED BY THE COMMON CARRIER AND THE COMMON CARRIER POSSESSES THE INFORMATION NECESSARY TO DECRYPT THE COMMUNICATION.

THE TERM "CALL SETUP INFORMATION" IS ESSENTIALLY THE DIALING INFORMATION ASSOCIATED WITH ANY COMMUNICATION WHICH IDENTIFIES THE ORIGIN AND DESTINATION OF A WIRE OR ELECTRONIC COMMUNICATION OBTAINED THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE PURSUANT TO COURT ORDER. IT DOES NOT INCLUDE ANY INFORMATION WHICH MIGHT DISCLOSE THE GENERAL LOCATION OF A MOBILE FACILITY OR SERVICE, BEYOND THAT ASSOCIATED WITH THE AREA CODE OR EXCHANGE OF THE FACILITY OR SERVICE. THERE IS NO INTENT WHATSOEVER, WITH REFERENCE TO THIS TERM, TO ACQUIRE ANYTHING THAT COULD PROPERLY BE CALLED "TRACKING" INFORMATION.

THE LEGISLATION INCLUDES SEVERAL PROVISIONS THAT ARE INTENDED TO IMPROVE COMMUNICATIONS PRIVACY. THESE INCLUDE THE CONFERRAL OF FULL PRIVACY PROTECTION FOR CORDLESS TELEPHONES, INCLUDING THOSE TRANSMISSIONS OCCURRING IN THE RADIO LINK BETWEEN THE TELEPHONE HANDSET AND BASE STATION. THIS PROVISION RECOGNIZES THAT NEWER GENERATIONS OF CORDLESS TELEPHONES TEND TO AFFORD GREATER PRIVACY PROTECTION TO USERS THAN THOSE PREVIOUSLY MARKETING, BECAUSE LAWFUL NETWORK MONITORING IS ALLOWED FOR ELECTRONIC AS WELL AS WIRE COMMUNICATIONS.

IT IS IMPORTANT TO UNDERSTAND THAT THIS LEGISLATION IS INTENDED TO STAND THE TEST OF TIME AND OVERCOME THE SHORTCOMINGS

OF THE 1970 AMENDMENT. IT IS SPECIFICALLY DESIGNED TO DEAL INTELLIGENTLY AND COMPREHENSIVELY WITH CURRENT AND EMERGING TELECOMMUNICATIONS TECHNOLOGIES AND TO PRECLUDE THE NEED FOR MUCH MORE RESTRICTIVE AND MORE COSTLY LEGISLATION IN FIVE OR TEN YEARS WHEN COURT-AUTHORIZED INTERCEPTIONS WOULD NO LONGER BE POSSIBLE DUE TO FURTHER TECHNOLOGY ADVANCES. ANY LEGISLATION THAT WOULD LIMIT ITS APPLICATION TO TECHNOLOGICAL IMPEDIMENTS ON A "PIECEMEAL" BASIS WOULD BE DISASTROUS. PIECEMEAL LEGISLATION WHICH DEALS ONLY WITH CURRENT PROBLEMS OR SOME OF THE PROBLEMS WOULD RESULT IN COMMON CARRIERS FULLY DEPLOYING NEW TECHNOLOGIES WHICH WOULD IMPEDE ELECTRONIC SURVEILLANCE AND WHICH WOULD CAUSE THE GOVERNMENT TO RETURN TO THE CONGRESS REPEATEDLY. IN THE MEANTIME, THE PUBLIC SAFETY, THE NATIONAL SECURITY, AND EFFECTIVE LAW ENFORCEMENT WOULD BE HARMED AND THE COST OF REMOVING THOSE FUTURE IMPEDIMENTS WOULD BE PROHIBITIVE. INDEED, IN THIS REGARD, BAD LEGISLATION WOULD BE WORSE THAN NO LEGISLATION AT ALL.

WHAT THE LEGISLATION DOES NOT PROPOSE

MUCH OF THE CRITICISM DIRECTED TOWARD THE ADMINISTRATION'S PROPOSAL HAS BEEN MISLEADING OR INCORRECT. I WOULD LIKE TO CLARIFY FOR THE RECORD WHAT THE LEGISLATION DOES NOT PROPOSE.

NO CHANGE IN LEGAL AUTHORITY

FIRST, AS I PREVIOUSLY STATED, THE PROPOSED LEGISLATION DOES NOT SEEK TO EXPAND THE CURRENT LAWS AUTHORIZING THE INTERCEPTION OF WIRE OR ELECTRONIC COMMUNICATIONS. TO THE

CONTRARY, THIS PROPOSAL SIMPLY SEEKS TO MAINTAIN LAW ENFORCEMENT'S ABILITY TO CONDUCT THE TYPES OF SURVEILLANCES CURRENTLY AUTHORIZED IN CHAPTERS 119 AND 206, TITLE 18, U.S.C.; THE FOREIGN INTELLIGENCE SURVEILLANCE ACT; AND THE LAWS IN 37 STATES, THE DISTRICT OF COLUMBIA, PUERTO RICO, AND THE U.S. VIRGIN ISLANDS. IN 1968, CONGRESS CAREFULLY CONSIDERED AND PASSED LEGISLATION SETTING FORTH THE EXACT PROCEDURE BY WHICH LAW ENFORCEMENT CAN OBTAIN COURT AUTHORIZATION TO CONDUCT ELECTRONIC SURVEILLANCE. THE STATUTE DEMANDS THAT LAW ENFORCEMENT USE ELECTRONIC SURVEILLANCE ONLY AS A TECHNIQUE OF LAST RESORT. REQUESTS FOR ELECTRONIC SURVEILLANCE RECEIVE RIGOROUS ADMINISTRATIVE AND JUDICIAL SCRUTINY AND ARE GRANTED ONLY AFTER A FEDERAL DISTRICT COURT JUDGE, OR HIS/HER STATE/LOCAL COUNTERPART, IS SATISFIED THAT ALL THE STATUTORY SAFEGUARDS HAVE BEEN MET AND ALL OTHER REASONABLE INVESTIGATIVE STEPS HAVE FAILED, OR ARE LIKELY TO FAIL. THE PROPOSED LEGISLATION WILL NOT CHANGE THIS.

FURTHERMORE, SERVICE PROVIDERS WILL NOT EXECUTE AN INTERCEPT WITHOUT THE REQUIRED COURT ORDER OR STATUTORY AUTHORIZATION. ANY ATTEMPT TO DO SO BY ANYONE, EITHER INSIDE THE GOVERNMENT OR THE PRIVATE SECTOR, WILL CONTINUE TO BE A VIOLATION OF FEDERAL LAW AND THOSE INDIVIDUALS WILL BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

IN ADDITION, THE PROPOSAL WILL NOT CHANGE WHO CONTROLS ACCESS TO THE COMMUNICATIONS TO BE INTERCEPTED. IN FACT, INTERCEPTION ACCESS POINTS INCREASINGLY ARE LIKELY TO BE ACTIVATED WITHIN THE COMMON CARRIER'S PREMISES, THEREBY SEVERELY

LIMITING THE POTENTIAL FOR ILLEGAL WIRETAPPING. THE PROPOSAL WILL NOT OPEN THE DOOR TO EASY OR WHOLESale WIRETAPPING, NOR DOES LAW ENFORCEMENT ENVISION A MARKED INCREASE IN THE NUMBER OF ELECTRONIC SURVEILLANCE COURT ORDERS THAT WILL BE SOUGHT OR AN INCREASE IN THE TYPES OF INVESTIGATIONS IN WHICH A COURT-AUTHORIZED INTERCEPTION CAN BE GRANTED. THE LEGISLATION DOES NOT, IN ANY WAY, RELAX THE ESTABLISHED STATUTORY AND COURT-IMPOSED REQUIREMENT FOR OBTAINING A COURT ORDER.

THIS PROPOSAL DOES NOT RESTRICT TECHNOLOGY. IT DEALS SOLELY WITH PRESERVING TECHNICAL CAPABILITIES. THE PROPOSED LEGISLATION SEEKS ONLY TO CLARIFY AND MORE CLEARLY DEFINE EXISTING LAW REGARDING THE "TECHNICAL ASSISTANCE" PROVISION BY MAKING IT APPLICABLE AND MEANINGFUL, REGARDLESS OF THE TECHNOLOGY EMPLOYED.

ENCRYPTION

THE PROPOSAL, IN ESSENCE, ONLY ADDRESSES THE TECHNOLOGICAL ISSUE CONCERNING ACCESS TO COMMUNICATIONS AND DOES NOT ALTER THE LEGAL REQUIREMENTS CURRENTLY ASSOCIATED WITH COURT-ORDERED INTERCEPTS. WITH MINOR EXCEPTION WHERE ENCRYPTION WAS PROVIDED BY THE COMMON CARRIER AND THE COMMON CARRIER POSSESS IN THE INFORMATION NECESSARY TO DECRYPT THE INFORMATION, THE LEGISLATION DOES NOT ADDRESS THE ISSUE OF ENCRYPTION. WHILE ENCRYPTION CERTAINLY POSES A PROBLEM FOR LAW ENFORCEMENT, THIS LEGISLATIVE PROPOSAL FOCUSES ONLY ON THE ISSUE OF INTERCEPTION ACCESS WITHIN ADVANCED COMMUNICATIONS NETWORKS. THE TOPIC OF

ACCESS WITHIN ADVANCED TELECOMMUNICATIONS NETWORKS IS DISTINCT FROM ENCRYPTION AND POSES AN IMMEDIATE AND CRITICAL PROBLEM FOR LAW ENFORCEMENT FOR WHICH WE ARE NOW SEEKING A LEGISLATIVE SOLUTION.

NETWORK SECURITY AND RELIABILITY

SOME HAVE RAISED CONCERNS REGARDING THE IMPACT THIS LEGISLATION MIGHT HAVE ON NETWORK SECURITY AND RELIABILITY. CERTAIN SPECIAL INTEREST SPOKESPERSONS HAVE ASSERTED THAT THE LEGISLATION WILL MAKE IT EASIER FOR ANYONE, FROM COMPUTER HACKERS TO FOREIGN SPIES, TO ACCESS AN INDIVIDUAL'S COMMUNICATIONS. THESE FEARS ARE UNFOUNDED AND MISPLACED. FIRST OF ALL, JUST AS NETWORK MAINTENANCE AND AUDIT ACCESS CAN BE ACCOMPLISHED WITH FULL REGARD FOR NETWORK AND SYSTEM SECURITY, SO ALSO CAN LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE ACCESS BE ACCOMPLISHED WITH THE SAME HIGH REGARD FOR SECURITY AND PRIVACY. SECOND, THE PROPOSED LEGISLATION INCLUDES A "SYSTEMS SECURITY" PROVISION WHICH MEANS THAT ONLY DESIGNATED TELEPHONE COMPANY EMPLOYEES WILL ACTIVATE INTERCEPTIONS WHICH ORIGINATE WITHIN TELEPHONE COMPANY PREMISES. THIRD, UNAUTHORIZED ACCESS TO COMMUNICATIONS REMAINS A SERIOUS CRIME WHICH IS ADDRESSED IN THE CURRENT ELECTRONIC SURVEILLANCE STATUTES. ANY UNAUTHORIZED INDIVIDUAL OR GROUP BREACHING COMMUNICATIONS SECURITY AND PRIVACY IS SUBJECT TO PROSECUTION TO THE FULLEST EXTENT OF THE LAW. FOURTH, THIS PROPOSAL WILL NOT INTRODUCE ANY VULNERABILITIES INTO SYSTEMS THAT ARE NOT ALREADY PRESENT. AS TECHNOLOGY EVOLVES AND AS ANY NEW

FEATURES AND SERVICES ARE INTRODUCED, INDUSTRY WILL NECESSARILY PLAN NETWORK SECURITY MEASURES AND COUNTERMEASURES EARLY IN THE DESIGN PHASE AND ADDRESS INTENSIVELY THE ARCHITECTURAL DESIGN FOR NETWORK SECURITY.

THE PROPOSED LEGISLATION FITS WELL WITHIN THE CONTEXT OF THESE ACTIVITIES. BY REQUIRING COMMON CARRIERS TO DEVELOP LAW ENFORCEMENT ACCESS SOLUTIONS WITHIN THEIR OWN NETWORKS, WE ARE BEST ASSURING APPROPRIATE SECURITY. THEREFORE, CONTRARY TO MANY PUBLIC STATEMENTS MADE ON THE SUBJECT, LAW ENFORCEMENT IS NOT SEEKING TO BUILD "BACK DOORS" TO SNEAK INTO COMMON CARRIERS' SYSTEMS. THE PROPOSED LEGISLATION IS NOT SOME DREADED ORWELLIAN PROPHECY COME TRUE. RATHER, THIS LEGISLATIVE PROPOSAL REPRESENTS A RECOGNITION OF LEGITIMATE LAW ENFORCEMENT NEEDS AND A DESIRE TO PROTECT THE AMERICAN PEOPLE.

TO SUPPORT NORMAL OPERATIONS, SERVICE PROVIDERS MUST MANAGE AND MAINTAIN THEIR NETWORKS. THIS IS TERRIBLY IMPORTANT TO THE FBI JUST AS IT IS FOR EVERYONE. LAW ENFORCEMENT ELECTRONIC SURVEILLANCE INTERCEPTION ACCESS TO COMMUNICATIONS WILL BE A STRINGENTLY CONTROLLED EXTENSION OF THE SYSTEM'S FEATURES. WITH ADEQUATE PLANNING, THE INTEGRATION OF LAW ENFORCEMENT'S NEEDS SHOULD BE EASILY ACCOMMODATED WITHIN THE REQUIREMENTS FOR NETWORK SECURITY. TO FURTHER ENHANCE THE PUBLIC'S CONFIDENCE IN THE SECURITY OF OUR COMMUNICATIONS NETWORKS, SUBCOMMITTEE STAFF HAVE RAISED WITH US THE ISSUE OF IMPOSING REPORTING AND AUDITING REQUIREMENTS ON COMMON CARRIES

CONCERNING THEIR IMPLEMENTATION OF AUTHORIZED INTERCEPTS. WE ARE
SUPPORTIVE OF SUCH REQUIREMENTS.

EFFECTS ON NETWORK DESIGN AND TECHNOLOGY

ANOTHER CONCERN THAT HAS BEEN RAISED IS THE POSSIBLE NEGATIVE IMPACT THIS LEGISLATION MIGHT HAVE ON NETWORK DESIGN AND TECHNOLOGY, REQUIRING A BROAD RE-ENGINEERING OF THE NETWORK COMPONENTS. THE PROPOSED LEGISLATION DOES NOT REQUIRE COMMON CARRIERS TO DESIGN THEIR SYSTEMS IN ANY ONE, PARTICULAR WAY. THE PROPOSAL SIMPLY REQUIRES THAT COMMON CARRIERS RESPOND TO THE GENERIC REQUIREMENTS OF LAW ENFORCEMENT AND PROVIDE LAW ENFORCEMENT WITH INTERCEPTION ACCESS AND THE CAPABILITY AND CAPACITY TO INTERCEPT WIRE AND ELECTRONIC COMMUNICATIONS, IN REAL TIME, WHEN AUTHORIZED BY LAW.

THIS LEGISLATION ALSO DOES NOT PROPOSE THAT INDUSTRY DESIGN SYSTEMS WITH THE ABILITY TO WIRETAP AS THE "DESIGN GOAL." LAW ENFORCEMENT IS SIMPLY REQUIRING COMMON CARRIERS TO CRAFT APPROPRIATE SOLUTIONS THAT INTERFACE WITH THEIR NETWORKS' DESIGNS. INDUSTRY IS IN THE BEST POSITION TO DEVELOP REASONABLE AND COST-EFFECTIVE SOLUTIONS AND, AT THE SAME TIME, MAINTAIN THE SECURITY AND RELIABILITY OF THE NETWORKS.

FURTHERMORE, WE ARE UNAWARE OF ANY AUTHORITATIVE INDUSTRY STATEMENT THAT THESE REQUIREMENTS WOULD SIGNIFICANTLY DELAY DEVELOPMENT OF NEW TECHNOLOGIES.

ADDITIONALLY, THIS LEGISLATION DOES NOT PROHIBIT OR IMPEDE THE DEPLOYMENT OF NEW TELECOMMUNICATIONS TECHNOLOGIES.

ADVANCED TECHNOLOGIES SUPPORT A NUMBER OF FEATURES THAT MAKE SYSTEMS MORE INTELLIGENT. THE BASIC TECHNOLOGY UNDERPINNING THE INTRODUCTION OF ADVANCED FEATURES AND SERVICES, WHICH OFTEN IMPEDE ELECTRONIC SURVEILLANCE, LIKELY WILL OFFER SOLUTIONS TO THESE VERY PROBLEMS.

LAW ENFORCEMENT'S REQUIREMENTS WILL NOT DICTATE THE COURSE OR PACE OF TECHNOLOGY. HOWEVER, WITH THIS LEGISLATION, OUR REQUIREMENTS INTENTIONALLY WILL BE INCLUDED, RATHER THAN EXCLUDED, IN THE DEVELOPMENT OF NEW TECHNOLOGY IN MUCH THE SAME FASHION THAT OTHER LEGISLATION REQUIRES NEW TECHNOLOGIES AND PRODUCTS TO TAKE PUBLIC SAFETY INTO ACCOUNT.

COMPETITIVENESS

ANOTHER ISSUE RAISED PERTAINS TO THE EFFECT OF THE LEGISLATION ON AMERICAN COMPETITIVENESS. THE PROPOSED LEGISLATION WILL NOT IN ANY FASHION ADVERSELY AFFECT COMPETITIVENESS. DOMESTICALLY, THE PROPOSED LEGISLATION WOULD MEAN THAT ALL 2,000 COMMON CARRIERS WOULD COMPETE ON A "LEVEL PLAYING FIELD" BECAUSE ALL PROVIDERS WOULD BE REQUIRED TO MEET THE SAME ELECTRONIC SURVEILLANCE SPECIFICATIONS. THE PROPOSED LEGISLATION DOES NOT PROHIBIT U.S. MANUFACTURERS OR INTERNATIONAL SERVICE PROVIDERS FROM DEVELOPING OR DEPLOYING EQUIPMENT OR SERVICE FEATURES FOR SALE OUTSIDE THE UNITED STATES THAT ARE DIFFERENT FROM THAT REQUIRED PURSUANT TO THE PROPOSED LEGISLATION. THIS PROPOSAL ONLY APPLIES TO COMMON CARRIER COMMUNICATIONS SERVICES DEPLOYED WITHIN THE UNITED STATES. IF

ANYTHING, THIS LEGISLATION COULD PROVIDE U.S. INDUSTRY WITH A COMPETITIVE EDGE. OTHER DEMOCRATIC NATIONS WILL VERY LIKELY WANT TELECOMMUNICATIONS SYSTEMS AND EQUIPMENT THAT PRECLUDE SERVICE PROVIDERS FROM DEVELOPING OR DEPLOYING EQUIPMENT OR SERVICE FEATURES NOT CAPABLE OF INTERCEPT.

PRIVACY-BASED OBJECTIONS

A SPOKESPERSON FOR THE AMERICAN CIVIL LIBERTIES UNION (ACLU) HAS STATED ON NUMEROUS OCCASIONS THAT THE ACLU OPPOSES THE PROPOSED LEGISLATION BECAUSE IT WOULD ALLOW LAW ENFORCEMENT TO MAINTAIN TECHNICAL CAPABILITIES COMMENSURATE WITH EXISTING FEDERAL AND STATE LEGAL AUTHORITIES. THIS IS BECAUSE THE ACLU OPPOSES THE EXISTING LEGAL AUTHORITIES -- THOSE FOUND IN THE TITLE III AND FISA STATUTES, AS IT PERSISTS IN THE ERRONEOUS POSITION THAT WIRETAPPING IS UNCONSTITUTIONAL PER SE. THIS RADICAL POSITION IS IN FLAT OPPOSITION TO THE POLICY POSITIONS AND THE CONSTITUTIONAL ANALYSES OF THE EXECUTIVE, LEGISLATIVE, AND JUDICIAL BRANCHES OF BOTH THE FEDERAL AND STATE GOVERNMENTS. THE UNITED STATES SUPREME COURT HELD LONG AGO THAT THE TITLE III WIRETAP STATUTE IS CONSTITUTIONAL. SEE UNITED STATES V. DONOVAN, 429 U.S. 413 (1977).

PRIVACY IS PROTECTED IN THE FEDERAL AND STATE ELECTRONIC SURVEILLANCE STATUTES BY REQUIRING LAW ENFORCEMENT AGENCIES' ADHERENCE TO A NUMBER OF LEGISLATIVELY-CREATED PROTECTIONS THAT FAR EXCEED THE FOURTH AMENDMENT REQUIREMENTS RELATING TO COURT ORDERS BASED UPON PROBABLE CAUSE.

IN FACT, THE PROPOSED LEGISLATION CONTAINS A NUMBER OF PRIVACY-ENHANCING PROVISIONS, SUCH AS EXTENDING FULL PRIVACY PROTECTION TO CORDLESS TELEPHONES, RADIO-BASED ELECTRONIC COMMUNICATIONS, AND COMMUNICATIONS TRANSMITTED USING PRIVACY-ENHANCING MODULATION TECHNIQUES.

THE FALSE "TRANSACTIONAL DATA SCARE"

THE DIGITAL PRIVACY AND SECURITY WORKING GROUP (DPSWG) HAS ATTEMPTED TO INTERJECT A FALSE "TRANSACTIONAL DATA SCARE" INTO THE CURRENT DISCUSSION OF THE NEED FOR LEGISLATION THAT WILL ALLOW LAW ENFORCEMENT TO MAINTAIN ITS ELECTRONIC SURVEILLANCE AND PEN REGISTER/TRAP AND TRACE TECHNICAL CAPABILITIES COMMENSURATE WITH EXISTING LAW.

IN A LETTER TO ME, DATED MARCH 11, 1994, A COPY OF WHICH WAS SENT DIRECTLY TO THE CHAIRMEN, THE DPSWG FALSELY ALLEGES THAT WE ARE SEEKING TO "DICTATE TO INDUSTRY" A NEW CAPABILITY TO ACQUIRE "MINUTE-BY-MINUTE SURVEILLANCE OF INDIVIDUALS" THROUGH TRANSACTIONAL DATA. THIS IS A FALSE ISSUE FOR A NUMBER OF REASONS.

FIRST, AS IS CLEARLY SET FORTH IN THE "PURPOSE" SECTION OF THE PROPOSED LEGISLATION, THE INTENT OF THE LEGISLATION IS TO MAINTAIN EXISTING TECHNICAL CAPABILITIES AND TO "CLARIFY AND DEFINE THE RESPONSIBILITIES OF COMMON CARRIERS ... TO PROVIDE THE ASSISTANCE REQUIRED TO ENSURE THAT GOVERNMENT AGENCIES CAN IMPLEMENT COURT ORDERS AND LAWFUL AUTHORIZATIONS TO INTERCEPT THE CONTENT OF WIRE AND ELECTRONIC COMMUNICATIONS AND ACQUIRE CALL

SETUP INFORMATION UNDER CHAPTERS 119 AND 206 OF TITLE 18 AND CHAPTER 36 OF TITLE 50." (EMPHASIS ADDED.) THESE CHAPTERS HAVE NOTHING TO DO WITH "TRANSACTIONAL INFORMATION" UNDER OUR FEDERAL ELECTRONIC SURVEILLANCE AND PRIVACY LAWS. ALL TELECOMMUNICATIONS "TRANSACTIONAL" INFORMATION IS ALREADY PROTECTED BY FEDERAL LAW AND IS EXCLUSIVELY DEALT WITH IN CHAPTER 121 OF TITLE 18 OF THE UNITED STATES CODE ("STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS"). THE PROPOSED LEGISLATION DOES NOT RELATE TO CHAPTER 121 OF TITLE 18.

SECOND, UNDER FEDERAL LAW, CONGRESS TREATS LAW ENFORCEMENT'S USE OF PEN REGISTERS AND DIALING INFORMATION DIFFERENTLY THAN "TRANSACTIONAL INFORMATION" -- SUCH AS DETAILED TELEPHONE BILLING INFORMATION. THE DIALING INFORMATION DERIVED FROM A PEN REGISTER IS OBTAINED BY LAW ENFORCEMENT AND IS LIMITED TO A SPECIFIC TELEPHONE LINE AND NUMBER. ON THE OTHER HAND, TRANSACTIONAL BILLING INFORMATION IS COMPILED BY TELEPHONE COMPANIES AND CAPTURES BILLING INFORMATION FROM EVERY TELEPHONE A SUBSCRIBER MAY USE DURING THE BILLING PERIOD, SUCH AS CREDIT CARD CALLS, COLLECT CALLS, OPERATOR ASSISTED CALLS, AND THIRD NUMBER BILLING INFORMATION WHICH ARE ASSOCIATED WITH ALL THE DIFFERENT TELEPHONES A SUBSCRIBER MAY USE.

THIRD, CONGRESS HAS ENACTED LEGISLATION THAT REQUIRES LAW ENFORCEMENT TO OBTAIN A COURT ORDER IN ORDER TO OBTAIN "CALL SETUP INFORMATION" THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE, BASED UPON A CERTIFICATION OF AN ATTORNEY FOR THE GOVERNMENT THAT THE INFORMATION LIKELY TO BE OBTAINED IS RELEVANT

TO AN ONGOING CRIMINAL INVESTIGATION. SUCH COURT ORDERS LAST FOR UP TO SIXTY DAYS. ANY RENEWAL REQUIRES THE APPROVAL OF AN APPROPRIATE JUDGE. ON THE OTHER HAND, CONGRESS HAS LEGISLATED THAT "TRANSACTIONAL INFORMATION" CAN BE OBTAINED THROUGH A NUMBER OF LEGAL PROCESSES, INCLUDING SUBPOENAS, WITHOUT RESORT TO COURT ORDERS. SUBPOENAS FOR TRANSACTIONAL INFORMATION TYPICALLY COVER PERIODS OF SIX MONTHS OR LONGER. IN ANY EVENT, LAW ENFORCEMENT IS NOT AUTHORIZED TO OBTAIN NONCRIMINAL, IRRELEVANT INFORMATION ABOUT ANY INDIVIDUAL, AND ANY ACQUISITION OF TRANSACTIONAL INFORMATION OR DIALING-TYPE INFORMATION MUST BE GROUNDED IN RELEVANCY TO A CRIMINAL INVESTIGATION OR INQUIRY.

FOURTH, THE LETTER INDICATES THAT ENACTMENT OF THIS LEGISLATION, WITH REGARD TO MAINTAINING OUR ABILITY TO LAWFULLY ACQUIRE CALL SETUP (DIALING) INFORMATION PURSUANT TO COURT ORDER, WILL SOMEHOW PERMIT LAW ENFORCEMENT TO ACQUIRE SOME NEW INFORMATION THAT IS NOT NOW AVAILABLE. THAT IS SIMPLY UNTRUE. THIS LEGISLATION ENSURES A MAINTENANCE OF THE STATUS QUO AS IT RELATES TO LEGAL AUTHORITIES UNDER CHAPTERS 119 AND 206 OF TITLE 18 AND CHAPTER 36 OF TITLE 50, AND AS IT RELATES TO THE TYPES OF INFORMATION OBTAINABLE THROUGH PEN REGISTER AND TRAP AND TRACE DEVICES USED PURSUANT TO THE COURT ORDER.

FIFTH, UNLIKE THE GOVERNMENT'S PROPOSED LEGISLATION, WHICH SPECIFICALLY ASSERTS NO INTENTION TO ALTER THE EXISTING LAWS REGARDING THE CONDUCT OF ELECTRONIC SURVEILLANCE AND THE INSTALLATION AND USE OF PEN REGISTER AND TRAP AND TRACE DEVICES, THE DPSWG, BY INTERJECTING A FALSE TRANSACTIONAL DATA SCARE, IS

APPARENTLY SEEKING TO REPEAL CHAPTER 206 OF TITLE 18 AND THE PEN REGISTER AND TRAP AND TRACE AUTHORIZATIONS FOUND IN CHAPTER 36 OF TITLE 50. AS EXPLAINED ABOVE, CALL SETUP INFORMATION (THAT IS DIALING INFORMATION) IS OBTAINED THROUGH THE USE OF PEN REGISTER AND TRAP AND TRACE DEVICES. IN THE DPSWG LETTER REFERRED TO ABOVE, IT STATES: "LEGISLATION SHOULD APPLY TO "CALL SETUP INFORMATION" ONLY WHEN THAT INFORMATION IS INCIDENT TO A WARRANT ISSUED FOR WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS AS SET FORTH IN 18 U.S.C. 2518 [TITLE III]." TO ACCEPT THIS RADICAL POSITION ON PRIVACY WOULD MEAN, FOR EXAMPLE, THAT ANYTIME AN FBI AGENT SIMPLY SOUGHT TO ACQUIRE A TELEPHONE NUMBER DIALED BY A CRIMINAL SUBJECT THROUGH THE USE OF A PEN REGISTER, HE/SHE SHOULD BE REQUIRED BY LAW TO DRAFT A 30-40 PAGE TITLE III AFFIDAVIT, AND SEND IT TO WASHINGTON, D.C., FOR THE DEPUTY ASSISTANT ATTORNEY GENERAL OF THE CRIMINAL DIVISION TO REVIEW AND AUTHORIZE, BEFORE TAKING IT TO A FEDERAL DISTRICT COURT JUDGE FOR REVIEW AND APPROVAL. FRANKLY, SUCH A NOTION IS ABSURD AND IS WILDLY INCONSISTENT WITH CURRENT LAW.

ALLEGATIONS OF "TRACKING" PERSONS

LAW ENFORCEMENT'S REQUIREMENTS SET FORTH IN THE PROPOSED LEGISLATION INCLUDE AN ABILITY TO ACQUIRE "CALL SETUP INFORMATION." THIS INFORMATION RELATES TO DIALING TYPE INFORMATION -- INFORMATION GENERATED BY A CALLER WHICH IDENTIFIES THE ORIGIN, DURATION, AND DESTINATION OF A WIRE OR ELECTRONIC COMMUNICATION, THE TELEPHONE NUMBER OR SIMILAR COMMUNICATION

ADDRESS. SUCH INFORMATION IS CRITICAL TO LAW ENFORCEMENT AND, HISTORICALLY, HAS BEEN ACQUIRED THROUGH USE OF PEN REGISTER OR TRAP AND TRACE DEVICES PURSUANT TO COURT ORDER.

SEVERAL PRIVACY-BASED SPOKESPERSONS HAVE CRITICIZED THE WORDING OF THE DEFINITION REGARDING THIS LONG-STANDING REQUIREMENT, ALLEGING THAT THE GOVERNMENT IS SEEKING A NEW, PERVASIVE, AUTOMATED "TRACKING" CAPABILITY. SUCH ALLEGATIONS ARE COMPLETELY WRONG.

SOME CELLULAR CARRIERS DO ACQUIRE INFORMATION RELATING TO THE GENERAL LOCATION OF A CELLULAR TELEPHONE FOR CALL DISTRIBUTION ANALYSIS PURPOSES. HOWEVER, THIS INFORMATION IS NOT THE SPECIFIC TYPE OF INFORMATION OBTAINED FROM "TRUE" TRACKING DEVICES, WHICH CAN REQUIRE A WARRANT OR COURT ORDER WHEN USED TO TRACK WITHIN A PRIVATE LOCATION NOT OPEN TO PUBLIC VIEW. SEE UNITED STATES V. KARO, 468 U.S. 705, 714 (1984). EVEN WHEN SUCH GENERALIZED LOCATION INFORMATION, OR ANY OTHER TYPE OF "TRANSACTIONAL" INFORMATION, IS OBTAINED FROM COMMUNICATIONS SERVICE PROVIDERS, COURT ORDERS OR SUBPOENAS ARE REQUIRED AND ARE OBTAINED.

IN ORDER TO MAKE CLEAR THAT THE ACQUISITION OF SUCH INFORMATION IS NOT BEING SOUGHT THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE, AND IS NOT INCLUDED WITHIN THE TERM "CALL SETUP INFORMATION," WE ARE PREPARED TO ADD A CONCLUDING PHRASE TO THIS DEFINITION TO EXPLICITLY CLARIFY THE POINT: "... , EXCEPT THAT SUCH INFORMATION [CALL SETUP INFORMATION] SHALL NOT INCLUDE ANY INFORMATION THAT MAY DISCLOSE THE PHYSICAL LOCATION

OF A MOBILE FACILITY OR SERVICE BEYOND THAT ASSOCIATED WITH THE NUMBER'S AREA CODE OR EXCHANGE."

SUMMARY

IN SUMMARY, IT IS MY VIEW THAT THE DIGITAL TELEPHONY ISSUE IS THE NUMBER ONE LAW ENFORCEMENT, PUBLIC SAFETY, AND NATIONAL SECURITY ISSUE FACING US TODAY. THE MAINTENANCE OF AN EFFECTIVE ELECTRONIC SURVEILLANCE CAPABILITY IS ESSENTIAL TO OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES. THIS INVESTIGATIVE TECHNIQUE IS A UNIQUE AND INDISPENSABLE WEAPON AGAINST NATIONAL AND INTERNATIONAL DRUG-TRAFFICKING ORGANIZATIONS, ORGANIZED CRIME SYNDICATES, TERRORIST GROUPS, AND VIOLENT CRIMINAL CONSPIRACIES. WITHOUT AN EFFECTIVE ELECTRONIC SURVEILLANCE CAPABILITY, OUR LAW ENFORCEMENT AND INTELLIGENCE AGENCIES WILL NOT BE ABLE TO PROTECT THE PUBLIC ADEQUATELY OR ACQUIRE THE EVIDENCE NEEDED TO PUT SOME OF SOCIETY'S MOST DANGEROUS FELONS IN JAIL. RECENT EFFORTS TO ENSURE SUBSTANTIAL JAIL TIME FOR VIOLENT, HARDENED CRIMINALS WILL BE UNDERCUT, IF WE IN LAW ENFORCEMENT FIRST CANNOT IDENTIFY THEM, ARREST THEM, AND OBTAIN THE COMPELLING EVIDENCE REQUIRED TO SECURE THEIR CONVICTIONS.

AS YOU ARE AWARE, AFTER AN EXTENSIVE REVIEW OF THIS SERIOUS PROBLEM THE ADMINISTRATION HAS CONCLUDED THAT FEDERAL LEGISLATION IS THE ONLY VIABLE MEANS OF SOLVING THE SO-CALLED "DIGITAL TELEPHONY" PROBLEM. THE TECHNOLOGICAL IMPEDIMENTS TO COURT-ORDERED ELECTRONIC SURVEILLANCE, WHICH ARE THE UNINTENDED

BY-PRODUCTS OF ADVANCED DIGITAL TELEPHONY, CONSTITUTE A MAJOR NATIONWIDE OBSTACLE TO EFFECTIVE LAW ENFORCEMENT. TO DATE, NUMEROUS COURT ORDERS HAVE BEEN FRUSTRATED, IN WHOLE OR IN PART, BY THESE IMPEDIMENTS. LEFT UNADDRESSED, THIS PROBLEM WILL SOON GROW TO DANGEROUS PROPORTIONS. THE FEDERAL BUREAU OF INVESTIGATION AND THE ENTIRE FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT COMMUNITY ARE COMPLETELY UNIFIED IN OUR ASSESSMENT THAT IMPEDIMENTS WHICH HINDER OR PRECLUDE COURT-ORDERED ELECTRONIC SURVEILLANCE MUST NOT BE ALLOWED TO STAND.

THE DECISION TO PRESS FOR LEGISLATION WAS NOT REACHED LIGHTLY. OVER THE LAST FOUR YEARS, WE HAVE MADE SUBSTANTIAL EFFORTS TO RESOLVE THIS MATTER THROUGH NUMEROUS MEETINGS WITH LEADERS IN THE TELECOMMUNICATIONS INDUSTRY. INCLUDED IN THESE EFFORTS HAS BEEN A LAW ENFORCEMENT/INDUSTRY TECHNICAL WORKING GROUP WHICH WAS SPECIFICALLY INSTITUTED BY INDUSTRY TO "SOLVE THE PROBLEM." EVEN THOUGH WE HAVE MET FOR NEARLY TWO YEARS (AND HAVE MUTUALLY BENEFITTED FROM THE DISCUSSIONS), THERE IS NO MECHANISM FOR ASSURING THE TIMELY, COMPREHENSIVE DEVELOPMENT AND IMPLEMENTATION OF THE REQUIRED TECHNOLOGICAL SOLUTIONS. IN FACT, THE CHAIRMAN OF THE INDUSTRY TECHNICAL WORKING GROUP ACKNOWLEDGES THIS FUNDAMENTAL SHORTCOMING AND PROBLEM. OBTAINING THESE SOLUTIONS CAN NO LONGER BE LEFT TO CHANCE. FEDERAL LEGISLATION REPRESENTS THE ONLY REALISTIC PROSPECT FOR OBTAINING, WITH CERTAINTY, THE TIMELY AND COMPREHENSIVE DEVELOPMENT AND IMPLEMENTATION OF THE REQUIRED TECHNOLOGICAL SOLUTIONS BY THE TELECOMMUNICATIONS INDUSTRY.

AS I INDICATED, THE PROPOSED LEGISLATION IS FOCUSED ON "MAINSTREAM" TELECOMMUNICATIONS SERVICE PROVIDERS, ON "COMMON CARRIERS," WHO HISTORICALLY HAVE BEEN SUBJECT TO REGULATION. THIS LEGISLATIVE PROPOSAL SHOULD BE MORE ACCEPTABLE TO THE COMMON CARRIERS. FOR INSTANCE, THE ELECTRONIC SURVEILLANCE REQUIREMENTS HAVE BEEN CLARIFIED; A NETWORK "SYSTEMS SECURITY" PROVISION ADDED, WHICH SPECIFIES THAT ALL PREMISES-BASED INTERCEPTS (SWITCHES, NETWORK ELEMENTS) MUST BE ACTIVATED EXCLUSIVELY BY COMMON CARRIER PERSONNEL; A MANDATE THAT SUPPORT SERVICE PROVIDERS AND EQUIPMENT MANUFACTURERS, UPON WHOM THE CARRIERS RELY, WILL FURNISH THE TIMELY COOPERATION REQUIRED TO PERMIT COMPLIANCE; AN ATTORNEY GENERAL "CONSULTATION" PROVISION DESIGNED TO FACILITATE DISCUSSION AND COST-EFFECTIVE APPROACHES TO COMPLIANCE; AND, IMPORTANTLY, FEDERAL GOVERNMENT PAYMENT TO COMMON CARRIERS FOR REASONABLE AND COST-EFFECTIVE CHARGES DIRECTLY ASSOCIATED WITH ATTAINING COMPLIANCE WHICH ARE INCURRED WITHIN THE THREE YEAR PERIOD SET FOR COMPLIANCE.

ALSO INCLUDED IN THE LEGISLATION ARE AMENDMENTS TO THE FEDERAL CRIMINAL ELECTRONIC SURVEILLANCE LAWS ("TITLE III") WHICH IMPROVE COMMUNICATIONS PRIVACY PROTECTION: PRIVACY PROTECTION FOR HANDHELD "CORDLESS" TELEPHONES ON A PAR WITH WIRELINE AND CELLULAR TELEPHONES, CLARIFICATION OF PRIVACY PROTECTION FOR ELECTRONIC COMMUNICATIONS TRANSMITTED BY RADIO, AND PRIVACY PROTECTION FOR COMMUNICATIONS TRANSMITTED USING SECURITY-ENHANCING MODULATION TECHNIQUES.

LAW ENFORCEMENT FULLY SUPPORTS THE INTRODUCTION AND DEPLOYMENT OF ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AS A MEANS OF SHARING INFORMATION, EDUCATING AMERICANS, AND INCREASING OUR PRODUCTIVITY. IN PARTICULAR, WE ARE EXTREMELY SUPPORTIVE OF THE VICE PRESIDENT'S INITIATIVE TO CREATE A NATIONAL INFORMATION INFRASTRUCTURE FOR THE BENEFIT OF ALL AMERICANS. AS WE ALL EMBRACE THE VAST POTENTIAL OFFERED BY ADVANCED TECHNOLOGY, AND ADVANCED TELECOMMUNICATIONS TECHNOLOGY IN PARTICULAR, IT IS CRITICAL THAT THE EQUITIES OF OUR LAW ENFORCEMENT AND INTELLIGENCE AGENCIES NOT BE FORGOTTEN OR IGNORED. HOWEVER, IT WOULD BE WRONG FOR ALL OF US AS PUBLIC SERVANTS, BOTH WITHIN THE EXECUTIVE AND LEGISLATIVE BRANCHES OF GOVERNMENT, TO KNOWINGLY ALLOW THIS INFORMATION SUPERHIGHWAY TO JEOPARDIZE THE SAFETY AND ECONOMIC WELL-BEING OF LAW-ABIDING AMERICANS BY BECOMING AN EXPRESSWAY AND SAFE HAVEN FOR TERRORISTS, SPIES, DRUG DEALERS, MURDERERS, AND THUGS.

I DO NOT RELISH THE THOUGHT OF BEING THE FIRST FBI DIRECTOR TO TELL A FATHER AND MOTHER THAT WE WERE UNABLE TO SAVE THEIR SON OR DAUGHTER BECAUSE ADVANCED TELECOMMUNICATIONS TECHNOLOGY PRECLUDED THE TELEPHONE COMPANY FROM PROVIDING US WITH LAWFUL ACCESS TO THE CRIMINAL CONVERSATIONS THAT WOULD HAVE PREVENTED THE UNTIMELY DEATH OF AN INNOCENT CHILD. NOR DO I WANT THE PRESIDENT PLACED IN THE POSITION OF HAVING TO TELL THE AMERICAN PUBLIC THAT WE IN LAW ENFORCEMENT COULD NOT PREVENT A VIOLENT TERRORIST ACT DIRECTED AGAINST INNOCENT AMERICANS IN A

MAJOR METROPOLITAN AREA SOLELY BECAUSE OF ADVANCED
TELECOMMUNICATIONS TECHNOLOGY.

IT IS IMPERATIVE THAT CONGRESS PROMPTLY ENACT THE
ADMINISTRATION'S PROPOSED LEGISLATION THAT WILL SOLVE THIS
SERIOUS PROBLEM ON A TIMELY AND COMPREHENSIVE BASIS. EVERY DAY
THAT PASSES IN WHICH THIS PROBLEM REMAINS UNRESOLVED, THE LONGER
THE SAFETY AND ECONOMIC WELL-BEING OF THE AMERICAN PUBLIC ARE
UNNECESSARILY PLACED AT RISK. I LOOK FORWARD TO WORKING WITH
EACH ONE OF YOU AND THIS CONGRESS REGARDING THE ENACTMENT OF THIS
IMPORTANT LEGISLATIVE INITIATIVE.

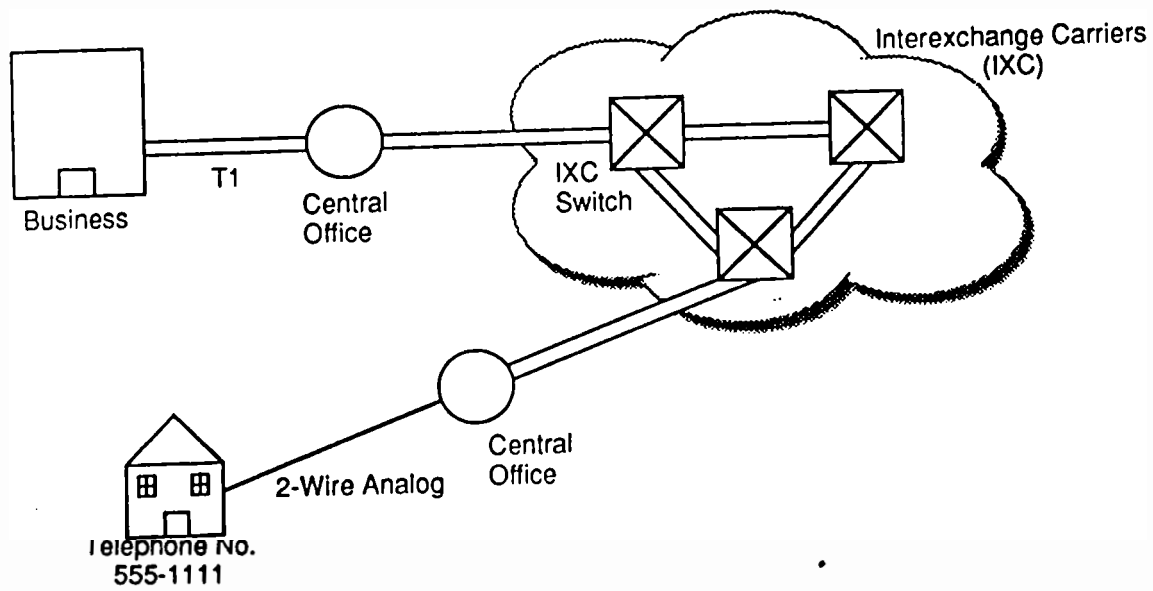
THANK YOU MR. CHAIRMEN AND THE MEMBERS OF THESE
SUBCOMMITTEES FOR PROVIDING ME THIS OPPORTUNITY TO TESTIFY AND
PROVIDE YOU WITH INFORMATION CONCERNING THE MOST IMPORTANT PUBLIC
SAFETY AND NATIONAL SECURITY ISSUES FACING US TODAY.

"TITLE III" INTERCEPTIONS ¹					
Year	Original Interception Applications Authorized			Reported Results	
	State	Federal	Total	Arrests	Convictions ²
1982	448	130	578	2,870	1,886
1983	440	208	648	2,890	2,007
1984	512	289	801	3,719	2,429
1985	541	243	784	4,178	2,616
1986	504	250	754	3,830	2,447
1987	437	236	673	3,225	1,956
1988	445	293	738	3,830	2,404
1989	453	310	763	4,199	2,205
1990	548	324	872	3,167	1,327
1991	500	356	856	2,189	2,185
1992	579	340	919	2,685	607
Total	5,407	2,979	8,386	36,782	22,069

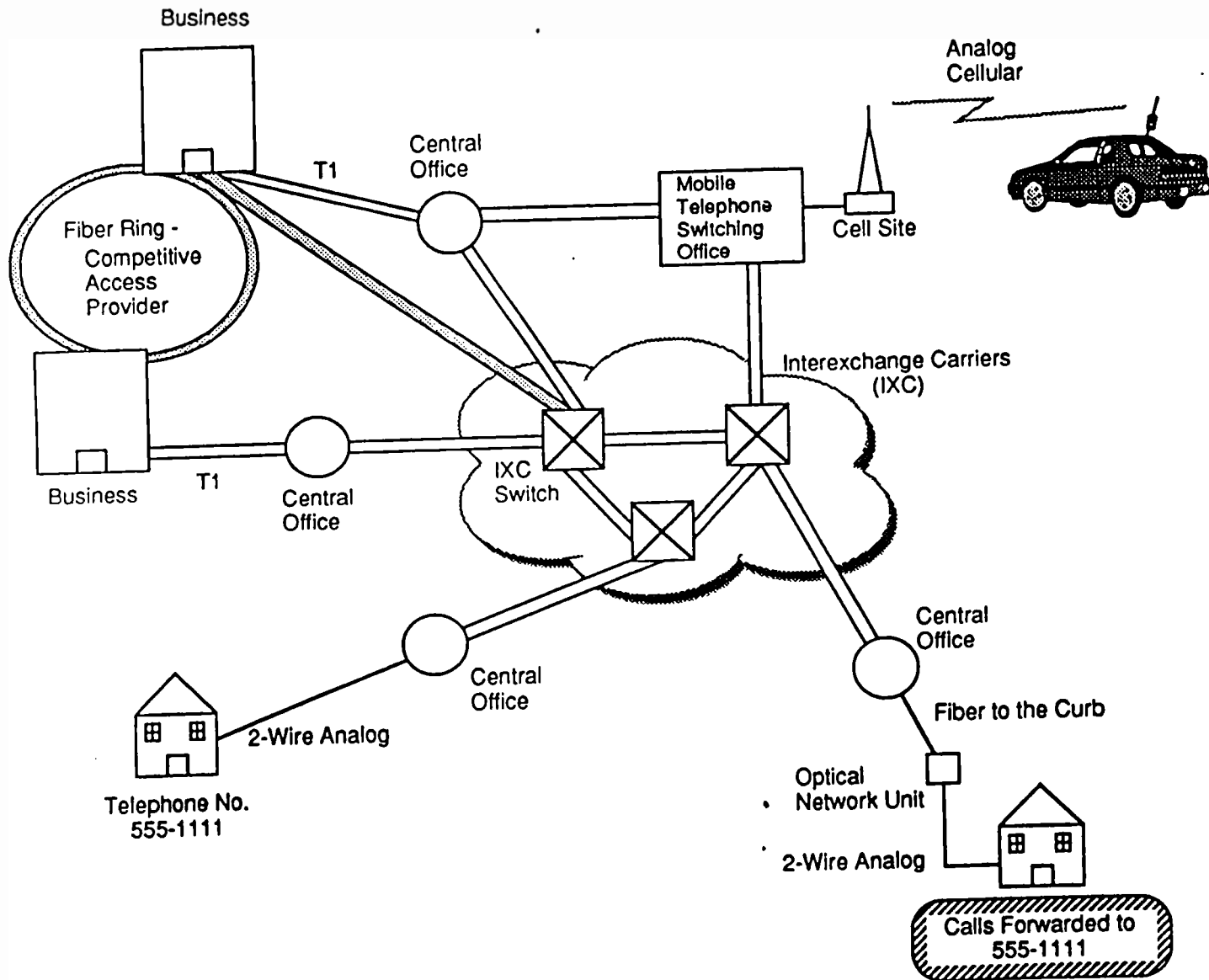
¹ Administrative Office of the United States Courts, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS (WIRETAP REPORT) (1983 - 1992).

² A substantial number of prosecutions are ongoing and total convictions will not be reported for several years. Convictions continue to be reported as a result of interceptions going as far back as 1982. Unfortunately, the reporting of convictions appears to lag substantially behind the actual convictions and there are indications that convictions that should be reported by State prosecutors and judges are not actually reported.

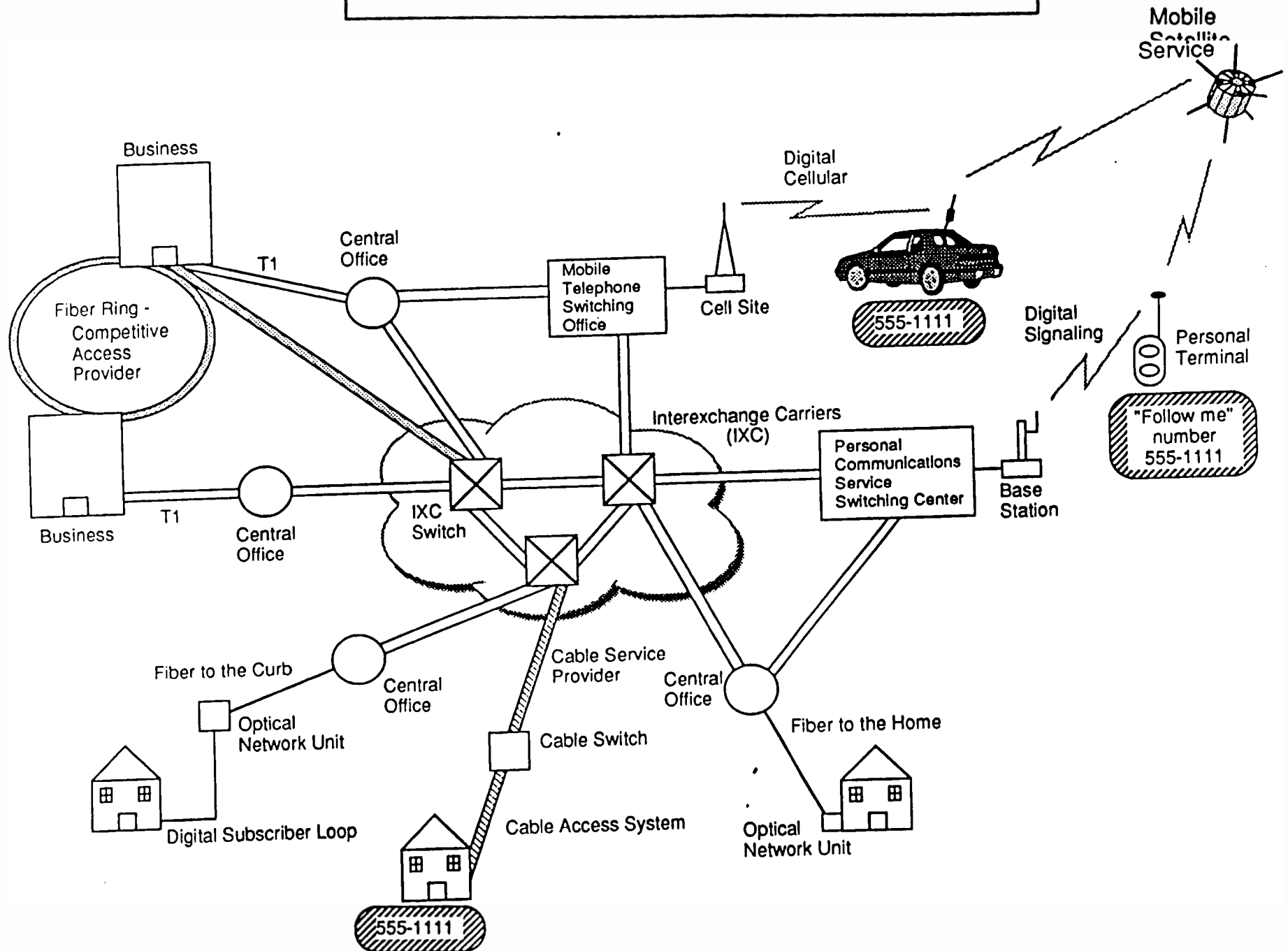
PAST OPERATING ENVIRONMENT



PRESENT OPERATING ENVIRONMENT



FUTURE OPERATING ENVIRONMENT





U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

January 5, 1994

Mr. Casimir S. Skrzypczak
President
NYNEX Science and Technologies, Inc.
120 Bloomingdale Road
White Plains, New York 10605

Dear Mr. Skrzypczak:

Upon receipt of your November 8, 1993, letter, my staff and I conducted a careful and detailed review of the results of the industry working group, which was formed at the request of industry, in March 1992 to address the electronic surveillance requirements of our Nation's state and federal law enforcement agencies. According to senior telecommunications executives, this group was to be "the approach" to address law enforcement's concerns in this area. Although the efforts of industry have been useful to a degree, an honest and candid assessment of the results achieved to date, unfortunately, leads me to conclude that this body does not appear to be equipped or able to develop and implement the solutions that are needed to remove the current and emerging impediments which prevent or hinder law enforcement agencies in executing court orders for electronic surveillance. Although I have held out hope that the industry working group, the Alliance for Telecommunications Industry Solutions (ATIS), and the Electronic Communications Service Providers Committee (ECSPC) would provide a mechanism for achieving solutions and removing the impediments, this recent assessment compels me to acknowledge that these efforts have been inadequate.

As I mentioned in my letter of September 28, 1993, at the outset, back in March 1992, we were pleased with and supportive of the committee's mission to resolve this significant threat to the public safety, national security, and effective law enforcement. To aid in the initiative, we have devoted FBI technical experts and engineers to this process, as well as funding a telecommunications consulting firm to facilitate meetings, provide subject matter expertise, and prepare written contributions. Also, as I previously mentioned, some of the industry representatives have worked hard and appear to have been

Mr. Casimir S. Skrzypczak

sincere in their efforts to reach solutions. However, some companies have not supported these efforts and others have not contributed meaningfully to the effort. In my estimation, this is a result of the voluntary basis and elective nature of the working group and committee approach. Particularly troubling is the fact that new service providers who are now entering the marketplace are unaware of law enforcement's requirements, and efforts by the FBI to have these requirements brought to the attention of industry standards bodies, such as the one now considering Personal Communications Services (PCS) systems, were not supported by industry representatives in the committee.

I believe that in order to successfully accommodate law enforcement's needs and to ensure that electronic surveillance responsibilities are discharged as new technologies emerge, a mechanism must exist that, in a certain and comprehensive fashion:

- Identifies fully law enforcement's electronic surveillance requirements to the telecommunications industry;
- Prompts the technical solutions necessary to meet the requirements of law enforcement;
- Assures timely implementation of these solutions into the telecommunications industry's existing and emerging technologies; and
- Addresses the cost issues associated with the technical solutions and their implementation.

Time has shown that the ECSPC, by itself, is not capable of achieving our goal of ensuring the ability of law enforcement to perform electronic surveillance without fail within existing and emerging telecommunications systems.

As I have previously indicated, the efforts of many committee members have been greatly appreciated by law enforcement. However, it is apparent that the recommended industry approach, the ECSPC, cannot address all of the necessary elements I have listed above. In fact, several committee members have made the point that, as matters stand, only an individual company can determine whether or not it is willing to pursue and implement solutions once they are identified.

Mr. Casimir S. Skrzypczak

It is my view that the committee process should be a mechanism for discussing law enforcement needs and identifying technical solutions. Committee products thus far, such as those reflected in the ISDN, Digital Loop Carriers, and Cellular action teams' written recommendations, have not included solutions, but rather have largely only restated law enforcement's current abilities and limitations in performing electronic surveillance in these technical environments--information which the FBI itself provided nearly two years ago. In the main, these products observe the need for the development of solutions to meet law enforcement needs, but they do not provide these solutions. Inasmuch as the committee is not empowered to resolve cost and other issues key to the implementation of solutions, the lack of meaningful and timely solutions to these technological problems will continue.

As we have indicated previously, we shall continue our active participation in the committee process. However, given the results to date, we are also obligated to pursue other approaches which will ensure law enforcement's continued ability to protect the safety and economic well-being of the American public through the use of this essential investigative technique.

Sincerely yours,

James K. Kallstrom
Special Agent in Charge

March 1, 1994

Office for Telecommunications
Industry Solutions

Exchange Carriers Standards Association

Problem Solvers to the
Telecommunications Industry

200 G Street, NW
Suite 500
Washington DC 20005

202 525 6250
Fax: 202 393 5453

Casimir S. Skrzypczak
Chairman
INYNEX Corporation

Frank D. Reese
Vice Chairman
North Pittsburgh Systems Inc.

Gregory L. Thoms
Treasurer
GTE Telephone Operations

George L. Edwards
President
ATIS

Susan M. Miller
Secretary & General Counsel
ATIS

COMMITTEES

Committee 1:
Telecommunications

Carrier Liaison Committee

Industry Forum

Information Industry
Liaison Committee

Protective Engineers Group

Standards Committee (S)

Electronic Communications
Service Provider Committee

Telecommunications
Committee (T)

Mr. James K. Kallstrom
Special Agent in Charge, Special Operations Division
Federal Bureau of Investigation
26 Federal Plaza
New York, NY 10278

Dear Jim,

I am writing in response to your letter of January 5, 1994, in which you expressed your concerns regarding industry efforts to address the electronic surveillance requirements of state and federal law enforcement agencies.

First, let me say that your observations regarding the functioning of the Electronic Communications Service Provider Committee (ECSP) and its progress to date in resolving issues are understandable. These comments included: the Committee is not equipped to implement the technical solutions which it identifies; some companies have not supported these efforts and others have not contributed meaningfully to the effort; and, efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all representatives on the Committee. However, these observations which you find troubling are aspects of the committee process which are fundamental to the operation and interest of open industry forums.

One of the basic principles of any inter-industry committee or forum is that solutions reached are proposals for voluntary implementation by the participants: recommendations are non-binding. While each participant is committed to good faith discussions and consideration of timely implementation, each company represented also reserves fully independent judgment in terms of any implementation. This tenet of operation serves a number of purposes, a key one being that it mitigates the legal/antitrust risks of conducting these discussions in any industry meeting.

The forum process also ensures that there is careful consideration of all views and objections, appropriate notification and opportunity for the industry to review and provide comments on any proposed solution, and ultimate resolution by consensus. While there is no guarantee, the fact that all participants have been a part of these sensitive discussions, have been afforded due process, and have willingly expended the necessary resources in the development of a solution, more often than not results in strong incentives to implement. It simply may not produce the direct and open commitment to implement solutions at the Committee level that you appear to be looking for.

As I am sure you are aware, most of the solutions developed or being discussed are costly to implement, and can require months, even years to develop. Quite frankly, decisions of this magnitude require review by higher levels of management than those representatives present at the ECSP Committee. Industry sends the subject matter experts to these meetings to develop the technical solutions. Typically, industry does not send representatives who are authorized to make business decisions which may involve large expenditures. While you may view that as a shortcoming of this industry process, I believe that federal agencies operate in the same fashion.

Another characteristic of industry forums is that participating companies do not support and/or contribute to efforts equally. Participants tend to gravitate toward and contribute to those issues in which they have the most interest or the greatest business need. They rely on other participants to provide leadership on the remaining issues. Over time, leadership and contributions tend to balance. Evaluating an individual company's commitment to the process by its level of participation on a single issue can possibly provide a distorted view. The fact that a particular company is not among the leaders on a particular issue does not mean it is not aware or does not care about what is being discussed. The minutes or notes of all meetings, as well as the contributions discussed, are available to all participants for review and comment; and I assure you they are scrupulously reviewed. The stakes are simply too high for them to be ignored. Even though resolutions and recommendations are non-binding, no company wishes to be part of a consensus it cannot ultimately support.

Your concern that efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all industry representatives on the Committee, has proved short lived. At the October meeting the Committee agreed to provide a contribution to the Joint Experts Meeting (JEM) on Privacy and Authentication for Personal Communications held November 8-12. It was reported at the December 1993 Committee meeting that at the JEM the law enforcement requirements were presented and

discussed. The Committee observed that the "objective to raise awareness of the needs of law enforcement to support surveillance were met." At the most recent meeting of the ECSP Committee, the PCS action team was empowered by the full committee to prepare and submit contributions to a number of standards bodies addressing PCS issues. The initial reluctance of the Committee to support this effort was no doubt due to the short turn-arounds required to prepare and approve contributions, and the fact that both industry and law enforcement continue to insist that nearly all Committee documents be considered proprietary. The standards process is an open, public process which requires that all contributions submitted be non-proprietary. Similarly, if new service providers are to become aware of law enforcement's requirements, those requirements must be publicly available. To date, the Committee has been reluctant to publicize these requirements in the belief that to do so will serve to highlight current shortcomings.

Even though discussions between law enforcement and industry have been ongoing for some time, this particular committee, which is co-chaired by industry and law enforcement, and its incumbent operating principles, has been in existence for less than one year. Participants are only now gaining the mutual respect required to bring forth meaningful solutions. You note the fact that the Committee's products to date merely "observe the need for the development of solutions to meet law enforcement needs." I see this as a necessary step forward. If meaningful solutions are to result, all participants must first understand that there is in fact a problem, not that one participant, or one group of participants, says so. Now that the Committee recognizes the problems, it can proceed to identify and develop appropriate solutions.

I understand your obligation to pursue whatever approaches you deem necessary to ensure law enforcement's continued ability to conduct the lawful intercept of communications. However, whatever those other approaches may be, and whatever results those approaches may yield, it will still be necessary for industry and law enforcement to work together to identify and develop suitable technical solutions. I believe the ECSP Committee is the appropriate forum for that purpose.

Sincerely,

Casimir S. Skrzypczak
ATIS Chairman

Organized Crime Appendix

The President's Commission on Organized Crime stated the following conclusions in its report, The Edge: Organized Crime, Business and Labor Unions:

- If unchecked, organized crime can take over, own, and operate legitimate business. It can also control entire industries. The ways in which industry can be affected are by the increased price of items due to theft, bribery (kick-backs), price fixing and the control of trade.
- The control of the marketplace by organized crime is also obtained by the control of unions and by monopolizing power in specific industries.
- Through the control of unions, payoffs can be demanded to ensure labor peace. Businesses comply with the labor union's demands rather than lose profits or lose business. Another deleterious effect of organized crime control is through the illegal utilization of union funds. At the time of the report of the PCOC, union benefit funds had cumulative assets of over \$51 billion. Influence in the unions on a local level, if strong enough, may lead to control of the union at the international level.
- The costs of labor racketeering are hard to trace. The Commission estimated that millions of dollars in workers' labor union dues were stolen from the unions through embezzlement, lost through illegal loans, and taken through extortionate and illegal fees paid to trust and service fund providers.

As a result, the U.S. public is forced to pay higher commodity costs because of organized crime's control. Examples cited by the Commission of the various types of economic loss are:

- Amalgamated Local 355, an independent union in Queens, New York, lost nearly \$2 million in a kickback and embezzlement scheme in the mid-1970s. The scheme involved the union's secretary/treasurer and a well-known real estate developer.
- The control of the concrete industry by the LCN in New York, as brought out in the LCN Commission indictment, was demonstrated in evidence which showed that over the period 1981 - 1984, the 2% skim collected on the total cost of poured concrete, on the delivery of it to the job site, and on the attendant labor costs could range anywhere from \$1.6 to \$3.5 million. This figure was estimated on the control of the concrete industry alone. Increased construction costs then lead to higher overall building project costs and increased rental rates, etc. Essential evidence supporting this prosecution was derived from electronic surveillance.

Through the utilization of electronic surveillance, Federal and state investigations continue to have a significant impact upon organized crime groups. In Fiscal Year 1991, at the Federal level, there were 239 recorded convictions and 246 indictments of LCN members and associates. In addition, civil RICO complaints spawned by the criminal investigations were filed against 25 individuals and/or entities, and judgments were entered against 23. Aggressive use of the seizure and forfeiture provisions of the RICO statute yielded \$17,554,865. Over \$11,779,106 in fines were levied against convicted individuals; recoveries and restitutions totaling \$22,881,539 were obtained; and \$7,044,625 in potential economic losses were prevented. A few recent cases, wherein electronic surveillance played a critical role, illustrate the importance of maintaining the efficiency of this investigative technique.

- Commercial seafood and longshoremen dock-loading industries. For over 70 years, organized crime, and particularly the Genovese LCN family, had dominated and controlled the Fulton Fish Market and its immediate environment in New York City. Through electronic surveillance which spanned over two years, the government acquired substantial evidence as to the influence and control of organized crime in the seafood industry and the labor unions related to it. As a result, in October 1987, a civil RICO complaint was filed against the Genovese LCN crime family, certain unions controlled by organized crime, and a number of LCN members and associates. In 1988, in a landmark RICO decree and judgment, the Fulton Fish Market was placed under the oversight of a court-appointed administrator. Judgments in this civil RICO action permanently bar the Genovese LCN crime family and other defendants from having any future dealings in that seafood market.

Although it is difficult to quantify the impact of the government's intervention into this industry, the enormous economic and social costs associated with the LCN's control of this market have been significantly reduced. Illegal activities such as hijacking, gambling, robbery, burglary, loansharking, extortion, murder, narcotics trafficking, and labor racketeering flourished in the Market's environment while under the dominion of the LCN. These activities have dramatically abated with the imposition of the consent and default judgments. The court-appointed administrator and other independent sources of information, such as the media, report that the Fulton Fish Market has sales approximating two billion dollars annually. Seafood that passes through the market is bought and sold throughout the United States. Illegal activity at the Market has inflated seafood costs by \$1 - \$2 dollars per pound and virtually every household in America has absorbed that cost. By a conservative estimate, the American public has been spared literally millions of dollars in increased seafood costs as a result of this investigation.

- International Longshoremen's Association. This investigation focused primarily upon corruption on the New York and New Jersey waterfront, the second largest port in the world. The civil RICO complaint names as defendants the International Longshoremen's Association (ILA), their executive boards, six local labor unions, and 32 present or former officials of these ILA locals, 21 of whom are identified as members or associates of the Gambino and Genovese LCN crime families, and the "Westies" criminal gang. Twelve additional individuals are identified in the complaint as members or associates of the Gambino and Genovese LCN families and the Westies, and several employers in industries affecting waterfront commerce are named for purposes of obtaining adequate relief.

The complaint alleges that the LCN figures have used these locals and their various affiliated benefit funds to conduct a pattern of racketeering activity on the waterfront, which includes murder, extortion, embezzlement of union funds, illegal labor and benefit fund payments and mail fraud. To prove such wide-ranging conspiracies, the type of evidence needed typically requires substantial reliance upon electronic surveillance-based information.

These investigations, which heavily relied upon electronic surveillance, demonstrated an extraordinary breadth of control by the Genovese LCN family over waterfront activity that extended from the New York - New Jersey piers all the way to the Port of Miami. This pervasive control by organized crime over the waterfront extends back to the turn of the century. Organized crime obtained this control by its early recognition that to transport goods to the eastern seaboard, markets often required passage through the New York/New Jersey waterfront, and that this transportation terminal point presented a labor intensive bottleneck. To control waterfront labor, thus, was

to exercise tremendous leverage over the entire shipping industry, effect the commerce of a huge section of the American economy, and ultimately to drive up prices of a myriad of commodities sold in the United States.

There are numerous other examples where, through the use of court-ordered electronic surveillance, major economic harm was abated. The nationwide investigation into organized crime-labor racketeering influence in the union health and dental care industry has resulted in the termination of frauds and kickbacks which cost unions and insurance companies millions of dollars. In one investigation, sixteen different FBI field offices were involved, eight of which conducted extensive electronic surveillance. At the conclusion of the investigation in September, 1988, seven separate Federal Grand Jury indictments were returned in Atlanta, Chicago, Baltimore, San Diego, and San Francisco, charging ten individuals and five corporations with numerous Federal violations including RICO, conspiracy, mail fraud, wire fraud, and labor racketeering. As a result of this investigation, ten health care executives were convicted, the U.S. Public Health Service changed its bidding procedures nationwide, SAFECO Insurance Company terminated its practice of paying double commissions to insurance agents nationwide, and spin-off investigations resulted in the conviction of a Federal judge and two labor-related, organized crime leaders.

Electronic surveillance was extensively utilized in the landmark civil RICO investigation called "Liberatus" which resulted in the formal break up of LCN control over the nation's largest union, the International Brotherhood of Teamsters. The LCN's grip over this union had been intact since the 1950s. As a result, for the first time in decades the nation's largest union is free from organized crime control and corruption, and the continued pillage of union funds has ceased.

MAIL-IT REQUESTED: AUGUST 2, 1995

104SR3

CLIENT: WHITE-CCU
LIBRARY: NEWS
FILE: ALLNWS

YOUR SEARCH REQUEST AT THE TIME THIS MAIL-IT WAS REQUESTED:

("DIGITAL TELEPHONY" OR "TELEPHONE CARRIER COMPLIANCE" OR WIRETAP! W/2 BILL OR
LAW) W/20 JUSTICE OR "CIVIL FINES" OR BUDGET AND DATE AFT 12/31/1994 AND
NOT MEXICO

NUMBER OF STORIES FOUND WITH YOUR REQUEST THROUGH:

LEVEL 1... 31

LEVEL 1 PRINTED

THE SELECTED STORY NUMBERS:

6,8,9,23,24,25

DISPLAY FORMAT: FULL

SEND TO: SCHWARTZ, MARTIN
DOJ-CRIM-ADM
CRIMINAL DIVISION - ADM
1400 NEW YORK AVENUE, N.W.
BOND BUILDING
WASHINGTON DISTRICT OF COLUMBIA 20530

*****04358*****

LEVEL 1 - 6 OF 31 STORIES

Copyright 1995 Warren Publishing, Inc.
Communications Daily

June 13, 1995, Tuesday

SECTION: Vol. 15, No. 113; Pg. 8

LENGTH: 597 words

BODY:

Administration generally supported antiterrorism legislation (HR-1710) sponsored by House Judiciary Committee Chmn. Hyde (R-Ill.). In testimony Mon. before Hyde's panel, Deputy Attorney Gen. Jamie Gorelick said, however, that Administration disagreed with his proposal that common carrier records, including telephone records, given to investigators under special new procedure be disclosed publicly in 180 days. She said that requirement would jeopardize long investigations. Gorelick also disagreed with Hyde proposal to pay for digital telephony conversions, saying it was necessary to make certain that law enforcement continue to have access to digital wiretaps. Hyde bill would create new Dept. of Justice Telecommunications Carrier Compliance Fund that would continue-until 2000. Administration proposes to finance fund with 40% surcharge on non-IRS civil monetary penalties, but under Hyde bill that would end Oct. 1, 1998 and bill would authorize \$100 million in FY 1996, \$305 million in FY 1997 and \$80 million in FY 1998 of funds that would be collected from surcharge to be applied to digital telephony. Rep. Skaggs (D-Colo.) testified in favor of bill (HR-1638) he introduced with Judiciary panel member Schiff (R-N.M.) that would set up separate inspector gen. with jurisdiction to monitor constitutional questions generated as result of antiterrorist activity by govt. agencies. Skaggs said measure was needed because antitrust matters cross agency lines. Hyde said he didn't see need for creating such position.

Adelphia agreed to buy cable systems with 108,000 subscribers from 4 small operators for total of nearly \$178 million. Purchases include Southeast Fla. cable systems owned by Fairbanks Communications, plus others owned by Eastern Telecom and Robinson Cable TV in Pittsburgh area, and New England systems of First Carolina Cable TV. Adelphia said each of purchases would add to existing clusters. Systems will be owned by Olympus Communications, joint venture of Adelphia and FPL Group. Olympus also said it completed \$475-million financing deal with group of 21 lenders.

Ninth U.S. Appeals Court, San Francisco, has been asked by broadcasters not to relitigate fairness doctrine issues that they claim have been fully considered by FCC and other courts. In filing by Coalition for a Healthy Cal. on 1994 ballot issue, group claimed doctrine is mandated by statute. RTNDA and NAB said that other federal courts have "repeatedly affirmed" 1987 FCC order repealing doctrine. Even if legislative intent is in doubt, 9th Circuit "must defer to the FCC's view" that doctrine wasn't codified into law, broadcasters said. Also, they argued, Coalition argument is moot since no relief could be granted as election is over and ballot issue was resolved in Coalition's favor. Also, for court to reinstitute doctrine would be unconstitutional, NAB and RTNDA said.

93-48["at" symbol]fcc.gov is new FCC e-mail address for anyone who wants to express views on children's TV. Comr. Chong announced number in e-mail hookup last week to discuss kidvid issues. She said Commission rulemaking on

Communications Daily, June 13, 1995

children's TV (CD April 6 p5) is designed to explore "ways to increase the amount of information to parents about when kids' educational TV shows will be shown." She asked for public's input on current state of children's programming, stressing that "parents should be involved in helping choose programs for their kids to watch."

Clarification: Eleven equipment companies have joined CableLabs' Cable/Information Technology Convergence Forum (CD June 12 p11).

LANGUAGE: ENGLISH

LOAD-DATE: June 13, 1995

LEVEL 1 - 8 OF 31 STORIES

Copyright 1995 Information Access Co., a division of Ziff Communications Co.
Telecom Publishing Group

FCC Report

June 1, 1995

SECTION: No. 11, Vol. 14

LENGTH: 509 words

HEADLINE: ADMINISTRATION SEEKS MONEY TO FINANCE DIGITAL WIRETAP LAW

BODY:

Two of the three proposed means for raising the \$500 million to reimburse telcos for compliance with the digital wiretap bill may be seriously flawed.

And the third means, a straight appropriation from the U.S. Treasury, is politically unpalatable since it puts the extent of the government's financing of the law before a money-cautious committee. If approved, the law might take money from the budgets of the Department of Justice (DOJ) or the Federal Bureau of Investigation (FBI). Last year, the FBI pushed for the digital wiretap law, saying technological advances and rising demand to execute wiretaps have thwarted law enforcement access to such surveillance.

The use of a direct appropriation would put the funding matter before Congress's appropriations committee, a more cost-conscious venue than either chambers' judiciary committees. The latter committees last year held hearings on what became the digital wiretap law and endorsed the bill despite the industry's claim it could place as much as \$1 billion in new costs on telcos' shoulders.

Of the two alternatives to a direct appropriation, one involves the government adding a 40 percent surcharge to the civil fines ordered by federal courts. This plan, put forth by the Clinton administration, could be overwhelmed by the collection problems endemic with the government's criminal fines system. In Congressional testimony a year ago this month, a General Accounting Office (GAO) administrator revealed that, in 1991, one-third of all federal criminal fines were more than three- years-old - so old the DOJ recommended they be written off.

Nonetheless, this appears to be the administration's preferred route. The administration's proposed fiscal 1996 budget identifies it as the way to raise the \$100 million worth of reimbursements it would make available to telcos next year.

The other of the two less-solid funding alternatives, according to a source with the Senate Finance Committee, is to have the first installment on the \$500 million fund come out of whatever is left over from the funds authorized by S. 735, the Senate "anti-terrorism bill." That bill, though, has since been combined with the "recission bill," a set of federal budget cuts that the Senate passed earlier this month - and which Clinton has threatened to veto.

Of the two alternatives, this is the least likely, though it too would prevent a reduction in DOJ or FBI funds.

FCC Report , June 1, 1995

In a speech to the United States Telephone Association (USTA) last month, FBI Director William Freeh suggested the \$100 million would be the first installment on a funding system that would contain a balloon payment of several hundred million dollars in a couple of years. This would speed the industry's conversion by making more money available sooner, rather than increasing the federal reimbursement fund in \$100 million allotments each year for the next five years.

However, Freeh did not say how the government would come by the money.

Copyright 1995 Capitol Publications, Inc.

LANGUAGE: ENGLISH

PTS-ACC-NO: 2783019

PTS-LOAD-DATE: 1995 Week 23

LOAD-DATE: June 08, 1995 0000022-0000023 P26381 SGD

LEVEL 1 - 23 OF 31 STORIES

Copyright 1995 Information Access Co., a division of Ziff Communications Co.
Telecom Publishing Group

FCC Report

May 4, 1995

SECTION: No. 9, Vol. 14

LENGTH: 706 words

HEADLINE: DESPITE BOMBING, PRIVACY GROUPS WILL FIGHT WIRETAP LAW'S FUNDS

BODY:

Two privacy groups still plan to cut or eliminate funds for the 1994 digital wiretap act despite a political climate favoring increased police powers and the administration's effort to fund the law "off the books."

The American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) say they want the act's \$500 million cost voted on directly by Congress, a move that could trim or eliminate the funding.

Claiming the FBI already has sufficient wiretapping power to prevent another terrorist attack, ACLU lawyer Don Haines said the wiretap law's funding "could be better spent on necessary government functions."

Rather than seek an increase in the FBI's budget, the administration wants the wiretap law's funding to come from a 30 percent increase in the civil and criminal fines levied by federal courts. The administration has included the law's \$100 million first-year cost in its proposed 1996 budget, which will not get voted on until late this year. By then, anger over the Oklahoma City bombing may have cooled.

The law requires telephone companies to expand the wiretapping capacity they make available to law enforcement agencies. The changes needed at telco central offices will total in the billions of dollars, said Roy Neel, president of the United States Telephone Association (USTA).

To settle the FBI-telco battle over who should bear the bill's cost, the bill was modified to have the government pay the first \$500 million. However, actual appropriation of the money was left to the new Congress.

By financing the law via an increase in federal fines, the administration neatly avoids putting the controversial law before the House Appropriations Committee, where budget cuts are the order of the day and there's a danger of re-opening the battle over the law's privacy impact.

Instead, the funding issue would go before the FBI-friendly House Judiciary Committee, which must approve the increased fines.

The ACLU, said a privacy source, will fight that effort and also will call on the Appropriations Committee to divert the resulting funds to other governmental uses.

FCC Report , May 4, 1995

EPIC policy analyst Dave Banisar claimed the funding scheme is a "Rube Goldberg contraption," but admitted that "the climate's changed" in the wake of the Oklahoma City bombing.

Last week, the Senate Judiciary Committee's anti-terrorism subcommittee held the first of several hearings on the administration's new anti-terrorism proposal. The proposal expands FBI wiretap powers to include conducting "roving wiretaps," or a tap involving several telephones.

The 1994 digital wiretap act arose from the FBI's claim that police agencies nationwide were finding their wiretapping stymied by a limited number of tapping "ports" on central office (CO) equipment and the increasing use of digital transmission technology. The FBI cited 183 instances and EPIC responded by requesting the data underlying that total.

The heavily-edited information provided by the FBI showed that less than a third of the problems were related to CO capacity, the main issue the law addresses, Banisar charged.

During last year's debate on the bill, privacy groups like EPIC said they feared the amount of the bill's funding would directly relate to the amount of wiretapping the FBI would soon be engaged in.

Underlying their concern, sources say, is a fear the FBI will expand its wiretap powers to encompass the Internet, the anything-goes network where innocent e-mail travels alongside bomb-making recipes being shared among "militia" groups.

In the minds of some Internet surfers, the digital wiretap law "would open it up" to future federal tapping, said USTA lobbyist Larry Clinton.

(USTA plans a day-long seminar May 11 on the implications of the law, which it wants fully funded.)

During last week's Senate hearing, Sen. Edward Kennedy, D-Mass., said his staff was able to download a "terrorist handbook" after spending just 10 minutes on the Internet. He called the network "a major issue" in the fight against terrorism. Sen. Diane Feinstein, D-Calif., said she doubted the First Amendment covered dissemination of such materials.

Copyright 1995 Capitol Publications, Inc.

LANGUAGE: ENGLISH

PTS-ACC-NO: 2750738

PTS-LOAD-DATE: 1995 Week 19

LOAD-DATE: May 08, 1995 0000018-0000019 P25935 SGD

LEVEL 1 - 25 OF 31 STORIES

Copyright 1995 Federal Document Clearing House, Inc.
Federal Document Clearing House Congressional Testimony

May 1, 1995, Monday

SECTION: CAPITOL HILL HEARING TESTIMONY

LENGTH: 5129 words

HEADLINE: TESTIMONY May 01, 1995 RONALD K. NOBLE UNDER SECRETARY TREASURY
SENATE APPROPRIATIONS TREASURY, POSTAL SERVICE, AND GENERAL GOVERNMENT FEDERAL
BUILDING SAFETY

BODY:

Testimony of Ronald K. Noble

Under Secretary of the Treasury for Enforcement

Senate Appropriations Subcommittee on Treasury,

Postal Service and General Government

DEPARTMENT OF THE TREASURY

STATEMENT OF RONALD K. NOBLE

UNDER SECRETARY (ENFORCEMENT)

MAY 1, 1995

BEFORE THE SENATE COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEE ON TREASURY, POSTAL SERVICE,

AND GENERAL GOVERNMENT

GOOD AFTERNOON MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE. TODAY I AM
ACCOMPANIED BY THE DIRECTOR OF THE SECRET SERVICE, ELJAY BOWRON AND THE
ASSOCIATE DIRECTOR OF THE BUREAU OF ALCOHOL, TOBACCO, AND FIREARMS, CHARLIE
THOMSON.

IT IS AN UNSPEAKABLE TRAGEDY THAT BRINGS US TOGETHER TODAY. THE EVENTS OF
APRIL 19TH, PERHAPS, HAVE FOREVER CHANGED SOME OF OUR PERCEPTIONS ABOUT OUR
SOCIETY. WHAT REMAINS IMMUTABLE, HOWEVER, IS THE ABILITY OF ALL GOOD AMERICANS
TO PULL TOGETHER IN TIMES OF CRISES. WE HAVE SEEN THIS IN THE SEARCH AND RESCUE
OPERATIONS IN OKLAHOMA CITY, AND WE HAVE SEEN THIS IN THE PUBLIC'S CHARITABLE
OUTPOURINGS. WE ALSO HAVE SEEN THIS SPIRIT AT WORK IN THE EXCEPTIONAL
COOPERATIVE EFFORTS OF LAW ENFORCEMENT IN THE AFTERMATH OF THE BOMBING.

THE TREASURY DEPARTMENT PLAYS A CENTRAL ROLE IN THE FIGHT AGAINST TERRORISM.
OUR ENFORCEMENT BUREAUS PROTECT THE MOST VISIBLE TERRORIST TARGETS IN THE U.S.,
ENFORCE LAWS DIRECTED AT THE MOST COMMON INSTRUMENTS OF TERROR, PROTECT AGAINST
THE SMUGGLING OF WEAPONS OF MASS DESTRUCTION, AND ENFORCE ECONOMIC SANCTIONS
AGAINST COUNTRIES AND GROUPS THAT PROMOTE TERRORISM.

FDCH Congressional Testimony, May 1, 1995

ALSO, I AM PLEASED TO TELL YOU THAT THERE IS OUTSTANDING COOPERATION AND JOINT EFFORT AMONG FEDERAL LAW ENFORCEMENT AGENCIES IN ATTACKING THE DOMESTIC TERRORISM PROBLEM. ATF, FBI, SECRET SERVICE, CUSTOMS, IRS, THE TREASURY DEPARTMENT, AND THE JUSTICE DEPARTMENT ARE SHARING INFORMATION ABOUT THE CRIME THREAT POSED BY CERTAIN ORGANIZED GROUPS.

DOMESTIC TERRORISM IS A BROAD CONCEPT WITHOUT A PRECISE DEFINITION. WHEN I USE THAT TERM TODAY, I AM REFERRING TO INDIVIDUALS OR GROUPS WITHIN THE UNITED STATES WHO REJECT THE LEGITIMATE AUTHORITY OF THE UNITED STATES GOVERNMENT, WHO DO NOT RECOGNIZE THE VALIDITY OF FEDERAL LAW, OR WHO ADVOCATE THE OVERTHROW OF THE UNITED STATES GOVERNMENT, AND WHO USE OR PLAN TO USE VIOLENCE OR TO OTHERWISE VIOLATE FEDERAL LAW IN FURTHERANCE OF THESE OBJECTIVES.

WE HAVE SEEN DOMESTIC TERRORISM IN THE FORM OF THE UNABOMBER WHO HAS STRUCK 16 TIMES SINCE 1978, KILLING THREE AND WOUNDING 23 OTHERS. A SAN FRANCISCO-BASED TASK FORCE COMPRISED OF ATF, FBI, AND THE POSTAL INSPECTION SERVICE IS INVESTIGATING THIS CASE. EXPLOSIVES TECHNICIANS AND AGENTS IN ATF FIELD OFFICES NEAREST THE SITE OF THE BOMBINGS (IN EIGHT STATES) ALSO HAVE BEEN INVOLVED CLOSELY. AFTER HIS MOST RECENT ATTACK WHICH KILLED A MAN IN SACRAMENTO ON APRIL 25, 1995, LETTERS WERE RECEIVED FROM THE UNABOMBER. THESE LETTERS AND OTHER LEADS ARE BEING EXAMINED TO ADD TO THE BOMBER'S PROFILE AND TO DETERMINE HIS MOTIVE; AND IT IS HOPED, LEAD TO HIS ARREST.

TREASURY'S ENFORCEMENT AGENCIES BELIEVE THAT DOMESTIC TERRORISM HAS BEEN GROWING STEADILY. WE HAVE NOTED AN ESCALATION IN VIOLENT INCIDENTS DURING THE PAST DECADE. BETWEEN 1983 AND 1993, THE NUMBER OF YEARLY BOMBINGS IN THE UNITED STATES MORE THAN TRIPLED. BOMBING DEATHS AND INJURIES WERE AT AN ALL TIME HIGH IN 1993 WITH 49 DEATHS AND 1,323 INJURED. THE OKLAHOMA CITY BOMBING WILL MAKE 1995 THE MOST DEADLY YEAR, YET.

OUR BEST ESTIMATE IS THAT IN THE PAST FIVE YEARS, THE VAST MAJORITY OF BOMBING INCIDENTS HAVE INVOLVED CRIMINAL DESTRUCTION OF PROPERTY OR NON-TERRORIST RELATED REVENGE. NEVERTHELESS, IT IS CLEAR THAT THERE IS AN INCREASING TENDENCY AMONG SOME GROUPS TO ENGAGE IN ANTI-GOVERNMENT AND ANTI-LAW ENFORCEMENT VIOLENCE.

CIVILIANS, AS WELL AS FEDERAL AND LOCAL LAW ENFORCEMENT PERSONNEL, HAVE BEEN THREATENED, HARASSED, SURVEILLED, ASSAULTED, AND MURDERED. FEDERAL EMPLOYEES, SUCH AS IRS AUDITORS, EXERCISING THEIR LAWFUL DUTIES HAVE BEEN CONFRONTED BY RESISTANCE, SOMETIMES ARMED, BY GROUPS THAT CHALLENGE THE AUTHORITY OF THE FEDERAL GOVERNMENT.

SCOPE OF THE PROBLEM

ACCORDING TO THE STATE DEPARTMENT, WHICH HAS PRINCIPAL RESPONSIBILITY FOR INTERNATIONAL TERRORIST MATTERS, THERE WERE 321 INTERNATIONAL TERRORIST ATTACKS DURING 1994. SIXTY-SIX OF THEM WERE ANTI-U.S. ATTACKS. THE NUMBER OF INTERNATIONAL AND ANTI-U.S. ATTACKS IN 1994 WAS A 23-YEAR LOW AND IT WAS A DECREASE OF 25% FROM 1993. NOTWITHSTANDING THOSE IMPROVED STATISTICS, WORLDWIDE CASUALTIES WERE 314 PERSONS KILLED AND 663 WOUNDED.

NEVERTHELESS, TREASURY'S ENFORCEMENT AGENCIES SEE NEW OPPORTUNITIES FOR INTERNATIONAL TERRORISM TO WIDEN IN SCOPE. WITH THE DISSOLUTION OF THE SOVIET UNION, AND THE END OF ITS CENTRALIZED CONTROL OVER NUCLEAR MATERIALS AND ASSOCIATED TECHNOLOGIES, WE ANTICIPATE INCREASED TERRORIST PROBLEMS. WEAPONS

FDCH Congressional Testimony, May 1, 1995

PROCUREMENT NETWORKS ARE BECOMING MORE ADVANCED AND CLANDESTINE.

TO COMBAT THESE PROBLEMS, TREASURY, THROUGH THE U.S. CUSTOMS SERVICE HAS A LONGSTANDING TRADITION OF OPERATING IN A FRAMEWORK OF INTERNATIONAL COOPERATION WITH FOREIGN CUSTOMS AGENCIES IN 126 COUNTRIES. THROUGH JOINT OPERATIONS, TACTICAL INTELLIGENCE, AND MUTUAL ASSISTANCE TREATIES, CUSTOMS HAS THE ABILITY TO DETECT AND DISMANTLE INTERNATIONAL SMUGGLING AND PROLIFERATION NETWORKS. THE ILLEGAL ACQUISITION NETWORKS WHICH SUPPORT INTERNATIONAL TERRORISM ARE BECOMING MORE SOPHISTICATED AND CLANDESTINE.

CUSTOMS RECENTLY HAS MADE A NOTABLE SHIFT IN IT'S ENFORCEMENT MISSION TO EMPHASIZE THE DETECTION AND DEVELOPMENT OF SYSTEMS WHICH WILL EXPOSE SUSPICIOUS INDIVIDUALS AND CARGO (I.E., AUTOMATED EXPORT SYSTEM, OUTBOUND STRATEGY). THIS CAPABILITY WILL WARN FEDERAL AUTHORITIES OF TERRORIST ACTIVITIES BEFORE PEOPLE ARE HURT OR BUILDINGS DESTROYED.

ATF ALSO IS CONTINUING ITS INTERNATIONAL TRAFFIC IN ARMS (I.T.A.R.) PROGRAM, WHICH IS DESIGNED TO CURTAIL INTERNATIONAL ARMS TRAFFICKING. THE I.T.A.R. PROGRAM WAS DEVELOPED WHEN IT BECAME APPARENT THAT FIREARMS ORIGINATING FROM THE UNITED STATES WERE BEING RECOVERED WORLDWIDE IN SUCH CRIMINAL ACTS AS NARCOTICS TRAFFICKING AND TERRORISM.

RESOURCES

THE ADMINISTRATION HAS SUBMITTED A FUNDING PACKAGE TO YOU WHOSE PURPOSE IT IS TO ENSURE THAT THE FEDERAL GOVERNMENT HAS ADEQUATE RESOURCES TO PROTECT OUR COUNTRY FROM TERRORIST ACTIVITIES. ADDITIONAL FUNDING IS BEING SOUGHT FOR EMERGENCY EXPENSES OF THE BOMBING OF THE ALFRED P. MURRAH FEDERAL BUILDING IN OKLAHOMA CITY, AND RELATED ANTI-TERRORISM EFFORTS, INCLUDING THE PRESIDENT'S ANTI-TERRORISM INITIATIVE.

THE OVERALL PACKAGE SEEKS \$150 MILLION FOR FY 1995, \$500 MILLION FOR 1996, AND \$1.5 BILLION FOR FY 1995-1999 (FIVE YEAR TIME FRAME). THIS INCLUDES ALL INVOLVED FEDERAL AGENCIES BUT PRINCIPALLY DOJ AND TREASURY. THE PROPOSAL REQUESTS \$24 MILLION AND 200 POSITIONS FOR TREASURY ENFORCEMENT IN FY 1995.

* ATF: \$16.2 MILLION AND 175 EMPLOYEES FOR A PERMANENT NATIONAL RESPONSE TEAM, FORENSICS LAB, EXPLOSIVES INSPECTIONS, COUNTERTERRORISM ANALYSTS, AND RELATED EQUIPMENT AND TRAVEL.

* SECRET SERVICE: \$3.8 MILLION TO UPGRADE AND REPLACE EXISTING WEAPONRY AND PROTECTIVE GEAR TO PROVIDE ENHANCED PROTECTION OF THE WHITE HOUSE AND ENVIRONS, AND REPLACEMENT EQUIPMENT AND TRAVEL ASSOCIATED WITH THE OKLAHOMA INCIDENT.

* CUSTOMS SERVICE: \$1.2 MILLION TO PROVIDE WORKING FACILITIES AND REPLACEMENT EQUIPMENT FOR DISPLACED OKLAHOMA EMPLOYEES, INCLUDING RELATED TRAVEL AND OVERTIME.

* IRS/CID: \$1 MILLION TO COVER EXPENSES RELATED TO THE OKLAHOMA INCIDENT.

* FINCEN: \$.3 MILLION TO COVER EXPENSES RELATED TO THE OKLAHOMA INCIDENT.

* DEPARTMENTAL OFFICES: \$.3 MILLION AND 10 EMPLOYEES FOR THE OFFICE OF ENFORCEMENT TO ASSIST IN OVERSIGHT OF THE DEPARTMENT'S ANTITERRORISM EFFORTS INCLUDING INCREASED SANCTIONS ENFORCEMENT.

FDCH Congressional Testimony, May 1, 1995

WE URGE YOU TO ADOPT THIS LEGISLATION WITHOUT DIMINISHING IN ANY WAY OUR REQUEST.

TREASURY BUREAUS' ACTIVITIES

NEXT, I WOULD LIKE TO TELL YOU BRIEFLY WHAT EACH OF OUR TREASURY ENFORCEMENT BUREAUS IS DOING TO COMBAT TERRORISM.

* ATF HAS LONG PLAYED A CRUCIAL ROLE INVESTIGATING TERRORIST ACTS BOTH IN THE UNITED STATES AND ABROAD. ATF HAS CLEAR RESPONSIBILITY IN THESE INVESTIGATIONS BECAUSE ILLEGAL FIREARMS AND EXPLOSIVES, WHICH ATF HAS STATUTORY JURISDICTION TO REGULATE, ARE THE TOOLS USED TO COMMIT ACTS OF VIOLENCE AGAINST THE UNITED STATES AND ITS CITIZENS. DURING THE 1989-1993 PERIOD, THERE WERE APPROXIMATELY 12,200 ACTUAL OR ATTEMPTED BOMBINGS IN THE UNITED STATES. THE FBI ESTIMATES THAT 24 WERE TERRORIST RELATED. THERE IS A MEMORANDUM OF UNDERSTANDING BETWEEN THE FBI, ATF, AND THE POSTAL INSPECTION SERVICE TO DETERMINE WHO HAS JURISDICTION OVER A BOMBING INCIDENT. NINETY FIVE PERCENT OF THE TOTAL BOMB INCIDENTS HAVE BEEN DETERMINED TO FALL WITHIN ATF'S JURISDICTION. ATF INVESTIGATES MORE BOMBING INCIDENTS THAN ANY OTHER U.S. LAW ENFORCEMENT AGENCY.

ATF HAS THE FOREMOST FEDERAL EXPERTISE IN EXPLOSIVES AND ARSON. THEY WORK CLOSELY WITH THE FBI AND THE POSTAL INSPECTION SERVICE. FEDERAL, STATE, LOCAL AND FOREIGN GOVERNMENTS ALIKE RECOGNIZE ATF AS BOMB INVESTIGATION EXPERTS, AND FREQUENTLY RELY ON ATF'S TECHNICAL AND INVESTIGATIVE EXPERTISE. FOR EXAMPLE, ATF'S INTERNATIONAL RESPONSE TEAMS ASSISTED IN THE INVESTIGATION OF THE 1992 BOMBING OF THE ISRAELI EMBASSY IN BUENOS AIRES, ARGENTINA.

AS WE SIT HERE TODAY, OVER 130 ATF PERSONNEL ARE IN OKLAHOMA CITY WORKING HAND-IN-HAND WITH THE FBI AND OTHER AGENCIES TO SOLVE THE EVIL BOMBING COMMITTED THERE. ATF IS PROVIDING THE TECHNICAL BOMBING EXPERTISE AT THE OKLAHOMA CITY BOMBING SITE. ATF'S FORENSIC'S CAPABILITIES ENABLED THEIR CHEMISTS TO IDENTIFY THE ELEMENTS OF THE BOMB AND THE PROPORTIONATE PRESENCE OF THOSE ELEMENTS. ATF ALSO BELIEVES IT HAS DETERMINED HOW THE EXPLOSION WAS INITIATED, HOW MANY CONTAINERS OF EXPLOSIVE MATERIAL WERE USED, AND WHERE THE CONTAINERS WERE POSITIONED IN THE TRUCK. FURTHER, ATF HAS IDENTIFIED THE LIKELY MANUFACTURER OF THE BARRELS BELIEVED TO HAVE HELD THE EXPLOSIVE MATERIALS.

* THE SECRET SERVICE IS CHARGED WITH PROTECTING, THE PRESIDENT, AND OTHER PROTECTEES WHO ARE PERHAPS THE HIGHEST PROFILE TARGETS OF POTENTIAL TERRORISTS ATTACKS IN THE WORLD. AS SUCH, THE SECRET SERVICE IS ACTIVELY INVOLVED IN IDENTIFYING INDIVIDUALS AND GROUPS, AS EARLY AS POSSIBLE, WHO MAY POSE A RISK TO ITS PROTECTEES. IN LIGHT OF RECENT EVENTS, WE MUST MAKE SURE THAT THE SERVICE HAS AT ITS DISPOSAL THE INVESTIGATIVE AND PROTECTIVE RESOURCES NECESSARY TO BE ABLE TO PROVIDE FOR THE SAFETY OF PROTECTEES, AS WELL AS ITS EMPLOYEES.

RELATIVE TO THE PRESIDENT'S COUNTERTERRORISM INITIATIVE, THE SECRET SERVICE SIGNIFICANTLY CONTRIBUTES BY UTILIZING ITS INVESTIGATIVE AND FORENSIC CAPABILITIES. THROUGHOUT THE WORLD, THE SECRET SERVICE IS WELL RESPECTED FOR ITS UNIQUE FORENSIC EXPERTISE AND CRIMINAL INVESTIGATIVE SKILLS. IN FACT, THOSE SKILLS ROUTINELY AND SUCCESSFULLY ARE EMPLOYED IN SUPPORT OF ITS TWO PRIMARY MISSIONS-- PROTECTION OF OUR NATION'S LEADERS AND ITS FINANCIAL SYSTEMS, TO INCLUDE IDENTIFYING POTENTIAL TERRORIST THREATS AS THEY RELATE TO THOSE RESPONSIBILITIES.

FDCH Congressional Testimony, May 1, 1995

* THE CUSTOMS SERVICE, BY VIRTUE OF ITS ENFORCEMENT AND SEARCH AUTHORITY, IS THE PRIMARY BORDER LAW ENFORCEMENT AGENCY. CUSTOMS MUST SUSTAIN AND EFFECTIVELY COORDINATE THEIR SYSTEMATIC INTERNATIONAL, INTELLIGENCE, INTERDICTION, AND INVESTIGATIVE PROGRAMS. THESE PROGRAMS ARE CRITICAL REQUIREMENTS TO DETER EFFECTIVELY THE USE OF AIR, SEA, AND LAND BORDERS AS GLOBAL SMUGGLING ROUTES TO SUPPORT TERRORIST ACTIONS.

CUSTOMS HAS ACHIEVED NOTABLE SEIZURES THROUGH THE IMPLEMENTATION OF PRO-ACTIVE INVESTIGATIONS, UNDERCOVER OPERATIONS, AND INNOVATIVE INSPECTION TECHNIQUES. SEIZURES INCLUDE SOPHISTICATED TECHNOLOGY AND CHEMICAL PRECURSORS SUCH AS AMMONIUM PERCHLORATE, SODIUM SULFIDE, ZIRCONIUM, LASER GUIDANCE DEVICES, ENCRYPTION COMMUNICATIONS EQUIPMENT, NUCLEAR TRIGGERS, AND NONRADIOACTIVE ISOTOPES. THESE SEIZURES ARE WORTH MILLIONS OF DOLLARS. DELIVERY OF ANY ONE OF THESE ITEMS INTO TERRORIST HANDS WOULD HAVE DEVASTATING EFFECTS TO PERSONS AND PROPERTY.

* THE OFFICE OF FOREIGN ASSETS CONTROL (OFAC) ADMINISTERS OUR COUNTRY'S ECONOMIC SANCTIONS PROGRAMS AGAINST SELECTED FOREIGN COUNTRIES AND GROUPS THAT SUPPORT TERRORISM OR COMMIT TERRORIST ACTS. THESE PROGRAMS INCLUDE \$2.8 BILLION IN ASSET FREEZES AND TRADE EMBARGOES AGAINST SEVERAL STATE SPONSORS OF TERRORISM, INCLUDING LIBYA AND IRAQ; AND IMPORT AND PETROLEUM DEVELOPMENT SANCTIONS AGAINST IRAN. OFAC SANCTIONS ALSO TARGET DOMESTIC FUNDRAISING ACTIVITY BY MIDDLE EAST TERRORIST GROUPS.

* THE INTERNAL REVENUE SERVICE, ALTHOUGH NOT USUALLY DIRECTLY INVOLVED IN COUNTER-TERRORISM INVESTIGATIONS, CONDUCTS INVESTIGATIONS OF TAX PROTESTERS, MANY OF WHOM ARE LINKED TO ORGANIZATIONS, SUCH AS MILITIAS, THAT CHALLENGE THE LEGITIMATE AUTHORITY OF THE U.S. GOVERNMENT.

* THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) PROVIDES VALUABLE INTELLIGENCE SUPPORT TO LAW ENFORCEMENT AGENCIES CONDUCTING INVESTIGATIONS OF TERRORISTS. IN THE PAST, FINCEN HAS PROVIDED ANALYTICAL INTELLIGENCE IN SUPPORT OF INVESTIGATIONS OF MURDER AND BOMBINGS CARRIED OUT BY SUSPECTED TERRORISTS. SUCCESSFUL TERRORIST ORGANIZATIONS REQUIRE FINANCING AND FINCEN FOLLOWS THE MONEY.

THROUGH RESEARCH AND ANALYSIS OF VARIOUS LAW ENFORCEMENT AND COMMERCIAL DATABASES, FINCEN RAPIDLY DEVELOPS INFORMATION CONCERNING RESIDENCES UTILIZED BY SUSPECTS, DOMESTIC AND INTERNATIONAL FINANCIAL TRANSACTIONS, FOREIGN TRAVEL, BUSINESS ACTIVITIES, NAMES OF ASSOCIATES, AND ALIASES USED BY SUSPECTS. THIS INFORMATION PROVIDES TIMELY INVESTIGATIVE LEADS THAT CAN BE USED TO IDENTIFY TERRORISTS AND THEIR ASSETS.

FINALLY, ALL OF TREASURY ENFORCEMENT BUREAUS ARE FOCUSED ON ATTACKING THE MEANS BY WHICH ORGANIZED CRIMINAL GROUPS FUND THEIR OPERATIONS. WE HAVE FOUND THAT CRIMES LIKE FINANCIAL FRAUD OR COUNTERFEITING FREQUENTLY ARE USED TO FINANCE ACTS OF TERRORISM. WE ARE DEDICATED TO USING OUR FINANCIAL CRIMES EXPERTISE TO ATTACK THESE FUNDING MECHANISMS.

RECENT PRESIDENTIAL INITIATIVES

ON JANUARY 23rd OF THIS YEAR, PRESIDENT CLINTON SIGNED AN EXECUTIVE ORDER PROHIBITING TRANSACTIONS WITH TERRORISTS WHO THREATEN TO DISRUPT THE MIDDLE EAST PEACE PROCESS. THIS ORDER IS BEING ENFORCED BY OFAC. THE ORDER BLOCKS THE MOVEMENT, SALE, PURCHASE, OR TRANSFER OF PROPERTY OF CERTAIN TERRORIST

FDCH Congressional Testimony, May 1, 1995

ORGANIZATIONS, OR PERSONS ACTING ON THEIR BEHALF, THAT THREATEN THE MIDDLE EAST PEACE PROCESS. THE ORDER ALSO PROHIBITS THE TRANSFERRING OF ANY CONTRIBUTION OF FUNDS, GOODS, OR SERVICES TO OR FOR THE BENEFIT OF SUCH PERSONS. THE ORDER PROVIDES A NEW TOOL TO COMBAT FUNDRAISING IN THIS COUNTRY ON BEHALF OF ORGANIZATIONS THAT USE TERROR TO UNDERMINE THE MIDDLE EAST PEACE PROCESS AND CUTS OFF THEIR ACCESS TO SOURCES OF SUPPORT IN THE U.S. AND TO THE U.S. FINANCIAL SYSTEM. SECTION 301 OF THE OMNIBUS COUNTERTERRORISM ACT OF 1995, WHICH RECENTLY WAS TRANSMITTED TO THE CONGRESS BY PRESIDENT CLINTON, CONTAINS SIMILAR BLOCKING PROVISIONS AND PROHIBITIONS AGAINST THE MAKING OR RECEIVING OF CERTAIN CONTRIBUTIONS TO DESIGNATED TERRORISTS. YESTERDAY, THE PRESIDENT ANNOUNCED HIS INTENTION TO IMPOSE ADDITIONAL SANCTIONS AGAINST IRAN. HE IS EXPECTED TO SIGN AN EXECUTIVE ORDER IMPLEMENTING HIS DECISION EARLY THIS WEEK.

AMONG THE IMPORTANT STEPS TAKEN BY PRESIDENT CLINTON IMMEDIATELY FOLLOWING THE NEWS OF THIS TRAGEDY WAS TO DIRECT HIS CABINET TO REVIEW EXISTING LEGISLATION, RESOURCES AND OPERATIONS TO DETERMINE WHAT ELSE NEEDED TO BE DONE IMMEDIATELY. WE COMMENCED AN INTENSE, COOPERATIVE REVIEW AND WITHIN A WEEK HAD DEVELOPED A NEW LEGISLATIVE AND RESOURCE PACKAGE WHICH IS SCHEDULED FOR SUBMISSION TO THE CONGRESS TODAY. I WOULD LIKE TO PROVIDE AN OVERVIEW OF THE PRESIDENT'S PACKAGE, INCLUDING THE NEW LEGISLATIVE INITIATIVES AND THE FY 1995 SUPPLEMENTAL. THE FY 1996 BUDGET AMENDMENT IS STILL BEING FINALIZED, BUT IT WILL BE TRANSMITTED TO THE CONGRESS LATER THIS WEEK.

-- THERE WILL BE A NEW DOMESTIC ANTI-TERRORISM CENTER, UNDER THE LEADERSHIP OF THE FBI. BECAUSE OF TREASURY'S IMPORTANT JURISDICTION AND ENFORCEMENT ACTIVITIES, TREASURY ENFORCEMENT WILL NECESSARILY PLAY AN IMPORTANT ROLE IN THIS CENTER. THE CONCEPTUAL FRAMEWORK OF THIS CENTER IS STILL BEING DEVELOPED.

-- A NEW PRESIDENTIAL DECISION DIRECTIVE IS BEING DEVELOPED ON BOTH FOREIGN AND DOMESTIC TERRORISM. AGAIN, TREASURY ENFORCEMENT IS ACTIVE IN THE DEVELOPMENT OF THE DIRECTIVE AND WILL PLAY AN IMPORTANT ROLE IN CARRYING OUT ITS MANDATE.

NEW LEGISLATIVE INITIATIVES

-- FBI WILL HAVE ACCESS TO FINANCIAL AND CREDIT REPORTS IN ANTI-TERRORISM CASES, ON THE SAME BASIS AS BANK RECORDS ARE CURRENTLY PROVIDED, ALLOWING ENFORCEMENT AGENCIES TO TRACK THE SOURCE AND USE OF FUNDS BY SUSPECTED TERRORISTS.

-- THE SAME LEGAL STANDARD WILL BE APPLIED IN NATIONAL SECURITY CASES THAT IS CURRENTLY USED IN OTHER CRIMINAL CASES FOR OBTAINING PERMISSION TO TRACK TELEPHONE TRAFFIC WITH "PEN REGISTERS" AND "TRAP AND TRACE" DEVICES.

-- LAW ENFORCEMENT AGENCIES WILL BE ABLE TO UTILIZE THE NATIONAL SECURITY LETTER PROCESS TO OBTAIN RECORDS CRITICAL TO TERRORISM INVESTIGATIONS FROM HOTELS, MOTELS, COMMON CARRIERS, STORAGE FACILITIES, AND VEHICLE RENTAL AGENCIES.

-- LAW ENFORCEMENT WILL HAVE EXPANDED AUTHORITY TO CONDUCT ELECTRONIC SURVEILLANCE, WITHIN CONSTITUTIONAL SAFEGUARDS. THIS IS AN IMPORTANT INVESTIGATIVE TOOL FOR ATF IN CARRYING OUT ITS EXPLOSIVE ENFORCEMENT MISSION.

-- ATF WILL BE REQUIRED TO STUDY THREE ISSUES: (1) THE INCLUSION OF TAGGANTS IN STANDARD EXPLOSIVE DEVICE RAW MATERIALS TO PERMIT TRACING OF THE SOURCE OF

FDCH Congressional Testimony, May 1, 1995

THOSE MATERIALS AFTER AN EXPLOSION; (2) WHETHER COMMON CHEMICALS USED TO MANUFACTURE EXPLOSIVES CAN BE RENDERED INERT; AND (3) WHETHER CONTROLS CAN BE IMPOSED ON CERTAIN BASIC CHEMICALS USED TO MANUFACTURE OTHER EXPLOSIVES.

-- TAGGANTS WILL BE REQUIRED IN STANDARD EXPLOSIVE DEVICE RAW MATERIALS AFTER THE PUBLICATION OF IMPLEMENTING REGULATIONS BY THE SECRETARY OF THE TREASURY.

-- LAW ENFORCEMENT AGENCIES WILL BE ABLE TO CALL ON THE TECHNICAL EXPERTISE OF THE DEPARTMENT OF DEFENSE IN INVESTIGATING OFFENSES INVOLVING CHEMICAL AND BIOLOGICAL WEAPONS.

-- WE WILL INCREASE MANDATORY MINIMUM PENALTIES FROM 5 TO 10 YEARS FOR TRANSFERRING A FIREARM OR EXPLOSIVES WITH KNOWLEDGE THAT IT WILL BE USED TO COMMIT A VIOLENT CRIME.

-- PENALTIES WILL BE ENHANCED FOR TERRORIST ATTACKS AGAINST CURRENT AND FORMER FEDERAL EMPLOYEES AND THEIR FAMILIES WHEN THE CRIME IS COMMITTED BECAUSE OF THE EMPLOYEE'S OFFICIAL DUTIES.

-- THROUGH A SURCHARGE ON CIVIL FINES, FUNDING WILL BE AVAILABLE FOR THE DIGITAL TELEPHONY BILL PASSED BY CONGRESS LAST SESSION, ENSURING COURT-AUTHORIZED LAW ENFORCEMENT ACCESS TO ELECTRONIC SURVEILLANCE OF DIGITIZED COMMUNICATIONS.

THAT COMPLETES MY STATEMENT. AFTER SECRET SERVICE'S DIRECTOR ELJAY BOWRON AND ATF'S ASSOCIATE DIRECTOR CHARLIE THOMSON PRESENT THEIR STATEMENTS, WE WILL BE GLAD TO RESPOND TO ANY QUESTIONS YOU MAY HAVE.

LANGUAGE: ENGLISH

LOAD-DATE: May 2, 1995


```

****-----****
*      18 PAGES      626 LINES      *
*      2:02 P.M. STARTED      2:04 P.M. ENDED      *
****-----****
****-----****
*      EEEEE      N      N      DDDD      *
*      E      N      N      D      D      *
*      E      NN      N      D      D      *
*      EEE      N      N      N      D      D      *
*      E      N      NN      D      D      *
*      E      N      N      D      D      *
*      EEEEE      N      N      DDDD      *
****-----****
****-----****

```

SEND TO: SCHWARTZ, MARTIN
 DOJ-CRIM-ADM
 CRIMINAL DIVISION - ADM
 1400 NEW YORK AVENUE, N.W.
 BOND BUILDING
 WASHINGTON, DISTRICT OF COLUMBIA 20530



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS FACSIMILE COVER PAGE

TO: Alex White FAX NO. 514-6113
DOJ PHONE NO. _____

FROM: Maggie Owen PHONE NO. (202) 324-
FAX NO. (202) 324-6490

DATE: _____, 1995

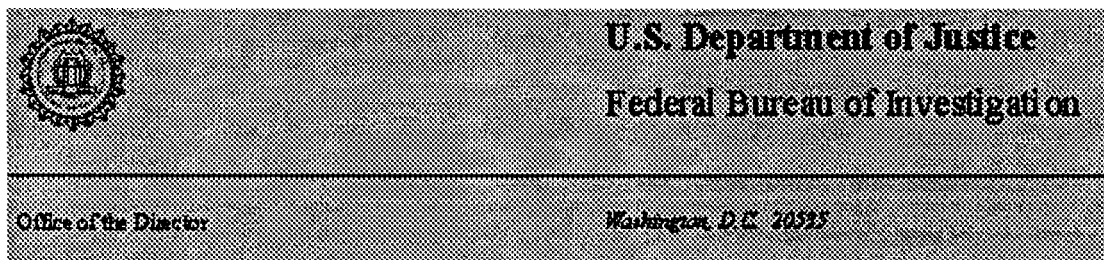
NUMBER OF PAGES: _____ (excluding transmittal page)

CONTENTS: hope this language helps



Congress is currently considering comprehensive anti-terrorism legislation which does contain sections which fine-tune issues relating to existing court-authorized electronic surveillance authorities. However, the only recent legislation enacted relating to electronic surveillance matters was the Communications Assistance for Law Enforcement Act (CALEA) (the so-called Digital Telephony Legislation), Public Law 103-414, which was signed into law by President Clinton on 10/25/94. The essence of the legislation is the preservation and maintenance of our Nation's law enforcement and counterintelligence agencies' ability to protect the American public through a critically important law enforcement tool -- court-authorized electronic surveillance. Passage of this legislation was crucial to law enforcement, since without it law enforcement would be bereft of a key tool that is so necessary to prevent the loss of human life, to effectively enforce the law, and to safeguard the national security.

As you know, federal, state and local law enforcement agencies throughout the United States rely heavily on electronic surveillance to identify, investigate, and successfully prosecute many of our societies most dangerous criminal and terrorist organizations. Frequently, this tool has been our only means of protecting human life and bringing society's most violent criminals to justice. It has been essential in fighting the tremendous onslaught of drug-trafficking and the violence of organized crime, and it has enabled law enforcement to prevent extremely violent criminal and terrorist acts. For example, through the use of electronic surveillance, the FBI was able to prevent an attempted rocket attack on a commercial airliner which, if successful, would have brutally sent hundreds of innocent passengers to death.



November 2, 1995

Honorable Henry Hyde
Chairman
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

An article published today in *The New York Times* states that the "FBI wants advanced system to vastly increase wiretapping." That simply is not so.

Court-ordered wiretapping is the single most effective investigative technique used by law enforcement to combat illegal drugs, terrorism, violent crime, espionage and organized crime. The majority of wiretapping is conducted by state and local law enforcement. Last year there were 1,154 wiretap court orders nationwide for all of law enforcement but these court-ordered wiretaps are critical to saving lives and solving the very worst crimes suffered by the public. Moreover, that number is not expected to increase in any significant manner when the law already passed by Congress is fully implemented.

Congress last year overwhelmingly passed legislation to preserve this ability in the face of advancing technology. The law neither expands authority nor ability, it merely maintains the status quo, that is, only maintains the ability of law enforcement to conduct court-ordered electronic surveillance. Without this, the public safety would be severely jeopardized.

The simple facts are:

- ☐ Congress last year did not expand the FBI's authority to conduct wiretaps nor did the FBI ask Congress to do so.
- ☐ The FBI and the telephone industry are working together -- as the law Congress passed last year requires -- to find reasonable and affordable solutions in the face of advancing technology. The initial public request for comment is part of that process.
- ☐ We have not and are not asking for the ability to monitor one out of every 100 telephone lines or any other ridiculous number like that. To obtain that many court orders and conduct that extent of wiretapping would be nearly impossible. Information supplied by the FBI was simply applied in a manner not intended to reach erroneous conclusions.
- ☐ Without this law, adequate funding and reasonable technical solutions, the Nation's public safety and national security are unquestionably jeopardized. Merely maintaining without expanding the ability of law enforcement to conduct court-ordered wiretaps is the single most important problem law enforcement faces today.

The new law requires the FBI, on behalf of all of law enforcement, to work with the telephone industry to identify technical design requirements for industry to build into their systems. The public notice mentioned in *The Times* article is part of that process and we are working with the telephone industry to define workable requirements and reasonable capacities.

Deputy Attorney General Gorelick said this morning: "Let me make it perfectly clear, there is no intention to expand the number of wiretaps or the extent of wiretapping." Those who are using the public comment notice to argue to the contrary are wrong.

Sincerely yours,

Louis J. Freeh
Director

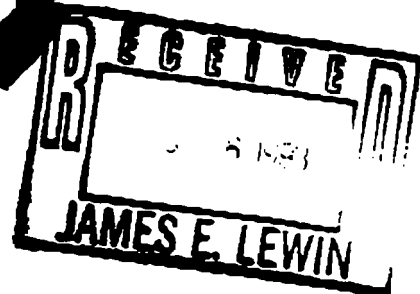


FBI Home Page

DATE: DECEMBER 2, 1993

TO: JOHN HOFFMAN
JIM LEWIN
BILL BARLOON

SUBJ: ALL-IN-ONE TRADE TALK of 11-22-93
INFO ONLY



'Operation Root Canal'

FBI'S DIGITAL TELEPHONY BILL WAS RESULT OF FAILED 2-YEAR BEHIND-SCENES CAMPAIGN

FBI's controversial Digital Wiretap Bill (CD March 3/92 p1) was result of failed 2-year campaign, code-named "Operation Root Canal," to win quiet telephone industry agreement to give law enforcement agencies easy wiretap access to digital conversations, Communications Daily has learned. Previously classified documents show how bill was introduced in light of industry's insistence that no voluntary agreement could ensure compliance by all of industry. Telephone companies ultimately opposed bill, confounding FBI, which thought it had full industry endorsement. Industry figures have denied publicly that they encouraged FBI to introduce bill. Documents also raise serious doubts about legitimacy of FBI's frequent claim that digital technologies are proved stumbling blocks to criminal investigations.

Month-long examination by Communications Daily that included interviews with telephone company and law enforcement officials and inspection of more than 180 pages of documents obtained from FBI and Justice Dept. under Freedom of Information Act (FOIA), supplied to us by Computer Professionals for Social Responsibility (CPSR), also revealed that Bureau: (1) Tried to get industry voluntarily to write digital wiretap "trapdoors" into future specifications for central office switches. (2) Attempted to convince industry to cooperate voluntarily by indicating that FBI wouldn't be able to protect network security. (3) Developed study of financial impact of digital wiretap access on industry, later claiming no such study existed.

In absence of law compelling industry to comply with FBI desire for digital wiretap access, Bureau tried to induce telephone companies to develop "immediate and interim solutions" to problem, according to internal FBI memo dated Feb. 8, 1991. Memo also said FBI agents, in conversations with industry executives, "stressed the necessity to incorporate these monitoring requirements in future specifications for central office switches." When FBI began to realize industry wouldn't go along voluntarily with its request for digital access, it painted dire picture of how Bureau would be limited in ability to fight crime if wiretap access weren't given, pointedly claiming that security of networks themselves would be at risk.

Industry reluctance to comply voluntarily with FBI plan meant agency had to turn to legislation. "It was the Bureau's court of last resort," FBI source said. Internal FBI memo dated Aug. 21, 1991, quoted unidentified PacBell official as saying: "The only viable solution for this problem would be through legislative action as technical solutions alone would be cost prohibitive and ineffective." PacBell official also is quoted saying legislation "would ensure the equal commitment of all providers."

Telephone company officials have denied publicly that they supported legislative solution. When existence of bill was made public, RHCs and equipment makers opposed it, confusing FBI. In Sept. 22, 1992, letter to Charles Bowsher, then Comptroller Gen., then-FBI Dir. William Sessions said that when Bureau efforts to gain industry's voluntary compliance failed "to achieve prompt action," industry reached consensus that "legislative mandate was both needed and desired -- a stance later repudiated by industry spokespersons." In fact, industry lobbying against bill became so intense that then-Attorney Gen. William Barr, in June 1992 letter to Sessions, told how he had sought to enlist efforts of then-Commerce Secy. Barbara Franklin because her "support is urgently needed to help diminish the telecommunications industry's intense lobbying efforts in opposition."

Whether companies flip-flopped on legislative issue is unclear. FBI refused to comment on apparent conflict between consensus Sessions thought he had from industry and industry's vehement opposition to bill when it was introduced: "You'll have to get those answers from the industry," said agent Barry Smith of FBI Legislative Affairs Office.

Although FBI documents clearly show industry agreed legislation was only way FBI could hope to gain industrywide compliance, it isn't clear that industry gave any indication it would support such a bill if introduced. Interviews with industry officials produced contradictory accounts. One senior RHC official who took part in FBI-industry meetings said flip-flop was "calculated game of political brinksmanship." He said industry never had any intention of backing legislation: "This was all an elaborate kind of shell game to discourage the FBI from making us spend millions of dollars

to make their job easier."

But another RHC official differed: "I don't recall the industry ever telling the FBI it would support legislation. Certainly our company never indicated that position." AT&T spokesman said company has "always been opposed to legislative solution." Yet, when idea of legislation was presented to representatives of AT&T, Bell Labs and Nynex at Aug. 21, 1991, meeting with FBI, as recorded in Sept. 30, 1991, internal FBI memo, none of those present was noted as opposing legislative idea. Indeed, almost year later, perceived industry flip-flop still bothered Bureau. Internal FBI memo dated Sept. 30, 1992 (after industry had come out against bill), written by Kier Boyd, FBI Deputy Asst. Dir. Operations-Technical Services Div., said "the RBOCs are playing both sides of the street, so as not to offend the Justice Dept., which enjoys considerable power over their activities" under MFJ. However, if that was intention, result was an FBI obviously irked by what it saw as duplicity.

FBI Worries Groundless?

Despite FBI insistence that digital technologies have potential to thwart investigations, Bureau has no evidence to support claim, documents revealed. Bureau has said publicly that investigations already have been hampered by current digital technologies, but has declined to respond to requests for specifics. However, FBI field report documents show Bureau received no support from field officers to back up claims of problems caused by digital technologies; field offices repeatedly reported no difficulty in carrying out electronic surveillance. Dec. 3, 1992, report from Newark office is typical, as it reported: (1) Drug Enforcement Administration "advised that as of this date, the DEA has not had any technical problems with advanced telephone technology." (2) N.J. Attorney Gen.'s office said it hasn't had any problems "since the last contact." (3) IRS reported no problems with "advanced telephone matters." (4) N.J. State Police said that "as of this date" agency has had no problems with technology's hindering investigations. Examination of all documents released turned up no reports of technology's hampering investigations. In Nov. 16 appearance on Wis. Public Radio, Special Agent James Kallstrom of FBI Technical Services Div. also contradicted previous FBI claims, admitting during debate with CPSR legal counsel David Sobel that digital technologies hadn't yet hampered FBI investigations.

Major concern of Congress, consumer advocates and industry is eventual cost of implementing FBI plan. Agency consistently has said it's in no position to evaluate such costs. When GAO investigators asked FBI for any cost analysis agency had done, FBI denied it had any. But in May 26, 1992, memo from Attorney Gen. Barr to FBI Dir. Sessions titled "Digital Telephony Information Memorandum," which outlines changes Justice Dept. made in FBI's original bill, Barr said "significant" change in measure "is that it is silent on how the cost burden for accommodating law enforcement's needs will be assumed." Same memo then said efforts to "compress the timetable" for presenting legislation included "a cost-benefits study formulated by the FBI [that] was forwarded through your staff to the OMB." FBI declined to release study.



OFFICE OF NATIONAL DRUG CONTROL POLICY
EXECUTIVE OFFICE OF THE PRESIDENT
Washington, D.C. 20500

MAY 23, 1994

MEMORANDUM TO DIRECTOR LEE P. BROWN

FROM:

[REDACTED]

THRU:

RICIA McMAHON

SUBJ:

Meeting With Congressman Don Edwards

You instructed me to schedule a meeting between yourself and Congressman Don Edwards regarding the FBI's Digital Telephony initiative. You are scheduled to meet with Congressman Edwards on May 24, 1994 at 430pm.

As you are aware, for approximately three years the FBI has been attempting to have a bill introduced that would require telecommunications carriers to maintain the ability of law enforcement to intercept telephone and other electronic communications. The FBI believes that this legislation is necessary because advances in digital telecommunications technology may make it difficult if not impossible for law enforcement to conduct wire taps in the same manner in which they have in the past.

Industry officials agree that advances in technology will change the way in which telephone and other electronic communications will be intercepted. They claim that in some cases it will be easier for wiretaps to be conducted, and in other cases technology may require that alternative methods be developed. Industry officials have testified to Congress that if the FBI legislation is enacted: (1) it will be extremely costly to implement; (2) it will negatively impact on the ability of U.S. companies to compete internationally; and (3) it may force the telephone companies to remove new technology from the telecommunications network. They also are adamant that the FBI's assertion that the ability to conduct wiretaps is in jeopardy is incorrect.

As of the date of this memorandum, the FBI still has not found a sponsor for their legislation and they are continuing their efforts to enlist support for the initiative. FBI believes that Senator Biden may introduce their bill, however it appears that the Senator prefers that Senator Leahy take the lead in any legislation.

Congressman Edwards' staff has indicated that Mr. Edwards' has recently told Director Freeh that the FBI's "one size fits all" proposal is not a realistic solution to the problem. The Congressman did say that he intends to provide a specific legislative remedy to this issue which will address the FBI's concerns. Mr. Edwards' staff has indicated that a bill is possible in the very near future.

Congressman Brooks' staff has indicated that it is doubtful that the Chairman would support any non-specific legislative initiative in this area. However, they said he would be supportive of efforts to address specific technological concerns that impede the ability of law enforcement to conduct wiretaps.

On May 17, 1994, Congressman Edwards' staff convened a meeting which the telephone companies, FBI, DEA and select Congressional staff were among those who participated. In that meeting, the FBI was asked to provide the specific technological impediments to their conducting wiretaps so that a legislative solution can be prepared. I have been told by DEA staff who attended the meeting that it was very clear that any legislative proposal supported by Mr. Edwards will have to be very specific.

In conclusion, it appears that Mr. Edwards and other members of the House and Senate are actively working toward closure on this issue. In your meeting with the Congressman you may wish to support his efforts in seeking a legislative solution so that this vital law enforcement tool can be preserved. The Congressman would probably appreciate any offer of assistance in working toward resolving this issue.

cc: Ed Jurith
Hank Marsden

DIGITAL TELPHONY

-The FBI promotes the position that advances in digital telecommunications technology have made it impossible for law enforcement to conduct wiretap operations -- and if technology continues to advance, national security and public safety will be jeopardized.

-For the past three years, the FBI has been attempting -- through the introduction of legislation -- to force the nation's telecommunications carriers (at tax payer expense) to downgrade the level of digital telecommunications technology. To date, they have been unsuccessful.

-The FBI reports that although they have been working with industry for two years to resolve the technology issue that these meetings have produced, no results nor any decision by industry to downgrade technology.

-The FBI reported in testimony on the Hill that a recent survey of Federal, State and local law enforcement has revealed 91 cases in which problems were experienced in attempting to obtain wire taps. However, it is unclear whether those problems were due to digital technology, cellular telephone technology (a different issue) or other timeliness problems.

-The FBI is not seeking to expand their wiretap authority, but only be able to have access to which they are already authorized.

-Many at DEA -- unofficially -- do not share the FBI's concern over the impact of technology -- they believe the main concern should be over forcing the telephone companies to provide a timely response to document and wiretap requests and other problems associated with cellular telephones.

INDUSTRY

-Industry vehemently opposes the FBI's proposal but have acknowledge that certain technology advancements such as call forwarding present obstacles to wiretaps (which can be overcome at some expense) and that some smaller companies do not cooperate with law enforcement. However, industry believes that the FBI is misrepresenting the problem.

-Industry officials claim that digital technology does not preclude -- and in the future will enhance their ability to provide access to conversations to law enforcement. They are very clear because of their own diagnostic, repair, and billing requirements -- the technology currently and in the future will exist for the carrier to intercept individual telephone conversations.

-Industry officials indicate the nation's telecommunication system will have analog components for quite some time so even if the FBI was correct about digital technology impeding wiretap capability -- the system would be accessible for the conceivable future.

-Industry argues that the FBI's proposed restrictions will create an unfair disadvantage to U.S. telecommunications manufacturers competing in the world marketplace with non-regulated foreign companies.

-No evidence has been presented that new technologies have resulted in any difficulty in intercepting telephone conversations.

CONGRESS

-Because of the negative reaction by both industry and privacy right groups, the FBI's proposal carries very little support on the Hill.

-However some Members of Congress such as Don Edwards have indicated that they would be willing to introduce legislation which forces telephone companies to respond in timely manner to wiretap requests.