UNITED STATES v. UNITED STATES DIST. COURT FOR THE EASTERN DIST. ..., 407 U.S. 297

Topic: All Topics : Constitutional Law : Search & Seizure : **Scope of Protection - Federal Constitutional Law Cases**
Terms: **wire tapping** (Edit Search)

*407 U.S. 297, *; 92 S. Ct. 2125, **;*
*1972 U.S. LEXIS 38, ***; 32 L. Ed. 2d 752*

UNITED STATES v. UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN ET AL. (PLAMONDON ET AL., REAL PARTIES IN INTEREST)

No. 70-153

SUPREME COURT OF THE UNITED STATES

407 U.S. 297; 92 S. Ct. 2125; 1972 U.S. LEXIS 38; 32 L. Ed. 2d 752

February 24, 1972, Argued
June 19, 1972, Decided

PRIOR HISTORY: [***1]

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT.

DISPOSITION: 444 F.2d 651, affirmed.

CORE TERMS: surveillance, domestic, Fourth Amendment, national security, electronic surveillance, interception, conversation, wiretap, intelligence, in camera, privacy, warrantless, clear and present danger, intercepted, constitutional power, sealed, Safe Streets Act, subvert, gather, probable cause, wiretapping, warrant requirement, presidential, authorize, inspection, safeguard, duty, intelligence information, deemed necessary, disclosure

SUMMARY: During pretrial proceedings in a prosecution in the United States District Court for the Eastern District of Michigan for conspiracy to destroy government property, the court ordered the government to make full disclosure to one of the defendants of his conversations overheard by electronic surveillance instituted without a search warrant. The United States Court of Appeals for the Sixth Circuit denied the government's petition for a writ of mandamus to compel the district judge to vacate the disclosure order (444 F2d 651).

On certiorari, the United States Supreme Court affirmed. In an opinion by Powell, J., expressing the views of six members of the court, it was held that the customary Fourth Amendment requirement of judicial approval before initiation of a search or surveillance applies in domestic security cases.

Douglas, J., while joining in the court's opinion, filed a separate concurring opinion in support of it.

White, J., concurred on the ground that the surveillance was statutorily prohibited.

Burger, Ch. J., concurred in the result.

Rehnquist, J., did not participate.

SYLLABUS: The United States charged three defendants with conspiring to destroy, and one of them with destroying, Government property. In response to the defendants' pretrial motion for disclosure of electronic surveillance information, the Government filed an affidavit of the Attorney General stating that he had approved the wiretaps for the purpose of "gather[ing] intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." On the basis of the affidavit and surveillance logs (filed in a sealed exhibit), the Government claimed that the surveillances, though warrantless, were lawful as a reasonable exercise of presidential power to protect the national security. The District Court, holding the surveillances violative of the Fourth Amendment, issued an order for disclosure of the overheard conversations, which the Court of Appeals upheld. Title III of the Omnibus Crime Control and Safe Streets Act, which authorizes court-approved electronic surveillance for specified crimes, [***2] contains a provision in 18 U. S. C. § 2511 (3) that nothing in that law limits the President's constitutional power to protect against the overthrow of the Government or against "any other clear and present danger to the structure or existence of the Government." The Government relies on § 2511 (3) in support of its contention that "in excepting national security surveillances from the Act's warrant requirement, Congress recognized the President's authority to conduct such surveillances without prior judicial approval." *Held*:

1. Section 2511 (3) is merely a disclaimer of congressional intent to define presidential powers in matters affecting national security, and is not a grant of authority to conduct warrantless national security surveillances. Pp. 301-308.

2. The Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for the type of domestic security surveillance involved in this case. Pp. 314-321; 323-324.

(a) The Government's duty to safeguard domestic security must be weighed against the potential danger that unreasonable surveillances pose to individual privacy and free expression. Pp. 314-315.

(b) The freedoms [***3] of the Fourth Amendment cannot properly be guaranteed if domestic security surveillances are conducted solely within the discretion of the Executive Branch without the detached judgment of a neutral magistrate. Pp. 316-318.

(c) Resort to appropriate warrant procedure would not frustrate the legitimate purposes of domestic security searches. Pp. 318-321.

COUNSEL: Assistant Attorney General Mardian argued the cause for the United States. With him on the briefs were Solicitor General Griswold and Robert L. Keuch.

William T. Gossett argued the cause for respondents the United States District Court for the Eastern District of Michigan et al. With him on the brief was Abraham D. Sofaer. Arthur Kinoy argued the cause for respondents Sinclair et al. With him on the brief were William J. Bender and William Kunstler.

Briefs of amici curiae urging affirmance were filed by Stephen I. Schlossberg for the International Union, United Automobile, Aerospace, and Agricultural Implement Workers of America (UAW), and by Benjamin Dreyfus for the Black Panther Party et al.

Briefs of amici curiae were filed by Herman Schwartz, Melvin L. Wulf, and Erwin B. Ellmann for the American Civil Liberties Union et [***4] al.; by John Ligtenberg for the American Federation of Teachers; and by the American Friends Service Committee.

JUDGES: Powell, J., delivered the opinion of the Court, in which Douglas, Brennan, Marshall, Stewart, and Blackmun, JJ., joined. Douglas, J., filed a concurring opinion, post, p. 324. Burger, C. J., concurred in the result. White, J., filed an opinion concurring in the judgment, post, p. 335. Rehnquist, J., took no part in the consideration or decision of the case.

OPINIONBY: POWELL

OPINION: [*299] [**2128] MR. JUSTICE POWELL delivered the opinion of the Court.

The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, n1 without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right [***5] to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n1 See n. 10, *infra*.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

This case arises from a criminal proceeding in the United States District Court for the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy Government property in violation of 18 U. S. C. § 371. One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan.

During pretrial proceedings, the defendants moved to compel the United States to disclose certain electronic [*300] surveillance information and to conduct a hearing to determine whether this information "tainted" the evidence on which the indictment was based or which the Government intended to offer at trial. In response, the Government filed an affidavit of the Attorney General, acknowledging that its agents had overheard conversations in which [***6] Plamondon had participated. The affidavit also stated that the Attorney General approved the wiretaps "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." n2 The logs of the surveillance [*301] were filed in a sealed exhibit for *in camera* inspection by the District Court.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n2 The Attorney General's affidavit reads as follows:

"JOHN N. MITCHELL being duly sworn deposes and says:

"1. I am the Attorney General of the United States.

"2. This affidavit is submitted in connection with the Government's opposition to the disclosure to the defendant Plamondon of information concerning the overhearing of his conversations which occurred during the course of electronic surveillances which the Government contends were legal.

"3. The defendant Plamondon has participated in conversations which were overheard by Government agents who were monitoring wiretaps which were being employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government. The records of the Department of Justice reflect the installation of these wiretaps had been expressly approved by the Attorney General.

"4. Submitted with this affidavit is a sealed exhibit containing the records of the intercepted conversations, a description of the premises that were the subjects of surveillances, and copies of the

memoranda reflecting the Attorney General's express approval of the installation of the surveillances.

"5. I certify that it would prejudice the national interest to disclose the particular facts concerning these surveillances other than to the court *in camera*. Accordingly, the sealed exhibit referred to herein is being submitted solely for the court's *in camera* inspection and a copy of the sealed exhibit is not being furnished to the defendants. I would request the court, at the conclusion of its hearing on this matter, to place the sealed exhibit in a sealed envelope and return it to the Department of Justice where it will be retained under seal so that it may be submitted to any appellate court that may review this matter."

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***7]

On the basis of the Attorney General's affidavit and the sealed exhibit, the Government asserted that the surveillance was lawful, though conducted [**2129] without prior judicial approval, as a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security. The District Court held that the surveillance violated the Fourth Amendment, and ordered the Government to make full disclosure to Plamondon of his overheard conversations. 321 F.Supp. 1074 (ED Mich. 1971).

[1A]
The Government then filed in the Court of Appeals for the Sixth Circuit a petition for a writ of mandamus to set aside the District Court order, which was stayed pending final disposition of the case. After concluding that it had jurisdiction, n3 that court held that the surveillance was unlawful and that the District Court had properly required disclosure of the overheard conversations, 444 F.2d 651 (1971). We granted certiorari, 403 U.S. 930.

[1B]

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - - n3 Jurisdiction was challenged before the Court of Appeals on the ground that the District Court's order was interlocutory and not appealable under 28 U. S. C. § 1291. On this issue, the court correctly held that it did have jurisdiction, relying upon the All Writs Act, 28 U. S. C. § 1651, and cases cited in its opinion, 444 F.2d, at 655-656. No attack was made in this Court as to the appropriateness of the writ of mandamus procedure.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***8]

I

[2]
Title III of the Omnibus Crime Control and Safe Streets Act, 18 U. S. C. §§ 2510-2520, authorizes the use of electronic surveillance for classes of crimes carefully [*302] specified in 18 U. S. C. § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger* v. *New York*, 388 U.S. 41 (1967), and *Katz* v. *United States*, 389 U.S. 347 (1967).

Together with the elaborate surveillance requirements in Title III, there is the following proviso, 18 U. S. C. § 2511 (3):

"Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U. S. C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to [***9] protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. *Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.* The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, [*303] or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power." (Emphasis supplied.)

The Government relies on § 2511 (3). It argues that "in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such [***10] surveillances without prior judicial approval." Brief for United States 7, 28. The section thus is viewed as a recognition or affirmance of a constitutional authority in the President to [**2130] conduct warrantless domestic security surveillance such as that involved in this case.

We think the language of § 2511 (3), as well as the legislative history of the statute, refutes this interpretation. The relevant language is that:

"Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . ."

against the dangers specified. At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers -- among other things -- to protection "against actual or potential attack or other hostile acts of a foreign power." But so far as the use of the President's electronic surveillance power is concerned, the language is essentially neutral.

Section 2511 (3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb [***11] such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them. This view is reinforced by the general context of Title III. Section 2511 (1) broadly prohibits the use of electronic [*304] surveillance "except as otherwise specifically provided in this chapter." Subsection (2) thereof contains four specific exceptions. In each of the specified exceptions, the statutory language is as follows:

"It shall not be unlawful . . . to intercept" the particular type of communication described. n4

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n4 These exceptions relate to certain activities of communication common carriers and the Federal Communications Commission, and to specified situations where a party to the communication has consented to the interception.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

The language of subsection (3), here involved, is to be contrasted with the language of the exceptions set forth in the preceding subsection. Rather than stating that warrantless presidential uses of electronic surveillance "shall not [***12] be unlawful" and thus employing the standard

language of exception, subsection (3) merely disclaims any intention to "limit the constitutional power of the President."

The express grant of authority to conduct surveillances is found in § 2516, which authorizes the Attorney General to make application to a federal judge when surveillance may provide evidence of certain offenses. These offenses are described with meticulous care and specificity.

Where the Act authorizes surveillance, the procedure to be followed is specified in § 2518. Subsection (1) thereof requires application to a judge of competent jurisdiction for a prior order of approval, and states in detail the information required in such application. n5 [*305] [**2131] Subsection (3) prescribes the necessary elements of probable cause which the judge must find before issuing an order authorizing an interception. Subsection (4) sets forth the required contents of such an order. [*306] Subsection (5) sets strict time limits on an order. Provision is made in subsection (7) for "an emergency situation" found to exist by the Attorney General (or by the principal prosecuting attorney of a State) "with respect to conspiratorial [***13] activities threatening the national security interest." In such a situation, emergency surveillance may be conducted "if an application for an order approving the interception is made . . . within forty-eight hours." If such an order is not obtained, or the application therefor is denied, the interception is deemed to be a violation of the Act.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n5 Title 18 U. S. C. § 2518, subsection (1), reads as follows:

"§ 2518. Procedure for interception of wire or oral communications

"(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

"(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

"(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

"(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

"(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

"(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***14]

[3]
In view of these and other interrelated provisions delineating permissible interceptions of particular criminal activity upon carefully specified conditions, it would have been incongruous for Congress to have legislated with respect to the important and complex area of national security in a single brief and nebulous paragraph. This would not comport with the sensitivity of the problem involved or with the extraordinary care Congress exercised in drafting other sections of the Act. We therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances. n6

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n6 The final sentence of § 2511 (3) states that the contents of an interception "by authority of the President in the exercise of the foregoing powers may be received in evidence . . . only where such interception was reasonable . . . ." This sentence seems intended to assure that when the President conducts lawful surveillance -- pursuant to whatever power he may possess -- the evidence is admissible.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***15]

The legislative history of § 2511 (3) supports this interpretation. Most relevant is the colloquy between Senators Hart, Holland, and McClellan on the Senate floor:

"Mr. HOLLAND. . . . The section [2511 (3)] from which the Senator [Hart] has read does not affirmatively [*307] give any power. . . . *We are not affirmatively conferring any power upon the President*. We are simply saying that nothing herein shall limit such power as the President has under the Constitution. . . . We certainly do not grant him a thing.

"There is nothing affirmative in this statement.

"Mr. McCLELLAN. Mr. President, *we make it understood that we are not trying to take anything away from him*.

"Mr. HOLLAND. The Senator is correct.

"Mr. HART. Mr. President, there is no intention here to expand by this language a constitutional power. Clearly we could not do so.

" [**2132] Mr. McCLELLAN. Even though intended, we could not do so.

"Mr. HART. . . . However, we are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now.

"In addition, Mr. President, *as I think our exchange makes clear,* [***16] *nothing in section 2511 (3) even attempts to define the limits of the President's national security power under present law, which I have always found extremely vague . . . . Section 2511 (3) merely says that if the President has such a power, then its exercise is in no way affected by title III*." n7 (Emphasis supplied.)

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n7 114 Cong. Rec. 14751. Senator McClellan was the sponsor of the bill. The above exchange

constitutes the only time that § 2511 (3) was expressly debated on the Senate or House floor. The Report of the Senate Judiciary Committee is not so explicit as the exchange on the floor, but it appears to recognize that under § 2511 (3) the national security power of the President -- whatever it may be -- "is not to be deemed disturbed." S. Rep. No. 1097, 90th Cong., 2d Sess., 94 (1968). See also The "National Security Wiretap": Presidential Prerogative or Judicial Responsibility, where the author concludes that in § 2511 (3) "Congress took what amounted to a position of neutral noninterference on the question of the constitutionality of warrantless national security wiretaps authorized by the President." 45 S. Cal. L. Rev. 888, 889 (1972).

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***17]

[*308] One could hardly expect a clearer expression of congressional neutrality. The debate above explicitly indicates that nothing in § 2511 (3) was intended to *expand* or to *contract* or to *define* whatever presidential surveillance powers existed in matters affecting the national security. If we could accept the Government's characterization of § 2511 (3) as a congressionally prescribed exception to the general requirement of a warrant, it would be necessary to consider the question of whether the surveillance in this case came within the exception and, if so, whether the statutory exception was itself constitutionally valid. But viewing § 2511 (3) as a congressional disclaimer and expression of neutrality, we hold that the statute is not the measure of the executive authority asserted in this case. Rather, we must look to the constitutional powers of the President.

II

It is important at the outset to emphasize the limited nature of the question before the Court. This case raises no constitutional challenge to electronic surveillance as specifically authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Nor is there any question [***18] or doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest. *Katz* v. *United States*, 389 U.S. 347 (1967); *Berger* v. *New York*, 388 U.S. 41 (1967). Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were [*309] "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of Government" (emphasis supplied). There is no evidence of any involvement, directly or indirectly, of a foreign power. n8

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n8 Section 2511 (3) refers to "the constitutional power of the President" in two types of situations: (i) where necessary to protect against attack, other hostile acts or intelligence activities of a "foreign power"; or (ii) where necessary to protect against the overthrow of the Government or other clear and present danger to the structure or existence of the Government. Although both of the specified situations are sometimes referred to as "national security" threats, the term "national security" is used only in the first sentence of § 2511 (3) with respect to the activities of foreign powers. This case involves only the second sentence of § 2511 (3), with the threat emanating -- according to the Attorney General's affidavit -- from "domestic organizations." Although we attempt no precise definition, we use the term "domestic organization" in this opinion to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies. No doubt there are cases where it will be difficult to distinguish between "domestic" and "foreign" unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***19]

[**2133] Our present inquiry, though important, is therefore a narrow one. It addresses a question left open by *Katz, supra*, at 358 n. 23:

"Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security . . . ."

The determination of this question requires the essential Fourth Amendment inquiry into the "reasonableness" of the search and seizure in question, and the way in which that "reasonableness" derives content and meaning [*310] through reference to the warrant clause. *Coolidge v. New Hampshire*, 403 U.S. 443, 473-484 (1971).

[4]
We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to "preserve, protect and defend the Constitution of the United States." Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President -- through the Attorney General -- may find it necessary to employ electronic surveillance to obtain intelligence information on the plans [***20] of those who plot unlawful acts against the Government. n9 The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July 1946. n10 [*311] Herbert Brownell, Attorney General under President Eisenhower, urged the use [**2134] of electronic surveillance both in internal and international security matters on the grounds that those acting against the Government

"turn to the telephone to carry on their intrigue. The success of their plans frequently rests upon piecing together shreds of information received from many sources and many nests. The participants in the conspiracy are often dispersed and stationed in various strategic positions in government and industry throughout the country." n11

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n9 Enactment of Title III reflects congressional recognition of the importance of such surveillance in combatting various types of crime. Frank S. Hogan, District Attorney for New York County for over 25 years, described telephonic interception, pursuant to court order, as "the single most valuable weapon in law enforcement's fight against organized crime." 117 Cong. Rec. 14051. The "Crime Commission" appointed by President Johnson noted that "the great majority of law enforcement officials believe that the evidence necessary to bring criminal sanctions to bear consistently on the higher echelons of organized crime will not be obtained without the aid of electronic surveillance techniques. They maintain these techniques are indispensable to develop adequate strategic intelligence concerning organized crime, to set up specific investigations, to develop witnesses, to corroborate their testimony, and to serve as substitutes for them -- each a necessary step in the evidence-gathering process in organized crime investigations and prosecutions." Report by the President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 201 (1967). [***21]

n10 In that month Attorney General Tom Clark advised President Truman of the necessity of using wiretaps "in cases vitally affecting the domestic security." In May 1940 President Roosevelt had authorized Attorney General Jackson to utilize wiretapping in matters "involving the defense of the nation," but it is questionable whether this language was meant to apply to solely domestic subversion. The nature and extent of wiretapping apparently varied under different administrations and Attorneys General, but, except for the sharp curtailment under Attorney General Ramsey Clark in the latter years of the Johnson administration, electronic surveillance has been used both against organized crime and in domestic security cases at least since the 1946 memorandum from Clark to Truman. Brief for United States 16-18; Brief for Respondents 51-56; 117 Cong. Rec. 14056.

n11 Brownell, The Public Security and **Wire Tapping,** 39 Cornell L. Q. 195, 202 (1954). See also

Rogers, The Case For **Wire Tapping,** 63 Yale L. J. 792 (1954).

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

Though the Government and respondents debate their [***22] seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them. n12 The covertness and complexity of potential unlawful conduct [*312] against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens.

- - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - -

n12 The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities. Respondents dispute these statistics as incorporating many frivolous incidents as well as bombings against nongovernmental facilities. The precise level of this activity, however, is not relevant to the disposition of this case. Brief for United States 18; Brief for Respondents 26-29; Reply Brief for United States 13.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***23]

It has been said that "the most basic function of any government is to provide for the security of the individual and of his property." *Miranda* v. *Arizona,* 384 U.S. 436, 539 (1966) (WHITE, J., dissenting). And unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered. As Chief Justice Hughes reminded us in *Cox* v. *New Hampshire,* 312 U.S. 569, 574 (1941):

"Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses."

[5]
[6]
But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development -- even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. n13 We [*313] look to the Bill of Rights to safeguard this privacy. Though physical [***24] entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. *Katz* v. *United States, supra; Berger* v. *New York, supra; Silverman* v. *United States,* 365 U.S. 505 (1961). Our decision [**2135] in *Katz* refused to lock the Fourth Amendment into instances of actual physical trespass. Rather, the Amendment governs "not only the seizure of tangible items, but extends as well to the recording of oral statements . . . without any 'technical trespass under . . . local property law.'" *Katz, supra,* at 353. That decision implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails n14 necessitate the application of Fourth Amendment safeguards.

- - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - -

n13 Professor Alan Westin has written on the likely course of future conflict between the value of privacy and the "new technology" of law enforcement. Much of the book details techniques of physical and electronic surveillance and such possible threats to personal privacy as psychological and personality testing and electronic information storage and retrieval. Not all of the contemporary threats to privacy emanate directly from the pressures of crime control. Privacy and Freedom (1967). [***25]

n14 Though the total number of intercepts authorized by state and federal judges pursuant to Tit. III of the 1968 Omnibus Crime Control and Safe Streets Act was 597 in 1970, each surveillance may involve interception of hundreds of different conversations. The average intercept in 1970 involved 44 people and 655 conversations, of which 295 or 45% were incriminating. 117 Cong. Rec. 14052.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure [*314] power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). History abundantly documents the tendency of Government -- however benevolent and benign its motives -- to view with suspicion those who most fervently dispute its policies. Fourth Amendment [***26] protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. Senator Hart addressed this dilemma in the floor debate on § 2511 (3):

"As I read it -- and this is my fear -- we are saying that the President, on his motion, could declare -- name your favorite poison -- draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government." n15

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

- - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - -

n15 114 Cong. Rec. 14750. The subsequent assurances, quoted in part I of the opinion, that § 2511 (3) implied no statutory grant, contraction, or definition of presidential power eased the Senator's misgivings.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***27]

III

As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government [*315] to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself

from acts of subversion and overthrow directed against it.

Though the Fourth Amendment speaks broadly of "unreasonable searches and seizures," the definition of "reasonableness [**2136] " turns, at least in part, on the more specific commands of the warrant clause. Some have argued that "the relevant test is not whether it is reasonable to procure a search warrant, but whether the search was reasonable," *United States* v. *Rabinowitz*, 339 U.S. 56, 66 (1950). n16 This [***28] view, however, overlooks the second clause of the Amendment. The warrant clause of the Fourth Amendment is not dead language. Rather, it has been

"a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should [*316] be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly overzealous executive officers' who are a part of any system of law enforcement." *Coolidge* v. *New Hampshire*, 403 U.S., at 481.

See also *United States* v. *Rabinowitz, supra*, at 68 (Frankfurter, J., dissenting); *Davis* v. *United States*, 328 U.S. 582, 604 (1946) (Frankfurter, J., dissenting).

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n16 This view has not been accepted. In *Chimel* v. *California*, 395 U.S. 752 (1969), the Court considered the Government's contention that the search be judged on a general "reasonableness" standard without reference to the warrant clause. The Court concluded that argument was "founded on little more than a subjective view regarding the acceptability of certain sorts of police conduct, and not on considerations relevant to Fourth Amendment interests. Under such an unconfined analysis, Fourth Amendment protection in this area would approach the evaporation point." *Id.*, at 764-765.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***29]

Over two centuries ago, Lord Mansfield held that common-law principles prohibited warrants that ordered the arrest of unnamed individuals who the *officer* might conclude were guilty of seditious libel. "It is not fit," said Mansfield, "that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge; and should give certain directions to the officer." *Leach* v. *Three of the King's Messengers*, 19 How. St. Tr. 1001, 1027 (1765).

[7]
[8]
[9]
Lord Mansfield's formulation touches the very heart of the Fourth Amendment directive: that, where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." *Coolidge* v. *New Hampshire, supra*, at 453; *Katz* v. *United States, supra*, at 356. The further requirement of "probable cause" instructs the magistrate that baseless [***30] searches shall not proceed.

[10]
These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive [*317] Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. *Katz* v. *United States, supra*, at 359-360 (DOUGLAS, J., concurring). But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally

sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating [**2137] evidence and overlook potential invasions of privacy and protected speech. n17

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n17 N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 79-105 (1937).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***31]

[11]
It may well be that, in the instant case, the Government's surveillance of Plamondon's conversations was a reasonable one which readily would have gained prior judicial approval. But this Court "has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end." *Katz, supra,* at 356-357. The Fourth Amendment contemplates a prior judicial judgment, n18 not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government. Harlan, Thoughts at a Dedication: Keeping the Judicial Function in Balance, 49 A. B. A. J. 943-944 (1963). The independent check upon executive discretion is not [*318] satisfied, as the Government argues, by "extremely limited" post-surveillance judicial review. n19 Indeed, post-surveillance review would never reach the surveillances which failed to [***32] result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights. *Beck* v. *Ohio,* 379 U.S. 89, 96 (1964).

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n18 We use the word "judicial" to connote the traditional Fourth Amendment requirement of a neutral and detached magistrate.

n19 The Government argues that domestic security wiretaps should be upheld by courts in post-surveillance review "unless it appears that the Attorney General's determination that the proposed surveillance relates to a national security matter is arbitrary and capricious, *i. e.*, that it constitutes a clear abuse of the broad discretion that the Attorney General has to obtain all information that will be helpful to the President in protecting the Government . . ." against the various unlawful acts in § 2511 (3). Brief for United States 22.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

[12]
It is true that there have been some exceptions to the warrant requirement. *Chimel* v. *California,* 395 U.S. 752 (1969); *Terry* v. *Ohio,* 392 U.S. 1 (1968); [***33] *McDonald* v. *United States,* 335 U.S. 451 (1948); *Carroll* v. *United States,* 267 U.S. 132 (1925). But those exceptions are few in number and carefully delineated, *Katz, supra,* at 357; in general, they serve the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction. Even while carving out those exceptions, the Court has reaffirmed the principle that the "police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure," *Terry* v. *Ohio, supra,* at 20; *Chimel* v. *California, supra,* at 762.

The Government argues that the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security. We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with [*319] respect to subversive [***34] forces, and are not an

attempt to gather evidence for specific criminal prosecutions. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not ongoing intelligence gathering. Brief for United States 15-16, 23-24; Reply Brief for United States 2-3.

[**2138] The Government further insists that courts "as a practical matter would have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security." These security problems, the Government contends, involve "a large number of complex and subtle factors" beyond the competence of courts to evaluate. Reply Brief for United States 4.

As a final reason for exemption from a warrant requirement, the Government believes that disclosure to a magistrate of all or even a significant portion of the information involved in domestic security surveillances "would create serious potential dangers to the national security and to the lives of informants and agents. . . . Secrecy is the essential ingredient in intelligence gathering; [***35] requiring prior judicial authorization would create a greater 'danger of leaks . . . , because in addition to the judge, you have the clerk, the stenographer and some other officer like a law assistant or bailiff who may be apprised of the nature' of the surveillance." Brief for United States 24-25.

These contentions in behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration. We certainly do not reject them lightly, especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent [*320] periods of our history. There is, no doubt, pragmatic force to the Government's position.

But we do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security [***36] surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of "ordinary crime." If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

Nor [***37] do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long [*321] involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason, §§ 2516 (1)(a) and (c), each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an *ex parte* request before a magistrate [**2139] or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance.

[13A]

Thus, we conclude that the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval [***38] prior to initiation of a search or surveillance. Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values. Nor do we think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review. By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur.

IV

We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion [*322] as to, the issues which may be involved with respect to activities of foreign powers or their agents. n20 Nor does our decision rest on the language of § 2511 (3) or any other section of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. That Act does not attempt to define or delineate the powers of the President to meet domestic [***39] threats to the national security.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n20 See n. 8, *supra*. For the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved, see *United States* v. *Smith*, 321 F.Supp. 424, 425-426 (CD Cal. 1971); and American Bar Association Project on Standards for Criminal Justice, Electronic Surveillance 120, 121 (Approved Draft 1971, and Feb. 1971 Supp. 11). See also *United States* v. *Clay*, 430 F.2d 165 (CA5 1970).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - -

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify [***40] than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

[14]
Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment [*323] if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. As the Court said in *Camara* v. *Municipal Court*, 387 U.S. 523, 534-535 (1967):

"In cases in which the Fourth Amendment requires that [***41] a warrant to search be obtained, 'probable cause' is the standard by which a particular decision to search is tested against the [**2140] constitutional mandate of reasonableness. . . . In determining whether a particular inspection is reasonable -- and thus in determining whether there is probable cause to issue a warrant for that inspection -- the need for the inspection must be weighed in terms of these

reasonable goals of code enforcement."

It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (*e. g.*, the District Court for the District of Columbia or the Court of Appeals for the District of Columbia Circuit); and that the time and reporting requirements need not be so strict as those in § 2518.

[13B]
The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt [***42] to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do [*324] hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

V

[15]
As the surveillance of Plamondon's conversations was unlawful, because conducted without prior judicial approval, the courts below correctly held that *Alderman* v. *United States*, 394 U.S. 165 (1969), is controlling and that it requires disclosure to the accused of his own impermissibly intercepted conversations. As stated in *Alderman*, "the trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect." 394 U.S., at 185. n21

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n21 We think it unnecessary at this time and on the facts of this case to consider the arguments advanced by the Government for a re-examination of the basis and scope of the Court's decision in *Alderman*.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***43]

The judgment of the Court of Appeals is hereby

Affirmed.

THE CHIEF JUSTICE concurs in the result.

MR. JUSTICE REHNQUIST took no part in the consideration or decision of this case.

CONCURBY: DOUGLAS; WHITE

CONCUR: MR. JUSTICE DOUGLAS, concurring.

While I join in the opinion of the Court, I add these words in support of it.

This is an important phase in the campaign of the police and intelligence agencies to obtain exemptions from the Warrant Clause of the Fourth Amendment. For, due to the clandestine nature of electronic eavesdropping, the need is acute for placing on the Government [*325] the heavy burden to show that "exigencies of the situation [make its] course imperative." n1 Other abuses, such as the search incident to arrest, have been partly deterred by the threat of damage actions against offending officers, n2 the risk of adverse publicity, [**2141] or the possibility of reform through the political process. These latter safeguards, however, are ineffective against lawless

wiretapping and "bugging" of which their victims are totally unaware. Moreover, even the risk of exclusion of tainted evidence would here appear to be of negligible deterrent value inasmuch as the United States [***44] frankly concedes that the primary purpose of these searches is to fortify its intelligence collage rather than to accumulate evidence to support indictments and convictions. If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n1 *Coolidge* v. *New Hampshire*, 403 U.S. 443, 455; *McDonald* v. *United States*, 335 U.S. 451, 456; *Chimel* v. *California*, 395 U.S. 752; *United States* v. *Jeffers*, 342 U.S. 48, 51.

n2 See *Bivens* v. *Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

Here, federal agents wish to rummage for months on end through every conversation, no matter how intimate or personal, carried over selected telephone lines, simply to seize those few utterances which may add to their sense of the pulse of a domestic underground.

We are told that one national security wiretap lasted for 14 months and [***45] monitored over 900 conversations. Senator Edward Kennedy found recently that "warrantless devices accounted for an average of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order." n3 He concluded that the Government's [*326] revelations posed "the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time." n4 Even the most innocent and random caller who uses or telephones into a tapped line can become a flagged number in the Government's data bank. See *Laird* v. *Tatum*, 1971 Term, No. 71-288.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n3 Letter from Senator Edward Kennedy to Members of the Subcommittee on Administrative Procedure and Practice of the Senate Judiciary Committee, Dec. 17, 1971, p. 2. Senator Kennedy included in his letter a chart comparing court-ordered and department-ordered wiretapping and bugging by federal agencies. This chart is reproduced in the Appendix to this opinion. For a statistical breakdown by duration, location, and implementing agency of the 1,042 wiretap orders issued in 1971 by state and federal judges, see Administrative Office of the United States Courts, Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications for 1971; The Washington Post, May 14, 1972, p. A30, col. 1 (final ed.). [***46]

n4 Kennedy, *supra*, n. 3, at 2. See also H. Schwartz, A Report on the Costs and Benefits of Electronic Surveillance (American Civil Liberties Union 1971); Schwartz, The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order," 67 Mich. L. Rev. 455 (1969).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

Such gross invasions of privacy epitomize the very evil to which the Warrant Clause was directed. This Court has been the unfortunate witness to the hazards of police intrusions which did not receive prior sanction by independent magistrates. For example, in *Weeks* v. *United States*, 232 U.S. 383; *Mapp* v. *Ohio*, 367 U.S. 643; and *Chimel* v. *California*, 395 U.S. 752, entire homes were ransacked pursuant to warrantless searches. Indeed, in *Kremen* v. *United States*, 353 U.S. 346, the *entire contents* of a cabin, totaling more than 800 items (such as "1 Dish Rag") n5 were seized incident to an arrest of its occupant and were taken to San Francisco for study by FBI agents. In a similar case, *Von Cleef* v. *New [*327] Jersey*, 395 U.S. 814, [***47] police, without a warrant, searched an arrestee's house for three hours, eventually seizing "several thousand articles, including books, magazines, catalogues, mailing lists, private correspondence (both open and unopened),

photographs, drawings, and film." *Id.*, at 815. In *Silverthorne Lumber Co.* v. *United States*, 251 U.S. 385, [**2142] federal agents "without a shadow of authority" raided the offices of one of the petitioners (the proprietors of which had earlier been jailed) and "made a clean sweep of all the books, papers and documents found there." Justice Holmes, for the Court, termed this tactic an "outrage." *Id.*, at 390, 391. In *Stanford* v. *Texas*, 379 U.S. 476, state police seized more than 2,000 items of literature, including the writings of Mr. Justice Black, pursuant to a general search warrant issued to inspect an alleged subversive's home.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n5 For a complete itemization of the objects seized, see the Appendix to *Kremen* v. *United States*, 353 U.S. 346, 349.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***48]

That "domestic security" is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment. In *Entick* v. *Carrington*, 19 How. St. Tr. 1029, 95 Eng. Rep. 807, decided in 1765, one finds a striking parallel to the executive warrants utilized here. The Secretary of State had issued general executive warrants to his messengers authorizing them to roam about and to seize libelous material and libellants of the sovereign. Entick, a critic of the Crown, was the victim of one such general search during which his seditious publications were impounded. He brought a successful damage action for trespass against the messengers. The verdict was sustained on appeal. Lord Camden wrote that if such sweeping tactics were validated, then "the secret cabinets and bureaus of every [*328] subject in this kingdom will be thrown open to the search [***49] and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel." *Id.*, at 1063. In a related and similar proceeding, *Huckle* v. *Money*, 2 Wils. K. B. 206, 207, 95 Eng. Rep. 768, 769 (1763), the same judge who presided over Entick's appeal held for another victim of the same despotic practice, saying "to enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition . . . ." See also *Wilkes* v. *Wood*, 19 How. St. Tr. 1153, 98 Eng. Rep. 489 (1763). As early as *Boyd* v. *United States*, 116 U.S. 616, 626, and as recently as *Stanford* v. *Texas*, *supra*, at 485-486; *Berger* v. *New York*, 388 U.S. 41, 49-50; and *Coolidge* v. *New Hampshire*, *supra*, at 455 n. 9, the tyrannical invasions described and assailed in *Entick*, *Huckle*, and *Wilkes*, practices which also were endured by the colonists, n6 have been recognized [*329] [***50] as the primary abuses which ensured the Warrant [**2143] Clause a prominent place in our Bill of Rights. See J. Landynski, Search and Seizure and the Supreme Court 28-48 (1966). N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 43-78 (1937); Note, Warrantless Searches In Light of *Chimel*: A Return To The Original Understanding, 11 Ariz. L. Rev. 457, 460-476 (1969).

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n6 "On this side of the Atlantic, the argument concerning the validity of general search warrants centered around the writs of assistance which were used by customs officers for the detection of smuggled goods." N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 51 (1937). In February 1761, all writs expired six months after the death of George II and Boston merchants petitioned the Superior Court in opposition to the granting of any new writs. The merchants were represented by James Otis, Jr., who later became a leader in the movement for independence.

"Otis completely electrified the large audience in the court room with his denunciation of England's whole policy toward the Colonies and with his argument against general warrants. John Adams, then a young man less than twenty-six years of age and not yet admitted to the bar, was a spectator, and many years later described the scene in these oft-quoted words: 'I do say in the most solemn

manner, that Mr. Otis's oration against the Writs of Assistance breathed into this nation the breath of life.' He 'was a flame of fire! Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against Writs of Assistance. Then and there was the first scene of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born. In 15 years, namely in 1776, he grew to manhood, and declared himself free.'" *Id.*, at 58-59.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***51]

As illustrated by a flood of cases before us this Term, *e. g., Laird* v. *Tatum*, No. 71-288; *Gelbard* v. *United States*, No. 71-110; *United States* v. *Egan*, No. 71-263; *United States* v. *Caldwell*, No. 70-57; *United States* v. *Gravel*, No. 71-1026; *Kleindienst* v. *Mandel*, No. 71-16; we are currently in the throes of another national seizure of paranoia, resembling the hysteria which surrounded the Alien and Sedition Acts, the Palmer Raids, and the McCarthy era. Those who register dissent or who petition their governments for redress are subjected to scrutiny by grand juries, n7 by the FBI, n8 or even by the military. n9 Their associates are interrogated. [*330] Their homes are bugged and their telephones are wiretapped. They are befriended by secret government informers. n10 Their patriotism [**2144] and loyalty are questioned. n11 [*331] Senator Sam Ervin, who has chaired hearings on military surveillance of civilian dissidents, warns that "it is not an exaggeration to talk in terms of hundreds of thousands of . . . dossiers." n12 Senator Kennedy, as mentioned *supra*, found "the frightening possibility that the conversations of [***52] untold thousands are being monitored on secret devices." More than our privacy is implicated. Also at stake is the reach of the Government's power to intimidate its critics.

- - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - -

n7 See Donner & Cerruti, The Grand Jury Network: How the Nixon Administration Has Secretly Perverted A Traditional Safeguard Of Individual Rights, 214 The Nation 5 (1972). See also *United States* v. *Caldwell*, O. T. 1971, No. 70-57; *United States* v. *Gravel*, O. T. 1971, No. 71-1026; *Gelbard* v. *United States* and *United States* v. *Egan*, O. T. 1971, Nos. 71-110 and 71-263. And see N. Y. Times, July 15, 1971, p. 6, col. 1 (grand jury investigation of N. Y. Times staff which published the Pentagon Papers).

n8 *E. g.*, N. Y. Times, April 12, 1970, p. 1, col. 2 ("U.S. To Tighten Surveillance of Radicals"); N. Y. Times, Dec. 14, 1969, p. 1, col. 1 ("F. B. I.'s Informants and Bugs Collect Data On Black Panthers"); the Washington Post, May 12, 1972, p. D21, col. 5 ("When the FBI Calls, Everybody Talks"); the Washington Post, May 16, 1972, p. B15, col. 5 ("Black Activists Are FBI Targets"); the Washington Post, May 17, 1972, p. B13, col. 5 ("Bedroom Peeking Sharpens FBI Files"). And, concerning an FBI investigation of Daniel Schorr, a television correspondent critical of the Government, see N. Y. Times, Nov. 11, 1971, p. 95, col. 4; and N. Y. Times, Nov. 12, 1971, p. 13, col. 1. For the wiretapping and bugging of Dr. Martin Luther King by the FBI, see V. Navasky, Kennedy Justice 135-155 (1971). For the wiretapping of Mrs. Eleanor Roosevelt and John L. Lewis by the FBI see Theoharis & Meyer, The "National Security" Justification For Electronic Eavesdropping: An Elusive Exception, 14 Wayne L. Rev. 749, 760-761 (1968). [***53]

n9 See *Laird* v. *Tatum*, O. T. 1971, No. 71-288; see also Federal Data Banks, Computers and the Bill of Rights, Hearings before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92d Cong., 1st Sess. (1971); N. Y. Times, Feb. 29, 1972, p. 1, col. 3.

n10 "Informers have been used for national security reasons throughout the twentieth century. They were deployed to combat what was perceived to be an internal threat from radicals during the early 1920's. When fears began to focus on Communism, groups thought to have some connection with the Communist Party were heavily infiltrated. Infiltration of the Party itself was so intense that one former FBI agent estimated a ratio of one informant for every 5.7 members in 1962. More recently, attention has shifted to militant antiwar and civil rights groups. In part because of support for such groups among university students throughout the country, informers seem to have become ubiquitous on campus. Some insight into the scope of the current use of informers was provided by the Media Papers, FBI documents stolen in early 1971 from a Bureau office in Media, Pennsylvania.

The papers disclose FBI attempts to infiltrate a conference of war resisters at Haverford College in August 1969, and a convention of the National Association of Black Students in June 1970. They also reveal FBI endeavors 'to recruit informers, ranging from bill collectors to apartment janitors, in an effort to develop constant surveillance in black communities and New Left organizations' [N. Y. Times, April 8, 1971, p. 22, col. 1]. In Philadelphia's black community, for instance, a whole range of buildings 'including offices of the Congress of Racial Equality, the Southern Christian Leadership Conference [and] the Black Coalition' [*ibid.*] was singled out for surveillance by building employees and other similar informers working for the FBI." Note, Developments In The Law -- The National Security Interest and Civil Liberties, 85 Harv. L. Rev. 1130, 1272-1273 (1972). For accounts of the impersonation of journalists by police, FBI agents and soldiers in order to gain the confidences of dissidents, see Press Freedoms Under Pressure, Report of the Twentieth Century Fund Task Force on the Government and the Press 29-34, 86-97 (1972). For the revelation of Army infiltration of political organizations and spying on Senators, Governors and Congressmen, see Federal Data Banks, Computers and the Bill of Rights, Hearings before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92d Cong., 1st Sess. (1971) (discussed in my dissent from the denial of certiorari in *Williamson* v. *United States*, 405 U.S. 1026). Among the Media Papers was the suggestion by the FBI that investigation of dissidents be stepped up in order to "'enhance the paranoia endemic in these circles and [to] further serve to get the point across there is an FBI agent behind every mailbox.'" N. Y. Times, March 25, 1971, p. 33, col. 1. [***54]

n11 *E. g.*, N. Y. Times, Feb. 8, 1972, p. 1, col. 8 (Senate peace advocates said, by presidential adviser, to be aiding and abetting the enemy).

n12 *Amicus curiae* brief submitted by Senator Sam Ervin in *Laird* v. *Tatum*, No. 71-288, O. T. 1971, p. 8.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

When the Executive attempts to excuse these tactics as essential to its defense against internal subversion, we are obliged to remind it, without apology, of this Court's long commitment to the preservation of the Bill of Rights from the corrosive environment of precisely such expedients. n13 [*332] As Justice Brandeis said, concurring in *Whitney* v. *California*, 274 U.S. 357, 377: "Those who won our independence by revolution were not cowards. They did not fear political change. They did not exalt order at the cost of liberty." Chief Justice Warren put it this way in *United States* v. *Robel*, 389 U.S. 258, 264: "This concept of 'national defense' cannot be deemed an end in itself, justifying any . . . power designed to promote such a goal. Implicit in the term 'national defense' is [***55] the notion of defending those values and ideas which set this Nation apart. . . . It would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which [make] the defense of the Nation worthwhile."

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n13 *E. g., New York Times Co.* v. *United States*, 403 U.S. 713; *Powell* v. *McCormack*, 395 U.S. 486; *United States* v. *Robel*, 389 U.S. 258, 264; *Aptheker* v. *Secretary of State*, 378 U.S. 500; *Baggett* v. *Bullitt*, 377 U.S. 360; *Youngstown Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579; *Duncan* v. *Kahanamoku*, 327 U.S. 304; *White* v. *Steer*, 327 U.S. 304; *De Jonge* v. *Oregon*, 299 U.S. 353, 365; *Ex parte Milligan*, 4 Wall. 2; *Mitchell* v. *Harmony*, 13 How. 115. Note, The "National Security Wiretap": Presidential Prerogative or Judicial Responsibility, 45 S. Cal. L. Rev. 888, 907-912 (1972).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***56]

The Warrant Clause has stood as a barrier against intrusions by officialdom into the privacies of life. But if that barrier were lowered now to permit suspected subversives' most intimate conversations to be pillaged then why could not their abodes or mail be secretly searched by the same authority? To defeat so terrifying a claim of inherent power we need only stand by the enduring [**2145] values served by the Fourth Amendment. As we stated last Term in *Coolidge* v. *New Hampshire*, 403 U.S. 443, 455: "In times of unrest, whether caused by crime or racial conflict or fear of internal

subversion, this basic law [*333] and the values that it represents may appear unrealistic or 'extravagant' to some. But the values were those of the authors of our fundamental constitutional concepts. In times not altogether unlike our own they won . . . a right of personal security against arbitrary intrusions . . . . If times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important." We have as much or more to fear from the erosion of our [***57] sense of privacy and independence by the omnipresent electronic ear of the Government as we do from the likelihood that fomenters of domestic upheaval will modify our form of governing. n14

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n14 I continue in my belief that it would be extremely difficult to write a search warrant specifically naming the particular conversations to be seized and therefore any such attempt would amount to a general warrant, the very abuse condemned by the Fourth Amendment. As I said, dissenting in *Osborn* v. *United States*, 385 U.S. 323, 353: "Such devices lay down a dragnet which indiscriminately sweeps in all conversations within its scope, without regard to the nature of the conversations, or the participants. A warrant authorizing such devices is no different from the general warrants the Fourth Amendment was intended to prohibit."

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

[*334] APPENDIX TO OPINION OF DOUGLAS, J.,

CONCURRING

FEDERAL WIRETAPPING AND BUGGING 1969-1970

Court Ordered Devices			**Executive Ordered Devices**		
				Days in Use	
Year	**Number**	**Days in Use**	**Number**	**Minimum (Rounded)**	**Maximum (Rounded)**
1969	30	462	94	8,100	20,8000
1970	180	2,363	113	8,100	22,600

Ratio of Days Used Executive Ordered:			Average Days in Use Per Device		
Court Ordered			Court Ordered Devices	Executive Ordered Devices	
Year	Minimum	Maximum		Minimum	Maximum
1969	17.5*	45.*	15.4	86.2	221.3
1970	3.4	9.6	13.1	71.7	200.0

[***58]

* Ratios for 1969 are less meaningful than those for 1970, since court-ordered surveillance program was in its initial stage in 1969.

Source:

(1) Letter from Assistant Attorney General Robert Mardian to Senator Edward M. Kennedy, March 1, 1971. Source figures withheld at request of Justice Department.

(2) Reports of Administrative Office of U.S. Courts for 1969 and 1970.

[*335] MR. [**2146] JUSTICE WHITE, concurring in the judgment.

This case arises out of a two-count indictment charging conspiracy to injure and injury to Government property. Count I charged Robert Plamondon and two codefendants with conspiring with a fourth person to injure Government property with dynamite. Count II charged Plamondon alone with dynamiting and injuring Government property in Ann Arbor, Michigan. The defendants moved to compel the United States to disclose, among other things, any logs and records of electronic surveillance directed at them, at unindicted coconspirators, or at any premises of the defendants or coconspirators. They also moved for a hearing to determine whether any electronic surveillance disclosed had tainted the evidence on which the grand jury indictment was based [***59] and which the Government intended to use at trial. They asked for dismissal of the indictment if such taint were determined to exist. Opposing the motion, the United States submitted an affidavit of the Attorney General of the United States disclosing that "the defendant Plamondon has participated in conversations which were overheard by Government agents who were monitoring wiretaps which were being employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government," the wiretaps having been expressly approved by the Attorney General. The records of the intercepted conversations and copies of the memorandum reflecting the Attorney General's approval were submitted under seal and solely for the Court's *in camera* inspection. n1

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n1 The Attorney General's affidavit concluded:

"I certify that it would prejudice the national interest to disclose the particular facts concerning these surveillances other than to the court *in camera*. Accordingly, the sealed exhibit referred to herein is being submitted solely for the court's *in camera* inspection and a copy of the sealed exhibit is not being furnished to the defendants. I would request the court, at the conclusion of its hearing on this matter, to place the sealed exhibit in a sealed envelope and return it to the Department of Justice where it will be retained under seal so that it may be submitted to any appellate court that may review this matter." App. 20-21.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - - [***60]

[*336] As characterized by the District Court, the position of the United States was that the electronic monitoring of Plamondon's conversations without judicial warrant was a lawful exercise of the power of the President to safeguard the national security. The District Court granted the motion of defendants, holding that the President had no constitutional power to employ electronic surveillance without warrant to gather information about domestic organizations. Absent probable cause and judicial authorization, the challenged wiretap infringed Plamondon's Fourth Amendment rights. The court ordered the Government to disclose to defendants the records of the monitored conversations and directed that a hearing be held to determine the existence of taint either in the indictment or in the evidence to be introduced at trial.

The Government's petition for mandamus to require the District Court to vacate its order was denied by the Court of Appeals. 444 F.2d 651 (CA6 1971). That court held that the Fourth Amendment barred warrantless electronic surveillance of domestic organizations even if at the direction of the President. It agreed with the District Court that [***61] because the wiretaps involved were therefore constitutionally infirm, the United States must turn over to defendants the records of overheard conversations for the purpose of determining whether the Government's evidence was tainted.

I would affirm the Court of Appeals but on the statutory ground urged by defendant-respondents (Brief 115) without reaching or intimating any views with respect [*337] to the constitutional issue decided by both the District Court and the Court of Appeals.

[**2147] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U. S. C. §§ 2510-2520, forbids, under pain of criminal penalties and civil actions for damages, any wiretapping or eavesdropping not undertaken in accordance with specified procedures for obtaining judicial

warrants authorizing the surveillance. Section 2511 (1) establishes a general prohibition against electronic eavesdropping "except as otherwise specifically provided" in the statute. Later sections provide detailed procedures for judicial authorization of official interceptions of oral communications; when these procedures are followed the interception is not subject to the prohibitions of § 2511 (1). Section [***62] 2511 (2), however, specifies other situations in which the general prohibitions of § 2511 (1) do not apply. In addition, § 2511 (3) provides that:

"Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U. S. C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents [*338] of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other [***63] proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power."

It is this subsection that lies at the heart of this case.

The interception here was without judicial warrant, it was not covered by the provisions of § 2511 (2) and it is too clear for argument that it is illegal under § 2511 (1) unless it is saved by § 2511 (3). The majority asserts that § 2511 (3) is a "disclaimer" but not an "exception." But however it is labeled, it is apparent from the face of the section and its legislative history that if this interception is one of those described in § 2511 (3), it is not reached by the statutory ban on unwarranted electronic eavesdropping. n2

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n2 I cannot agree with the majority's analysis of the import of § 2511 (3). Surely, Congress meant at least that if a court determined that in the specified circumstances the President could constitutionally intercept communications without a warrant, the general ban of § 2511 (1) would not apply. But the limitation on the applicability of § 2511 (1) was not open-ended; it was confined to those situations that § 2511 (3) specifically described. Thus, even assuming the constitutionality of a warrantless surveillance authorized by the President to uncover private or official graft forbidden by federal statute, the interception would be illegal under § 2511 (1) because it is not the type of presidential action saved by the Act by the provision of § 2511 (3). As stated in the text and n. 3, *infra*, the United States does not claim that Congress is powerless to require warrants for surveillances that the President otherwise would not be barred by the Fourth Amendment from undertaking without a warrant.

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - - [***64]

The defendants in the District Court moved for the production of the logs of any electronic surveillance to which they might have been subjected. The Government [*339] responded that conversations of Plamondon had been intercepted but took the position that turnover of surveillance records was not necessary because the interception complied with the law. Clearly, for the Government to prevail it was necessary to demonstrate, [**2148] first, that the interception involved was not subject to the statutory requirement of judicial approval for wiretapping because the surveillance was within the scope of § 2511 (3); and, secondly, if the Act did not forbid the warrantless wiretap, that the surveillance was consistent with the Fourth Amendment.

The United States has made no claim in this case that the statute may not constitutionally be applied to the surveillance at issue here. n3 Nor has it denied that to [*340] comply with the Act the surveillance must either be supported by a warrant or fall within the bounds of the exceptions provided by § 2511 (3). Nevertheless, as I read the opinions of the District Court and the Court of Appeals, neither court stopped to inquire whether [***65] the challenged interception was illegal under the statute but proceeded directly to the constitutional issue without adverting to the time-honored rule that courts should abjure constitutional issues except where necessary to decision of the case before them. *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288, 346-348 (1936) (concurring opinion). Because I conclude that on the record before us the surveillance undertaken by the Government in this case was illegal under the statute itself, I find it unnecessary, and therefore improper, to consider or decide the constitutional questions which the courts below improvidently reached.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n3 See Tr. of Oral Arg. 13-14:

"Q. . . . I take it from your answer that Congress could forbid the President from doing what you suggest he has the power to do in this case?

"Mr. Mardian [Assistant Attorney General]: That issue is not before this Court --

"Q. Well, I would -- my next question will suggest that it is. Would you say, though, that Congress could forbid the President?

"Mr. Mardian: I think under the rule announced by this court in *Colony Catering* that within certain limits the Congress could severely restrict the power of the President in this area.

"Q. Well, let's assume Congress says, then, that the Attorney General, or the President may authorize the Attorney General in specific situations to carry out electronic surveillance if the Attorney General certifies that there is a clear and present danger to the security of the United States?

"Mr. Mardian: I think that Congress has already provided that, and --

"Q. Well, would you say that Congress would have the power to limit surveillances to situations where those conditions were satisfied?

"Mr. Mardian: Yes, I would -- I would concur in that, Your Honor."

A colloquy appearing in the debates on the bill, appearing at 114 Cong. Rec. 14750-14751, indicates that some Senators considered § 2511 (3) as merely stating an intention not to interfere with the constitutional powers that the President might otherwise have to engage in warrantless electronic surveillance. But the Department of Justice, it was said, participated in the drafting of § 2511 (3) and there is no indication in the legislative history that there was any claim or thought that the supposed powers of the President reached beyond those described in the section. In any case, it seems clear that the congressional policy of noninterference was limited to the terms of § 2511 (3).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***66]

The threshold statutory question is simply put: Was the electronic surveillance undertaken by the Government in this case a measure deemed necessary by the President to implement either the first or second branch of the exception carved out by § 2511 (3) to the general requirement of a warrant?

The answer, it seems to me, must turn on the affidavit of the Attorney General offered by the United States in opposition to defendants' motion to disclose surveillance records. It is apparent that there

is nothing whatsoever in this affidavit suggesting that the surveillance was [*341] undertaken within the first branch of the § 2511 (3) exception, that is, to protect against foreign attack, to gather foreign intelligence or to protect national security information. The sole assertion was that the monitoring at issue was employed to gather intelligence information "deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the [**2149] existing structure of the Government." App. 20.

Neither can I conclude from this characterization that the wiretap employed here fell within the exception recognized by the second sentence of § 2511 (3); for [***67] it utterly fails to assume responsibility for the judgment that Congress demanded: that the surveillance was necessary to prevent overthrow by force or other unlawful means or that there was any other clear and present danger to the structure or existence of the Government. The affidavit speaks only of attempts to attack or subvert; it makes no reference to force or unlawfulness; it articulates no conclusion that the attempts involved any clear and present danger to the existence or structure of the Government.

The shortcomings of the affidavit when measured against § 2511 (3) are patent. Indeed, the United States in oral argument conceded no less. The specific inquiry put to Government counsel was: "Do you think the affidavit, standing alone, satisfies the Safe Streets Act?" The Assistant Attorney General answered "No, sir. We do not rely upon the affidavit itself . . . ." Tr. of Oral Arg. 15. n4

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n4 See also Tr. of Oral Arg. 17:

"Q. . . . If all the *in camera* document contained was what this affidavit contained, it would not comply with the Safe Streets Act?

"Mr. Mardian: I would concur in that, Your Honor."

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [***68]

Government counsel, however, seek to save their case by reference to the *in camera* exhibit submitted to the [*342] District Court to supplement the Attorney General's affidavit. n5 It is said that the exhibit includes the request for wiretap approval submitted to the Attorney General, that the request asserted the need to avert a clear and present danger to the structure and existence of the Government, and that the Attorney General endorsed his approval on the request. n6 But I am unconvinced that the mere endorsement of the Attorney General on the request for approval submitted to him must be taken as the Attorney General's own opinion that the wiretap was necessary to avert a clear and present danger to the existence or structure of the Government [*343] when, in an affidavit later filed in court specifically characterizing the purposes of the interception and at least impliedly the grounds for his prior approval, the Attorney General said only that the tap was undertaken to secure intelligence thought necessary to protect against attempts to attack and subvert [**2150] the structure of Government. If the Attorney General's approval of the interception is to be given [***69] a judicially cognizable meaning different from the meaning he seems to have ascribed to it in his affidavit filed in court, there obviously must be further proceedings in the District Court.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n5 The Government appears to have shifted ground in this respect. In its initial brief to this Court, the Government quoted the Attorney General's affidavit and then said, without qualification, "These were the grounds upon which the Attorney General authorized the surveillance in the present case." Brief for United States 21. Moreover, counsel for the Government stated at oral argument "that the *in camera* submission was not intended as a justification for the authorization, but simply [as] a proof of the fact that the authorization had been granted by the Attorney General of the United States, over his own signature." Tr. of Oral Arg. 6-7.

Later at oral argument, however, the Government said: "The affidavit was never intended as the basis for justifying the surveillance in question. . . . The justification, and again I suggest that it is only a partial justification, is contained in the *in camera* exhibit which was submitted to Judge Keith. . . . We do not rely upon the affidavit itself but the *in camera* exhibit." Tr. of Oral Arg. 14-15. And in its reply brief, the Government says flatly: "Those [*in camera*] documents, and not the affidavit, are the proper basis for determining the ground upon which the Attorney General acted." Reply Brief for United States 9. [***70]

n6 Procedures in practice at the time of the request here in issue apparently resulted in the Attorney General's merely countersigning a request which asserted a need for a wiretap. We are told that under present procedures the Attorney General makes an express written finding of clear and present danger to the structure and existence of the Government before he authorizes a tap. Tr. of Oral Arg. 17-18.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

Moreover, I am reluctant to proceed in the first instance to examine the *in camera* material and either sustain or reject the surveillance as a necessary measure to avert the dangers referred to in § 2511 (3). What Congress excepted from the warrant requirement was a surveillance which *the President* would assume responsibility for deeming an essential measure to protect against clear and present danger. No judge can satisfy this congressional requirement.

Without the necessary threshold determination, the interception is, in my opinion, contrary to the terms of the statute and subject therefore to the prohibition contained in § 2515 against the use of the fruits of the warrantless electronic [***71] surveillance as evidence at any trial. n7

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n7 "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter." 18 U. S. C. § 2515.

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

There remain two additional interrelated reasons for not reaching the constitutional issue. First, even if it were determined that the Attorney General purported to [*344] authorize an electronic surveillance for purposes exempt from the general provisions of the Act, there would remain the issue whether his discretion was properly authorized. The United States concedes that the act of the Attorney General authorizing a warrantless wiretap is subject to judicial review to [***72] some extent, Brief for United States 21-23, and it seems improvident to proceed to constitutional questions until it is determined that the Act itself does not bar the interception here in question.

Second, and again on the assumption that the surveillance here involved fell within the exception provided by § 2511 (3), no constitutional issue need be reached in this case if the fruits of the wiretap were inadmissible on statutory grounds in the criminal proceedings pending against respondent Plamondon. Section 2511 (3) itself states that "the contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding *only* where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power." (Emphasis added.) There has been no determination by the District Court that it would be reasonable to use the fruits of the wiretap against Plamondon or that it would be necessary to do so to implement the purposes for which the tap was authorized.

My own conclusion, again, is that, as long as nonconstitutional, [***73] statutory grounds for

excluding the evidence or its fruits have not been disposed of, it is improvident to reach the constitutional issue.

I would thus affirm the judgment of the Court of Appeals unless the Court is prepared to reconsider the necessity for an adversary, rather than an *in camera*, hearing with respect to taint. If *in camera* proceedings are sufficient and no taint is discerned by the judge, this case is over, whatever the legality of the tap.

View: Cite | KWIC | **Full** | Custom PREVIOUS **2 of 114** NEXT Text Only | Download | Fax | Email
FOCUS™ - Narrow Results | More Like This | More Like Selected Text | *Shepardize®*

UNITED STATES v. UNITED STATES DIST. COURT FOR THE EASTERN DIST. ..., 407 U.S. 297

Topic: All Topics : Constitutional Law : Search & Seizure : **Scope of Protection - Federal Constitutional Law Cases**
Terms: **wire tapping** (Edit Search)
View: Full
Date/Time: Wednesday, July 5, 2000 - 4:41 PM EDT

Search | Search Advisor | Get a Document | Check a Citation
ECLIPSE(TM) | History | Change Client | Options | Feedback | Sign Off | Help
About LEXIS-NEXIS | Terms and Conditions

KATZ v. UNITED STATES, 369 F.2d 130

*369 F.2d 130, *; 1966 U.S. App. LEXIS 4346, **

Charles KATZ, Appellant, v. UNITED STATES of America, Appellee

No. 20648

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

369 F.2d 130; 1966 U.S. App. LEXIS 4346

November 17, 1966

SUBSEQUENT HISTORY: [**1]

Certiorari Granted, 386 U.S. 954, 87 S. Ct. 1021, 18 L. Ed. 2d 102, March 13, 1967.

DISPOSITION: Affirmed.

CORE TERMS: bet, conversation, telephone, apartment, search warrant, betting, booth, wagers, Fourth Amendment, wagering, recording, microphone, nickel, evidence obtained, transmission, assisting, overheard, dollar, seized, sheets, interstate, indictment, instrumentalities, contest, wire communication, scintillator, carrying, occupied, packages, travel

JUDGES: Chambers and Barnes, Circuit Judges, and Powell, District Judge.

OPINIONBY: POWELL

OPINION: [*130] POWELL, District Judge:

The appellant was charged in each count of an eight count indictment with [*131] a violation of Title 18 U.S.C. § 1084. n1 That statute proscribes the interstate transmission by wire communication of bets or wagers, or information assisting in the placing of bets or wagers by a person engaged in the business of betting or wagering. Each count involved a violation on a different date or at different times on the same date. Appellant waived a jury. The district judge found appellant guilty on all counts.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n1 The pertinent part of 18 U.S.C. § 1084 is as follows:

> "(a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined not more than $10,000 or imprisoned not more

than two years, or both.
"(b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State where betting on that sporting event or contest is legal into a State in which such betting is legal."

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [**2]

The appellant moved to suppress evidence in the possession of the government and for the return of the evidence and the dismissal of the indictment. Following a hearing, the motions were denied. On the motion to suppress the evidence was substantially as follows:

In February of 1965 the appellant was seen placing calls from a bank of three public telephone booths during certain hours and on an almost daily basis. He was never observed in any other telephone booth.

In the period of February 19 to February 25, 1965, at set hours, Special Agents of the Federal Bureau of Investigation placed microphones on the tops of two of the public telephone booths normally used by the appellant. The other phone was placed out of order by the telephone company. The microphones were attached to the outside of the telephone booths with tape. There was no physical penetration inside of the booths. The microphones were activated only while appellant was approaching and actually in the booth. Wires led from microphones to a wire recorder on top of one of the booths. Thus the F.B.I. obtained a record of appellant's end of a series of telephone calls.

A study of the transcripts of the recordings made [**3] of the appellant's end of the conversations revealed that the conversations had to do with the placing of bets and the obtaining of gambling information by the appellant.

On February 23, 1965, F.B.I. Agent Allen Frei rented a room next to the appellant's apartment residence. He listened to conversations through the common wall without the aid of any electronic device. He overheard the appellant's end of a series of telephone conversations and took notes on them. These notes and the tapes made from the telephone booth recordings were the basis of a search warrant which was obtained to search appellant's apartment. The search warrant called for "* * * bookmaking records, wagering paraphernalia, including but not limited to, bet slips, betting markers, run-down sheets, schedule sheets indicating the lines, adding machines, money, telephones, telephone address listings * * *". (See N. 4). The articles seized are described in the return (C.T. 20-22). They are all related to the categories described in the warrant.

During the conversations overheard by Agent Frei, the appellant made numerous comments to the effect that "I have Northwestern minus 7", and "Oregon plus 3." Also, there was [**4] a statement by the appellant such as, "Don't worry about the line. I have phoned Boston three times about it today."

At the trial evidence was introduced to show that from February 19 to February 25, 1965, inclusive, the appellant placed calls from two telephone booths [*132] located in the 8200 block of Sunset Boulevard in Los Angeles. The conversations were overheard and recorded every day except February 22. The transcripts of the recordings and the normal business records of the telephone company were used to determine that the calls went to Boston, Massachusetts, and Miami, Florida.

The testimony of Joseph Gunn of the Administrative Vice Division of the Los Angeles Police Department, who was the expert called by the government in the area of bookmaking, was that the transcripts of the conversations showed that bets were made and information assisting in the placing of bets was transmitted on the dates and at the times alleged in the indictment. Bets were recorded like "Give me Duquesne minus 7 for a nickel." n2 Information relating to the line and the acquiring of credit was also transmitted.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n2 "A Mr. Katz is playing for somebody else and getting a percentage out of it. When he says he is only getting a dollar, this would mean that on a thousand dollar bet he would be getting a hundred dollars in this instance.

Q Is he using what is called the nickel system?

A Yes, sir.

Q In referring to his bets?

A Yes.

Q What is the nickel system?

A The nickel system is terminology in which a $500 bet would be called a nickel, a $1,000 bet would be called a dime. The $100 bets are usually referred to as a dollar or two dollars.

Also when you record on the nickel system you omit to the right of the decimal point so that $2,500 would be written 25 and two small zeros rather than writing four decimal point zero zero." (RT 240).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - [**5]

In correlating the transcript of the telephone conversations and line sheets and markers found in appellant's residence during the search pursuant to the warrant, Officer Gunn concluded that appellant was placing wagers with a bookmaker for another person for a consideration.

On February 25, 1965, the appellant was arrested. He was advised by a Special Agent of the F.B.I., Emmett Doherty, that he had a right to remain silent, he had a right to consult counsel, and that any statements he made could be used against him in a court of law. The appellant was arrested on the street. He was later present in his apartment where another agent of the F.B.I. was involved in the search authorized by the search warrant. Appellant asked when he could have his records back. He stated that without them he was out of business and that he knew no other trade. During this exchange, in response to a question about interstate betting, the appellant said that he could not bet locally because the bookmakers would not pay off.

The next day, which was February 26, 1965, Agent Donovan of the F.B.I. met appellant in the lobby of his apartment building to return two personal items which had been taken at [**6] the time of the search. Donovan had been with Agent Doherty the day before when Doherty advised the appellant of his rights with respect to statements made to the Federal Agents. Appellant again asked why he could not have his records back. He stated without them he was out of business and that he had been a handicapper and a bettor most of his life. He suggested that if he got his records back he would continue to bet. n3

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n3 "THE WITNESS: I returned to Mr. Katz a nail file and a key chain. Upon his taking them he said, 'I can replace these for 35 cents. Why can't I have my records? Without my records I am out of business. I have been a handicapper and a bettor most of my life, and it has taken hours and hours and hours of compilation to prepare these records.' "Mr. Katz continued as to the time factor in the records, and then suggested that if he could have his records back he would continue betting. And he facetiously made the comment, 'Then I can lead you to the big ones.'" (RT 219, 220).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - -

From all of the [**7] evidence in the case the court found the volume of business being done by the appellant indicated that it was not a casual incidental occupation of the appellant. The court found that he was engaged in the business of betting or wagering at the time of the telephone [*133] conversations which were transmitted and recorded. (RT 316, 317).

I. *Recording of Phone Booth Conversations.*

The appellant argues that the evidence obtained at the time of the recording of the appellant's end of the conversations in the phone booth constituted an illegal search and seizure in violation of the Fourth Amendment to the United States Constitution. Appellant urges this on authority of Silverman v. United States, 365 U.S. 505, 81 S. Ct. 679, 5 L. Ed. 2d 734 (1961), which he says expresses the current attitude of the Supreme Court.

In the Silverman case the agents used a spike microphone which was driven into a party wall. It contacted a heating duct of the house occupied by the petitioners. This enabled the agents to hear conversations in the entire house, including conversations on the telephone. The case was reversed because of the invasion into a "constitutionally protected [**8] area." The court said, "the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office". (365 U.S. at 511, 81 S. Ct. at 682). It was held to be a violation of the petitioner's Fourth Amendment rights.

Appellant cites cases which we have considered. In People of the State of California v. Hurst, 325 F.2d 891 (9 Cir. 1963), there was an unlawful invasion of premises used as a residence. We do not consider Lopez v. United States, 373 U.S. 427, 83 S. Ct. 1381, 10 L. Ed. 2d 462 (1963), as authority sustaining appellant's position as that case sustained the right to record a conversation between a government agent and the suspect. United States v. Paroutian, 299 F.2d 486 (2 Cir. 1962), was reversed because a search of an apartment without a warrant produced evidence later used to search the same apartment after the defendant's right to possession had terminated. This last case would apply only if we found that the evidence obtained by the recording of the phone conversations here was in violation of appellant's Fourth Amendment rights. This we decline to do.

The public phone booth [**9] was used by appellant, who argues that when he occupied it for the purpose of engaging in a personal conversation and closed the door to the booth, he is in effect in his own residence. By invitation from the telephone company and the payment of the toll he says he is entitled to consider the booth protected from intrusion by the Fourth Amendment. In Smayda v. United States, 352 F.2d 251 (9 Cir. 1965), police officers observed events in a stall in a public toilet through a camouflaged hole in the ceiling. The court held that this was not a violation of the Fourth Amendment rights of the defendants on two grounds, 1) the appellants impliedly consented to the search when they carried on their illegal acts in a public toilet, and 2) there was no unreasonable search within the meaning of the amendment. 352 F.2d at 253, 256.

In Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564, 72 L. Ed. 944 (1928), evidence was introduced which was obtained by tapping the wires of the telephones used by petitioners. It was held that the use of the evidence did not violate the Fourth Amendment rights of defendants.

In Goldman v. United States, 316 U.S. 129, 62 S. Ct. 993, 86 L. Ed. 1322 (1942), [**10] federal agents were permitted to testify to conversations overheard by the use of a detectaphone applied to the walls of a room adjoining the office of the defendant. This is similar to the instant case. It was held not to be an invasion of defendant's office.

In the recent case of Corngold v. United States, 367 F.2d 1, 3 (9 Cir. 1966), the appellant objected to the evidence obtained by the use of a "scintillator", an instrument sensitive to radiation. Customs agents saw appellant carrying packages into his apartment. The officers observed the appellant and two other men carrying packages from the apartment to the appellant's car. They followed the appellant as he drove to the Los Angeles International Airport. The scintillator, when used outside of the appellant's apartment, and while following appellant's [*134] car, reacted so as to indicate that there was a radioactive substance in the possession of the appellant. The court there said:

495179

"Appellant contends that the walls of his apartment were 'penetrated' and his apartment was searched by means of the scintillation detector in violation of his Fourth Amendment rights, and that it was error to admit [**11] evidence obtained in this way. "The agents entered the apartment building through an unlocked public entrance. They employed the scintillator in public hallways outside appellant's apartment. Goldman v. United States, 316 U.S. 129, [62 S. Ct. 993, 86 L. Ed. 1322] (1942), is controlling authority that appellant's Fourth Amendment rights were not violated. See also On Lee v. United States, 343 U.S. 747, 752-754, [72 S. Ct. 967, 96 L. Ed. 1270] (1952)."

The Corngold case sustains the government in the use of the evidence obtained by microphones and tape recordings of the telephone conversations of the appellant in this case. There was no physical entrance into the area occupied by appellant. The Corngold case was reversed on the ground that the agents were not authorized to search the packages in the airport terminal without a search warrant. Here a search warrant was obtained and executed.

II. *The Search Warrant.*

The search warrant described the items to be seized which were instrumentalities of the offense. n4 It is our conclusion that the search warrant does adequately describe the property to be seized. It was not general nor did [**12] it describe mere evidentiary matter.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n4 "* * * there is now being concealed certain property, namely bookmaking records, wagering paraphernalia, including but not limited to, bet slips, betting markers, run down sheets, schedule sheets indicating the lines, adding machines, money, telephones, telephone address listings which are designed and intended for use as the means of committing criminal offenses in violation of Title 18, United States Code Section 1084, and violations of 441, 4412 and Section 7203 of the Internal Revenue Code. * * *" (Vol. 1, CT 17).

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

In Gilbert v. United States, 291 F.2d 586 (9 Cir. 1961), this court held that the search was unreasonable when government agents allegedly maneuvered to make the arrest of the defendant in his home. No offense was committed in the presence of the arresting officer. The crime charged was the forgery of a check which the government had in its possession. The items seized were checks and income tax returns which were evidentiary only and not [**13] instrumentalities of the crime charged.

We have reviewed the authorities cited by the appellant. The case of United States v. Clancy, 276 F.2d 617 (7 Cir. 1960), (reversed on other grounds in 365 U.S. 312, 81 S. Ct. 645, 5 L. Ed. 2d 574), more nearly resembles the fact situation here. The search warrant described the property to be seized as in this case. n5

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n5 "* * * divers records, to wit books, memoranda, tickets, pads, tablets and papers recording the receipt of money from and the money paid out in connection with the operation of wagering business on said premises, such files, desks, tables and receptacles for the storing of the books, memoranda, tickets, pads, tablets and papers aforesaid, and divers receptacles in the nature of envelopes in which there is kept money won by patrons * * * and divers other tools, instruments, apparatus, United States currency and records * * *'". (276 F.2d at 624).

- - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

In Leahy v. United States, 272 F.2d 487, 491 (9 Cir. 1959), [**14] concerning a search, this court stated as follows:

> "* * * The revenue agents in the instant case seized an adding machine, a telephone, record books, receipts, pencils, pens, money and the keys to safety deposit boxes, as well as a number of rifles, shotguns and pistols. It is clear from the items seized that the search was specifically directed to the instrumentalities used in the commission of the crime of unlawfully engaging in the business of wagering. The [*135] records of an illicit business are instrumentalities of crime. Marron v. United States, 1927, 275 U.S. 192, 48 S. Ct. 74, 72 L. Ed. 231 (officers incident to arrest may lawfully seize account books and papers used in carrying on the criminal enterprise). Such were the records obtained in this case. The search was, therefore, a reasonable one."

The search warrant was valid and the court was correct in refusing to suppress the evidence obtained on the search.

III. *The Indictment.*

Counsel argues that there was a single violation under the statute, 18 U.S.C. § 1084. This is not borne out by the record as we view it. Each call was a separate act of the [**15] defendant in using the telephone and would constitute a separate and distinct offense.

In construing a related statute to 18 U.S.C. § 1084, the court in United States v. Teemer, 214 F. Supp. 952, 958 (N.D.W.Va.1963), said:

> "* * * (The) 'course of conduct' referred to in the * * * legislative history of section 1952, refers to the nature of the business promoted or facilitated -- and not to the essence of the federal offense, which is 'travel'. The phrase seems to refer to the fact that the Act was designed to attack an entrenched operation rather than a sporadic poker game or a floating crap game. No act of travel is to be deemed unlawful unless the enterprise is a continuing one; but once the continuity of the enterprise is established, any act or travel, * * * is a daily or regular event, and thus, perhaps, a 'continuing' activity. * * *"

Mitchell v. United States, 142 F.2d 480, (10 Cir. 1944), was an appeal from a conviction of mail fraud. It was held that a continuing scheme once established may support additional charges of violation of the statute. Each act of mailing would constitute a separate and distinct [**16] offense once the scheme was established. That would be the case here, as was found in the Teemer case, supra, under 18 U.S.C. § 1952.

IV. *Constitutionality of 18 U.S.C. § 1084.*

Appellant urges that the statute is unconstitutional in that it is indefinite, vague and uncertain, and therefore violates the Fifth Amendment. In support of his argument that this statute is void for vagueness, appellant quotes language from the recent case of Giaccio v. State of Pennsylvania, 382 U.S. 399, 86 S. Ct. 518, 15 L. Ed. 2d 447 (1966). The statute involved there was an 1860 law of

Pennsylvania that permitted the taxing of costs against a defendant acquitted in a criminal case. A reading of that statute shows that it fixed no standards for its application. It was vague and uncertain.

In Turf Center, Inc. v. United States, 325 F.2d 793, 795 (9 Cir. 1963), this court held 18 U.S.C. § 1952 as not void for vagueness. That section is similar to and a companion section to 18 U.S.C. § 1084.

> "A statute meets the standard of certainty required by the Constitution [**17] if its language conveys sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices. * * * The fact that in some cases it may be difficult to determine the side of the line on which a particular fact situation falls is not sufficient reason to hold the language too ambiguous to define a criminal offense. * * *"

We do not consider the authorities cited by the appellant as sustaining his position that this statute is void or that it interferes with the right of free speech. The plain and unambiguous language used in the statute is entitled to its ordinary and reasonable interpretation. This statute meets the standard of certainty required by the Constitution.

V. *Sufficiency of the Evidence.*

A complete review of the record has been made. The evidence was detailed and not substantially disputed. [*136] The defendant presented no testimony. We are convinced that there was sufficient evidence to sustain the conviction of the defendant.

The judgment of conviction is affirmed.

KATZ v. UNITED STATES, 369 F.2d 130

Service: **LEXSEE®**
Citation: **369 F2D 130**
View: Full
Date/Time: Wednesday, July 5, 2000 - 4:33 PM EDT

18 USCS § 1084

Service: **LEXSTAT®**
Citation: **18 USC 1084**

18 USCS § 1084

*** THIS SECTION IS CURRENT THROUGH 106-213, APPROVED 5/26/00 ***

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I. CRIMES
CHAPTER 50. GAMBLING

18 USCS § 1084 (2000)

§ 1084. Transmission of wagering information; penalties

(a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.

(b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State or foreign country where betting on that sporting event or contest is legal into a State or foreign country in which such betting is legal.

(c) Nothing contained in this section shall create immunity from criminal prosecution under any laws of any State.

(d) When any common carrier, subject to the jurisdiction of the Federal Communications Commission, is notified in writing by a Federal, State, or local law enforcement agency, acting within its jurisdiction, that any facility furnished by it is being used or will be used for the purpose of transmitting or receiving gambling information in interstate or foreign commerce in violation of Federal, State or local law, it shall discontinue or refuse, the leasing, furnishing, or maintaining of such facility, after reasonable notice to the subscriber, but no damages, penalty or forfeiture, civil or criminal, shall be found against any common carrier for any act done in compliance with any notice received from a law enforcement agency. Nothing in this section shall be deemed to prejudice the right of any person affected thereby to secure an appropriate determination, as otherwise provided by law, in a Federal court or in a State or local tribunal or agency, that such facility should not be discontinued or removed, or should be restored.

(e) As used in this section, the term 'State' means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, or a commonwealth, territory or possession of the United States.

HISTORY:

(Added Sept. 13, 1961, P.L. 87-216, § 2, 75 Stat. 491; Nov. 18, 1988, P.L. 100-690, Title VII, Subtitle B, § 7024, 102 Stat. 4397; Nov. 29, 1990, P.L. 101-647, Title XII, § 1205(g), 104 Stat. 4831.)

(As amended Sept. 13, 1994, P.L. 103-322, Title XXXIII, § 330016(1)(L), 108 Stat. 2147.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Amendments:

1988. Act Nov. 18, 1988, in subsec. (b), inserted "or foreign country"; in subsec. (c), deleted ", Commonwealth of Puerto Rico, territory, possession, or the District of Columbia" preceding the period; and added subsec. (e).

1990. Act Nov. 29, 1990, in subsec. (e), inserted "commonwealth".

1994. Act Sept. 13, 1994, in subsec. (a), substituted "under this title" for "not more than $ 10,000".

NOTES:

CROSS REFERENCES

Wire or oral communications, authorization for interception, 18 USCS § 2516.

Sentencing guidelines, Statutory Index, Sentencing Guidelines for U. S. Courts, 18 USCS Appendix.

This section is referred to in 18 USCS §§ 1961, 2516.

RESEARCH GUIDE

Federal Procedure:

8 Fed Proc L Ed, Criminal Procedure § 22:232.

31 Fed Proc L Ed, Telecommunications § 72:1008.

Am Jur:

38 Am Jur 2d, Gambling §§ 77, 149, 152, 153.

38 Am Jur 2d, Gambling §§ 135, 139.

Forms:

23 Am Jur Pl & Pr Forms (Rev), Telecommunications, § 116.

Annotations:

Validity and construction of federal statute (18 USC § 1084(a)) making transmission of wagering information a criminal offense. 5 ALR Fed 166.

Validity, construction, and application of statutes or ordinances involved in prosecutions for transmission of wagers or wagering information related to bookmaking. 53 ALR4th 801.

INTERPRETIVE NOTES AND DECISIONS

I. IN GENERAL

1. Constitutionality
2. Purpose
3. Construction
4. Relationship with other laws
5. Governing law
6. Conspiracy
7. Persons liable
8. --Recipient of information

II. ELEMENTS OF CRIME

A. In General

I. IN GENERAL

1. Constitutionality

18 USCS § 1084 is not unconstitutionally vague and does not interfere with right of free speech. Katz v United States (1966, CA9 Cal) 369 F2d 130, revd on other grounds (1967) 389 US 347, 19 L Ed 2d 576, 88 S Ct 507.

18 USCS § 1084 is not unconstitutional as applied to the transmission of wagers from Texas to Nevada on the theory that such application would defeat policies of Nevada. Martin v United States (1968, CA5 Tex) 389 F2d 895, cert den (1968) 391 US 919, 20 L Ed 2d 656, 88 S Ct 1808.

18 USCS § 1084, by proscribing interstate transmission of information assisting in placing of wagers or bets, does not unconstitutionally abridge freedom of speech in violation of defendant's rights under USCS Constitution, Amendment 1. Truchinski v United States (1968, CA8 Minn) 393 F2d 627, cert den (1968) 393 US 831, 21 L Ed 2d 103, 89 S Ct 104.

Section 1084(a) was not unconstitutionally vague and void for want of certainty in that it failed to

set up any ascertainable standard of conduct, since word "business" and phrase "engaged in business" as used in § 1084(a) were of common usage and could readily be understood by simple reading of statute, and because use of telephone may clearly be classified as "facility" as that term is used in statute to describe "wire communication"; § 1084(a) was therefore clear and unambiguous in its wording when words are given their usual and accepted meaning. United States v Smith (1962, ED Ill) 209 F Supp 907.

18 USCS § 1084 is constitutional. United States v Borgese (1964, SD NY) 235 F Supp 286.

Defendant's argument that § 1084(a) was beyond scope of "commerce clause" and constituted infringement of powers reserved to states by USCS Constitution, Amendment 10, was without merit; although gambling per se may be matter primarily of state concern, it was nonetheless clear that Congress, in exercise of its pervasive control over interstate commerce, could attempt to prevent use of interstate means for furtherance of crime. United States v Kelley (1966, SD NY) 254 F Supp 9, affd in part and revd in part (1968, CA2 NY) 395 F2d 727, cert den (1968) 393 US 963, 21 L Ed 2d 376, 89 S Ct 391.

Contention that 18 USCS § 1084 is unconstitutionally vague because the language "engaged in the business of betting or wagering" is such that persons of ordinary intelligence must guess at its meaning, was without merit. United States v Brodson (1975, ED Wis) 390 F Supp 774.

2. Purpose

Assistance to states directly in enforcing their gambling laws was only part of reason for enactment of 18 USCS § 1084 as it was part of omnibus crime bill recognizing need for independent federal action to combat interstate gambling operations. Martin v United States (1968, CA5 Tex) 389 F2d 895, cert den (1968) 391 US 919, 20 L Ed 2d 656, 88 S Ct 1808.

3. Construction

18 USCS §§ 2, 1084, and 1952, relating to interstate wire communication to promote and carry on gambling enterprise are criminal statutes and must be strictly construed; terms "gambling," "bets," and "wagers" as used in 18 USCS §§ 1084, 1952, are not so plain and unambiguous that there was no need to resort to legislative history to determine whether past-posting scheme was proscribed activity. United States v Bergland (1963, CA7 Wis) 318 F2d 159, cert den (1963) 375 US 861, 11 L Ed 2d 88, 84 S Ct 129.

18 USCS § 1084(d) is civil and regulatory in nature and is not subject to rule that it must be strictly construed. Tollin v Diamond State Tel. Co. (1968, DC Del) 286 F Supp 86.

4. Relationship with other laws

Although 18 USCS § 1084 does not have effect of conferring immunity from state prosecution for gambling, it does not derogate from effect of other statutes such as Communications Act [18 USCS §§ 1304 et seq.] which do confer immunity. Marcus v United States (1962, CA3 Del) 310 F2d 143, cert den (1963) 372 US 944, 9 L Ed 2d 969, 83 S Ct 933.

Unlike 18 USCS § 1955, evidence of use of interstate facilities is element of offense under both 18 USCS §§ 1084 and 1952; neither 18 USCS § 1084 nor § 1952 require minimum number of participants in offense. United States v Campagnuolo (1977, CA5 Fla) 556 F2d 1209.

Basis of federal jurisdiction underlying 18 USCS § 1084 was use of interstate communication facilities, which is wholly distinct from connection between large-scale gambling businesses and flow of commerce which provides jurisdictional basis for § 1955; necessary showing of interdependence between individuals involved in illegal gambling business under § 1955 is not required under § 1084(a); moreover, § 1084(a) is not limited to persons who are exclusively engaged in business of betting or wagering and statute does not distinguish between persons engaged in such business on their own behalf and those engaged in business on behalf of others. United States v Scavo (1979, CA8 Minn) 593 F2d 837, 4 Fed Rules Evid Serv 62.

Telephone company is not required to obey tribal court order to furnish Idaho tribe with toll-free interstate service to any state that provides company with notice in accordance with 18 USCS § 1084(d), where operation of Pick Six component of National Indian Lottery within jurisdiction of that state would violate state law, because tribal court wrongly concluded that IGRA (25 USCS §§ 2701 et seq.) applied to Lottery--Lottery simply is not covered by IGRA to extent that its operations occur off reservation. AT&T Corp. v Coeur D'Alene Tribe (1998, DC Idaho) 45 F Supp 2d 995.

5. Governing law

18 USCS § 1084(d) creates no offense and whether particular transmission or receipt of information is crime under given circumstances is to be determined not by reference to term "gambling information" as used in 18 USCS § 1084(d), but by reference to federal, state, and local criminal laws proscribing sending or receiving of gambling information over wire communications facilities. Telephone News System, Inc. v Illinois Bell Tel. Co. (1963, ND Ill) 220 F Supp 621, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

6. Conspiracy

Wharton's Rule did not prevent prosecution of defendant for conspiracy when also charged with substantive violations of 18 USCS § 1084, as substantive offenses may be committed by person acting alone and do not necessarily require concert of action between or among two or more persons. United States v Pezzino (1976, CA9 Cal) 535 F2d 483, cert den (1976) 429 US 839, 50 L Ed 2d 106, 97 S Ct 111.

7. Persons liable

Purpose of 18 USCS § 1084 is better served by imposing its duties on those who use communications facilities in day-to-day operation of gambling business and would be best able to comply. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

18 USCS § 1084(a) reaches activities of professional gamblers who conduct their activities through use of interstate telephone facilities, regardless of which party sends and which receives the wager. United States v Sellers (1973, CA5 Ala) 483 F2d 37, 25 ALR Fed 233, reh den (1973, CA5 Ala) 485 F2d 688 and cert den (1974) 417 US 908, 41 L Ed 2d 212, 94 S Ct 2604 and (ovrld on other grounds by United States v McKeever (1990, CA5 Tex) 905 F2d 829).

Substantive offenses stated in 18 USCS § 1084(a) can be committed by person acting alone as well as by person acting in concert. United States v Pezzino (1976, CA9 Cal) 535 F2d 483, cert den (1976) 429 US 839, 50 L Ed 2d 106, 97 S Ct 111.

Both the receiver and the transmitter of wagering information by interstate wire facilities are guilty of violating 18 USCS § 1084. United States v Sklaroff (1971, SD Fla) 323 F Supp 296.

8. --Recipient of information

18 USCS § 1084 includes the recipient of information in the bookmaking business which assists in the placing of bets and wagers. United States v Sklaroff (1975, CA5 Fla) 506 F2d 837, cert den (1975) 423 US 874, 46 L Ed 2d 105, 96 S Ct 142.

Defendant's contention that evidence was not sufficient to support conviction for violating 18 USCS § 1084(a) because he was receiver and not transmitter of wagering information was without merit as statute forbids use of interstate facilities for sending or receiving wagering information. United States v Pezzino (1976, CA9 Cal) 535 F2d 483, cert den (1976) 429 US 839, 50 L Ed 2d 106, 97 S Ct 111.

II. ELEMENTS OF CRIME

A. In General

9. Generally

Two elements must be present for violation of 18 USCS § 1084(a): (1) that information transmitted on telephone assisted in placing of bets or wagers and (2) that defendant during such time was engaged in business of wagering or betting. Truchinski v United States (1968, CA8 Minn) 393 F2d 627, cert den (1968) 393 US 831, 21 L Ed 2d 103, 89 S Ct 104.

In prosecution for using a wire communication facility to transmit wagering information in interstate commerce while engaged in the gambling business in violation of 18 USCS § 1084(a), the government must establish, in addition to the other elements of the offense, that defendant was in the business of gambling or in common parlance, was a "bookie". United States v Marder (1973, CA5 Fla) 474 F2d 1192.

Risk or chance is indispensable element of "betting," "wagering," or "gambling" under every federal statute involving gambling offenses. United States v Bergland (1962, ED Wis) 209 F Supp 547, revd on other grounds (1963, CA7 Wis) 318 F2d 159, cert den (1963) 375 US 861, 11 L Ed 2d 88, 84 S Ct

129.

In order for defendant to be convicted of violating 18 USCS § 1084(a), court must be convinced beyond reasonable doubt that defendant, while being in business of betting and wagering, knowingly used wire communication facility to transmit information assisting in placing of bets and wagers. United States v Alpirn (1969, SD NY) 307 F Supp 452.

Sine qua non of conviction under 18 USCS § 1084 is proof that defendant is in "business" of betting or wagering. United States v Baborian (1981, DC RI) 528 F Supp 324, 9 Fed Rules Evid Serv 964.

10. Use of wire communication facility

Word "uses" as employed in 18 USCS § 1084(a) refers to both sending and receiving such information. Sagansky v United States (1966, CA1 Mass) 358 F2d 195, cert den (1966) 385 US 816, 17 L Ed 2d 55, 87 S Ct 36.

Use of facility in interstate commerce to further business of betting or wagering is not limited to physical use; if principal acts to cause another, not engaged in betting or wagering, to use such facility principal is so engaged. United States v Kelley (1966, SD NY) 254 F Supp 9, affd in part and revd in part (1968, CA2 NY) 395 F2d 727, cert den (1968) 393 US 963, 21 L Ed 2d 376, 89 S Ct 391.

Word "use" in 18 USCS § 1084 is not limited to physical use by defendant, but, on contrary, one may "use" facility through another. United States v Sklaroff (1971, SD Fla) 323 F Supp 296.

11. Information assisting in placing bets

Defendant was convicted for violation of 18 USCS § 1084(a) on basis of phone conversation--between Connecticut and Minnesota--initiated by defendant, in which defendant informed recipient that "there wasn't much doing that day, only two games going that day," and recipient placed "two-team parlay bet for $ 30"; considering method of operation of those generally engaged in taking of bets, frequency with which particular recipient placed bets with defendant, and placing of bet, such conversation clearly demonstrated proscribed activity under 18 USCS § 1084 and jury could properly conclude that defendant transmitted information assisting in placing of bets or wagers on sporting events. Truchinski v United States (1968, CA8 Minn) 393 F2d 627, cert den (1968) 393 US 831, 21 L Ed 2d 103, 89 S Ct 104.

Scheme whereby bookmaker's out-of-state customers would call operator at hotel and ask for fictitious person, and thereafter customer would be told his party was not in and would then give operator code name, and thereupon bookmaker would be informed of call and would place return call to customer to take bet, violated § 1084(a); telephone calls to hotel informed bookmaker that someone was ready to place bet and how that person could be reached, which was "information assisting in the placing of bets or wagers" within meaning of 18 USCS § 1084(a). United States v Kelley (1968, CA2 NY) 395 F2d 727, cert den (1968) 393 US 963, 21 L Ed 2d 376, 89 S Ct 391.

12. Knowledge

Knowledge of the statutory prohibition is an element of an offense under 18 USCS § 1084. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

Knowing use of interstate facilities is not essential element of either substantive offense or conspiracy to commit it, and even if it were, evidence of one call established sufficient involvement to uphold conviction under 18 USCS § 1084(a). United States v Swank (1971, CA9 Cal) 441 F2d 264.

A conviction of conspiracy to violate 18 USCS § 1084 requires a showing that defendant knew or could reasonably foresee that interstate communication would be used in furtherance of the plan of action, and mere fact that telephone used to transmit wagering information was located near borders of other states is not sufficient to supply the element of knowledge. United States v Barone (1972, CA2 NY) 467 F2d 247.

There was ample factual basis for bookmaker in Dominican Republic's plea of guilty to violating and conspiring to violate 18 USCS § 1084, even if he did act without knowledge that his conduct was illegal, since such knowledge is not required for general intent crimes, and even though 18 USCS § 371 is specific intent crime, since prosecution need not prove that defendant intentionally violated known legal duty in order to sustain conviction under 18 USCS § 371, where underlying substantive

offense did not impose such requirement. United States v Blair (1995, CA10 Okla) 54 F3d 639.

District court did not err in accepting defendant's plea of guilty to knowingly and willfully entering into conspiracy to establish bookmaking operation in Dominican Republic in violation of 18 USCS §§ 371, 1084, and 1955, even if he was not cognizant of illegality of his actions, since 18 USCS § 1084 is general intent crime, and prosecution need not prove that defendant intentionally violated known legal duty in order to sustain conviction under 18 USCS § 371, where underlying substantive offense does not impose such requirement. United States v Blair (1995, CA10 Okla) 54 F3d 639.

13. Transmission

The word "transmission," as used in 18 USCS § 1084(a), is limited to "sending", and does not encompass mere reception. United States v Stonehouse (1971, CA7 Ill) 452 F2d 455.

18 USCS § 1084(a) is limited to prohibited transmissions and does not encompass mere reception; receipt of information assisting in placing of bets or wagers over ticker tape machine, which was unlike telephone in that it enabled defendant only to receive rather than transmit such information did not constitute violation of 18 USCS § 1084. United States v Stonehouse (1971, CA7 Ill) 452 F2d 455.

"Transmission" in 18 USCS § 1084(a) means sending as well as receiving bets. United States v Tomeo (1972, CA10 Colo) 459 F2d 445, cert den (1972) 409 US 914, 34 L Ed 2d 175, 93 S Ct 232.

Interstate telephone calls in which defendant obtained game scores for various sports could be considered "transmissions" within meaning of 18 USCS § 1084(a), despite contention that "transmission" was not intended to encompass reception of information. United States v Reeder (1980, CA8 Ark) 614 F2d 1179, 5 Fed Rules Evid Serv 1324.

Prohibited act of transmission under 18 USCS § 1084 was not completed by mere placing of telephone call, but only when there had been interstate communication of wagering information by use of wire facilities. United States v Synodinos (1963, DC Utah) 218 F Supp 479.

"Transmission" as used in § 1084(a) does not mean sending or receiving, and Congress meant it only as "sending" in this provision; since § 1084(d) uses term "transmitting or receiving," it would be illogical to suppose that Congress would not have used both terms in both subsections had it meant to include "receiving" in § 1084(a). Telephone News System, Inc. v Illinois Bell Tel. Co. (1963, ND Ill) 220 F Supp 621, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

14. --In interstate commerce

"Cruise to nowhere," where vessel had no contact whatsoever with foreign country or its waters within jurisdiction of foreign country, and where indeed no such contact was intended, did not involve foreign commerce within meaning of 18 USCS §§ 10, 1952, and 1084. United States v Montford (1994, CA5 Miss) 27 F3d 137.

Transmission of information assisting in placing of illegal wagers from one point in West Virginia to another point in that state by means of telephone lines which crossed borders of another state came within proscription of 18 USCS § 1084. United States v Yaquinta (1962, ND W Va) 204 F Supp 276.

Although father is not guilty of violating 18 USCS § 1084 where he receives out of state telephone call from his son asking him to place certain bets, third party to whom father relays bets to via telephone is definitely guilty of violating § 1084 where third party knows that bets received through father are from out of state source which is substantiated by fact that son told father in later conversation that he talked to third party while still being out of state. United States v Baborian (1981, DC RI) 528 F Supp 324, 9 Fed Rules Evid Serv 964.

B. Engagement in Business of Wagering

15. Betting legally under state law

18 USCS § 1084 was not applicable to activity of defendant consisting of pari-mutuel betting which was lawful under state law. United States v Donaway (1971, CA9 Cal) 447 F2d 940.

16. Horse race prediction for fee

A "turf advisor" who provided his clients with predictions as to the likely winners of given horse races and who collected the equivalent of $ 5 bet if the horse won, was not violating 18 USCS § 1084 notwithstanding that the "turf advisor" used telephone lines in transacting his business. United States v Alpirn (1969, SD NY) 307 F Supp 452.

17. Newspaper publication

18 USCS § 1084(a) prohibits transmission of gambling information in interstate commerce by persons directly or indirectly engaged in business of betting or wagering, but it does not reach such transmission by persons engaged in publication for sale to general public through normal channels of newspaper distribution of periodicals which contain information similar or identical to that contained in newspapers of general circulation. Kelly v Illinois Bell Tel. Co. (1962, ND Ill) 210 F Supp 456, affd (1963, CA7 Ill) 325 F2d 148.

18. Personal bets with friends

Wagers otherwise within 18 USCS § 1084(a) are not excluded because contracted with friends. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

18 USCS § 1084(a) requires that defendant be engaged in business of betting or wagering in order to be in violation; where record merely reflected that codefendant was friend of defendant who regularly placed bets with him, in absence of evidence that codefendant was in business of betting or wagering, there was no violation of 18 USCS § 1084. United States v Anderson (1976, CA7 Wis) 542 F2d 428.

18 USCS § 1084 does not encompass discussions between friends as to their opinions on outcome of sporting events. United States v Baborian (1981, DC RI) 528 F Supp 324, 9 Fed Rules Evid Serv 964.

19. Receiving bets on behalf of another

Defendant was "engaged in the business of betting or wagering" within meaning of 18 USCS § 1084(a), even though he accepted wagers on behalf of someone else, rather than as principal; language of 18 USCS § 1084 makes no distinction between those engaged in business of gambling on their own behalf and those engaged in that business on behalf of others. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

In prosecution under 18 USCS § 1084(a), it was no defense to say that defendant "passed on" bets made with him by regular customer, and was consequently acting as agent for someone else. Truchinski v United States (1968, CA8 Minn) 393 F2d 627, cert den (1968) 393 US 831, 21 L Ed 2d 103, 89 S Ct 104.

Although father is not guilty of violating 18 USCS § 1084 where he receives out of state telephone call from his son asking him to place certain bets, third party to whom father relays bets to via telephone is definitely guilty of violating § 1084 where third party knows that bets received through father are from out of state source which is substantiated by fact that son told father in later conversation that he talked to third party while still being out of state. United States v Baborian (1981, DC RI) 528 F Supp 324, 9 Fed Rules Evid Serv 964.

20. Single telephone call or other act

Use of words "bets or wagers" in plural was not of design but of somewhat imprecise, conversational language, and Congress intended to reach single use of interstate facilities by one who was engaged in business of betting or wagering. Sagansky v United States (1966, CA1 Mass) 358 F2d 195, cert den (1966) 385 US 816, 17 L Ed 2d 55, 87 S Ct 36.

One who in fact accepts or places bet or bets "uses" telephone for transmission within 18 USCS § 1084, and offense exists where single use of interstate facilities for betting arises. Sagansky v United States (1966, CA1 Mass) 358 F2d 195, cert den (1966) 385 US 816, 17 L Ed 2d 55, 87 S Ct 36.

18 USCS § 1084 was not intended to be applicable to isolated acts of wagering by individuals not engaged in the business of wagering since its purpose is to curb the activities of the professional gambler. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

Single telephone call is sufficient involvement to uphold conviction under 18 USCS § 1084. United States v Swank (1971, CA9 Cal) 441 F2d 264.

Evidence that defendant placed single telephone bet for another following single telephone call was not sufficient to prove defendant was engaged in business enterprise prohibited by 18 USCS § 1084. United States v Donaway (1971, CA9 Cal) 447 F2d 940.

III. DEFENSES

21. Double jeopardy

Since 18 USCS § 1084(d) is nonpenal and does not impose criminal sanctions, termination of telephone service followed by prosecution for violation of 18 USCS § 1952 arising out of same conduct did not violate prohibition against double jeopardy. United States v Cerone (1971, CA7 Ill) 452 F2d 274, cert den (1972) 405 US 964, 31 L Ed 2d 240, 92 S Ct 1168 and cert den (1972) 405 US 964, 31 L Ed 2d 240, 92 S Ct 1169.

Defendants were not twice placed in jeopardy by being subject to trial for violation of 18 USCS § 1084 after having been convicted of same gambling offenses in prior state proceeding. United States v Barone (1972, CA2 NY) 467 F2d 247.

Indictment charging in two counts violation of 18 USCS § 1084(a) and in two other counts violation of 18 USCS § 1952, by use of same interstate telephone facility on same days, was not duplicitous and did not place defendant in jeopardy twice for same offense; defendant was charged with violating two separate statutes, which require different elements of proof, and where each count of indictment required proof of fact not necessary to be proved under other counts, double jeopardy argument would be without merit. United States v Smith (1962, ED Ill) 209 F Supp 907.

22. Entrapment

In prosecution under 18 USCS § 1084 if evidence elicited would warrant finding of inducement by government, defendant is entitled to charge that government has burden of proving beyond reasonable doubt that there was in fact no inducement or that defendant was predisposed and where there was inducement as matter of law, only question of predisposition should have been submitted to jury and government had burden of proving such predisposition beyond reasonable doubt. Sagansky v United States (1966, CA1 Mass) 358 F2d 195, cert den (1966) 385 US 816, 17 L Ed 2d 55, 87 S Ct 36.

23. Immunity

Fact that defendant testified before county grand jury with respect to commercial gambling did not license him to engage in such conduct in future and enable him to avoid prosecution under 18 USCS § 1084. United States v Brodson (1975, ED Wis) 390 F Supp 774.

IV. DISCONTINUANCE OF FACILITIES

24. Generally; constitutionality

Since 18 USCS § 1084(d) is regulatory rather than penal, discontinuance of telephone service is not subject to procedural safeguards under USCS Constitution, Amendments 5, 6; 18 USCS § 1084(d) provides fair notice of type of conduct which will give rise to discontinuation of telephone service and contains sufficient standards to show what type of criminal offense will cause its application. Telephone News System, Inc. v Illinois Bell Tel. Co. (1963, ND Ill) 220 F Supp 621, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

18 USCS § 1084(d) does not limit legal right of telephone company to discontinue service when company believes that service is being used in furtherance of illegal purpose, and common-law authority for such right was not pre-empted by Congress in enacting 18 USCS § 1084(d). Delaware Sports Service v Diamond State Tel. Co. (1965, DC Del) 241 F Supp 847, affd (1966, CA3 Del) 355 F2d 929, cert den (1966) 385 US 817, 17 L Ed 2d 55, 87 S Ct 38.

Telephone company may, without incurring liability for damages, terminate service after reasonable notice upon being notified pursuant to 18 USCS § 1084(d) by any law enforcement agency to effect that its facilities are or will be used to transmit or receive gambling information in interstate commerce in violation of law. Tollin v Diamond State Tel. Co. (1968, DC Del) 286 F Supp 86.

25. Violation of state law

Telephone subscriber who transmitted betting odds and changes in betting odds by telephone in violation of Illinois statute, although not himself engaged in accepting or placing wagers, fell within the provisions of 18 USCS § 1084(d) requiring termination of subscriber's telephone service if the

betting information was transmitted interstate. Angelini v Illinois Bell Tel. Co. (1969, CA7 Ill) 418 F2d 111, cert den (1970) 397 US 1040, 25 L Ed 2d 651, 90 S Ct 1361.

26. Notice

18 USCS § 1084(d) requires no specific form of notice or particular language; notice is sufficient if it seems reasonably clear that it was predicated upon written communication from law enforcement agency stating that wires were being used or will be used for purpose of transmitting or receiving gambling information in interstate or foreign commerce in violation of law. Tollin v Diamond State Tel. Co. (1968, DC Del) 286 F Supp 86.

27. Subscribers' rights and remedies

Contract arising from lottery ticket purchase made while injunction was in effect which suspended application of Interstate Wagering Amendment, 18 USCS §§ 1084, 1301, and 1953, to private corporation selling lottery tickets over state lines was not unenforceable due to illegality, since injunction was presumptively valid. Wenner v Texas Lottery Comm'n (1997, CA5 Tex) 123 F3d 321.

Telephone subscriber's privilege against self-incrimination was not denied by necessity, under 18 USCS § 1084, of filing complaint in order to protect rights to telephone service. Telephone News System, Inc. v Illinois Bell Tel. Co. (1963, ND Ill) 220 F Supp 621, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

Owners of property where telephone facilities were installed were "affected" by threatened termination of telephone service within meaning of 18 USCS § 1084(d), and had standing to sue to enjoin threatened termination, even though subscriber to telephone service was another person; where defendant telephone company gave reasonable notice to subscriber of its intention to remove telephone facilities at property owned by plaintiffs, plaintiffs in accordance with 18 USCS § 1084(d), could not recover damages if defendant should actually remove facilities. Di Giacomo v Diamond State Tel. Co. (1973, DC Del) 356 F Supp 1063.

Money transfer service is protected from customer's efforts to secure money damages for loss of "Quick Collect" service, where service was summarily terminated as result of request by state attorney general concerned that citizens were using service to transmit funds for illegal offshore gambling, because contract remedy for damages is foreclosed by terms of 18 USCS § 1084(d). Cheyenne Sales v Western Union Fin. Servs. Int'l (1998, ED Pa) 8 F Supp 2d 469.

28. Burden of proof; sufficiency of evidence

In proceeding seeking to enjoin discontinuance of plaintiff's telephone service under 18 USCS § 1084(d), government and telephone company bear burden of proof and standard of proof is preponderance of evidence. Telephone News System, Inc. v Illinois Bell Tel. Co. (1962, ND Ill) 210 F Supp 471, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134; Telephone News System, Inc. v Illinois Bell Tel. Co. (1963, ND Ill) 220 F Supp 621, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

Plaintiff, seeking to enjoin telephone company from discontinuing telephone service, was not engaged in business of betting or wagering in violation of 18 USCS § 1084(a) by transmitting over telephone lines information regarding winners and wagering results where there was no evidence that transmission was directly or indirectly related to illegal gambling activities. Telephone News System, Inc. v Illinois Bell Tel. Co. (1962, ND Ill) 210 F Supp 471, affd (1964) 376 US 782, 12 L Ed 2d 83, 84 S Ct 1134.

In action to enjoin defendants from terminating, under 18 USCS § 1084(d), telephone service at plaintiffs' property, defendants failed to sustain their burden of proving by preponderance of evidence any present or threatened future illegal interstate or foreign use of telephone where it merely submitted affidavit of FBI agent which disclosed that from 1969 until May 8, 1972, telephone was used to transmit or receive gambling information in interstate or foreign commerce but which did not state that at any time since May 8, 1972, telephone has been used for that purpose. Di Giacomo v Diamond State Tel. Co. (1973, DC Del) 356 F Supp 1063.

29. Review

In review of action seeking to enjoin discontinuance of telephone service pursuant to 18 USCS § 1084 as result of violation of state law, Court of Appeals cannot address itself to question of criminal penalties in such civil action. Angelini v Illinois Bell Tel. Co. (1969, CA7 Ill) 418 F2d 111, cert den

(1970) 397 US 1040, 25 L Ed 2d 651, 90 S Ct 1361.

V. PROSECUTION AND PUNISHMENT

30. Venue

Defendants indicted for transmitting gambling information from Nevada to Utah in violation of 18 USCS § 1084(a) could be prosecuted in Utah as well as in Nevada, since essential ingredient of offense under 18 USCS § 1084 is communication from one state into or through another over wire facility; such offense is of continuing nature that may be committed both in district where use of wire facility occurred and district where communication was received. United States v Synodinos (1963, DC Utah) 218 F Supp 479.

Offense under 18 USCS § 1084(a) may be prosecuted either in district in which prohibited message originated or in which it was received. United States v Cohen (1964, ND Cal) 35 FRD 227.

Defendant, indicted in Federal District Court for District of Nebraska for violation of 18 USCS § 1084(a) and arrested in Southern District of New York, was denied request for order directing United States Commissioner in latter district to dismiss proceedings for removal to District of Nebraska, on alleged ground that no venue existed with regard to defendant in that district, where "transmission" or "sending" was alleged in indictment as being from New York, New York; question as to proper venue under 18 USCS § 1084(a) is determined by court in district where indictment was returned. United States v Winston (1967, SD NY) 267 F Supp 555.

In prosecution for violation of 18 USCS § 1084 arising from telephone transmission of information assisting in placing of bets or wagers, since defendant was charged as principal and since 18 USCS § 1084 is continuing offense, venue is proper in any district where offense was begun, continued, or completed. United States v Sklaroff (1971, SD Fla) 323 F Supp 296.

31. Grand jury proceedings

Indictment charging violation of 18 USCS § 1084 was proper even if some incompetent evidence had been placed before grand jury where defendant's conviction was based entirely upon admissible evidence and grand jury heard principal Government witness and scrutinized documentary evidence relating to telephone calls, all of which was competent and independent of suppressed evidence. Truchinski v United States (1968, CA8 Minn) 393 F2d 627, cert den (1968) 393 US 831, 21 L Ed 2d 103, 89 S Ct 104.

32. Indictment

Indictment which did not charge defendants with "gambling," but rather with interstate travel with intent to promote business enterprise involving gambling offenses, consisting of pastpost betting on horse races, was sufficient to charge violations of 18 USCS §§ 1084, 1952. United States v Bergland (1963, CA7 Wis) 318 F2d 159, cert den (1963) 375 US 861, 11 L Ed 2d 88, 84 S Ct 129.

Defendant was convicted on two counts of indictment charging violation of 18 USCS § 1084(a), and first count alleged that during certain period defendant knowingly used interstate telephone facilities to transmit information from Nevada to California for purpose of assisting in placement of wager; first count charged but single offense of knowingly transmitting wagering information by interstate telephone between points, during period, and for purpose specified, and it was not rendered duplicitous merely because bill of particulars and subsequent proof related to series of calls, even though each call might have been alleged as separate violation. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

Although indictment charging defendant in first count of transmitting by telephone information assisting in placing of bets and wagers in violation of 18 USCS § 1084 and in second count with interstate use of telephone facilities to carry on unlawful gambling business in violation of 18 USCS § 1952 was not duplicitous or so vague as to fail to charge offense, it should have been supplemented by bill of particulars which was sought but denied. Nolan v United States (1968, CA5 Tex) 395 F2d 283.

Defendants' contention that conspiracy count in indictment was insufficient because agreement was not defined was without merit where indictment alleged that defendants agreed together and with each other to use telephone facilities to carry on gambling business in violation of, inter alia, 18 USCS § 1084, since indictment clearly alleged offenses with which defendants agreed to commit and defined object of agreement and not simply course of conduct. United States v McLeod (1974, CA7

Ind) 493 F2d 1186.

Allegation that defendant bookkeeper made phone calls which violated 18 USCS §§ 1952 and 1084 over 9-day period was sufficiently specific, despite lack of itemization of which phone calls violated statute, since time frame was narrow, and defendant was charged with specific course of conduct, i.e., making book, so that he was fully able to defend himself against charge. United States v Segal (1989, CA8 Minn) 867 F2d 1173, 89-2 USTC P 9651, 64 AFTR 2d 89-5187.

Count of indictment alleging violation of 18 USCS § 1084 during football season was not duplicitious where, in view of amended and corrected bill of particulars, count was limited to one date on which one bettor was alleged to have placed bet over interstate telephone with defendant on one sporting event. United States v Cohen (1964, ND Cal) 35 FRD 227.

Exact words used by sender or receiver are not critical to conviction under 18 USCS § 1084 prohibiting use of interstate facilities to transmit wagering information; hence indictment charging violation of 18 USCS § 1084 was not defective for failure to specify conversations transmitted interstate. United States v Brodson (1975, ED Wis) 390 F Supp 774.

33. Joinder and severance

Failure to sever as to defendant charged with violating 18 USCS §§ 1084, 1952 was abuse of discretion in violation of USCS Rules of Criminal Procedure, Rule 14, where (1) government's case covered more than 2300 pages of transcript, and less than 50 of those pages were relevant to defendant, (2) most of the rest dealt with other defendants and transactions involving the handling and "doping" of horses, with which defendant had no connection, and (3) conspiracy charge linking other defendants had been dismissed as against defendant. United States v Donaway (1971, CA9 Cal) 447 F2d 940.

Although severance is required when defendant will be unable to have fair trial in absence of codefendant's testimony, statement of codefendant that defendant was not engaged in business of betting and wagering, in prosecution under 18 USCS § 1084, was not so exculpatory in nature that its absence would deny defendant fair trial and severance was not justified. United States v Brodson (1975, ED Wis) 390 F Supp 774.

34. Separate offenses

Each interstate call made by defendant engaged in making interstate telephone calls to place wagers was separate offense under 18 USCS § 1084. Katz v United States (1966, CA9 Cal) 369 F2d 130, revd on other grounds (1967) 389 US 347, 19 L Ed 2d 576, 88 S Ct 507.

Defendant's contention that he was prejudiced by inclusion of multiple violations in single count of indictment, one count of which charged him with multiple violations of 18 USCS § 2(b), general aiding and abetting statute, for causing interstate calls which, if made by defendant directly, would have constituted violation of 18 USCS § 1084(a) was without merit where Government had provided bill of particulars as to specific telephone calls that it intended to prove, and offense was continuing course of conduct that to advantage of defendant in that respect, might have been treated as one course of conduct and one offense. United States v Kelley (1968, CA2 NY) 395 F2d 727, cert den (1968) 393 US 963, 21 L Ed 2d 376, 89 S Ct 391.

35. Search and seizure

Tape recording which was apparently record of bets was not outside scope of search warrant since it was clearly within description contained in search warrant "bookmaking records and wagering paraphernalia" and was admissible in prosecution for violation of, inter alia, 18 USCS § 1084. United States v Fuller (1971, CA4 SC) 441 F2d 755, cert den (1971) 404 US 830, 30 L Ed 2d 59, 92 S Ct 74.

Affidavit of informant was sufficient to support issuance of search warrant where defendant was suspected of violating 18 USCS § 1084 and where informant made detailed statements relating to organizational procedures of gambling operation, disclosed to magistrate that he was advised that two telephones were maintained at each of the specified addresses, that frequent long-distance toll calls were made between all 3 addresses, and that telephone service at one of addresses was in name of known gambler. United States v Sellers (1973, CA5 Ala) 483 F2d 37, 25 ALR Fed 233, reh den (1973, CA5 Ala) 485 F2d 688 and cert den (1974) 417 US 908, 41 L Ed 2d 212, 94 S Ct 2604 and (ovrld on other grounds by United States v McKeever (1990, CA5 Tex) 905 F2d 829).

Search warrants which alleged that evidence to be seized was being used by persons engaged in

bookmaking business who transmit bets and wagers and information assisting in placing of bets and wagers in interstate commerce in violation of 18 USCS §§ 371, 1084, and 1952 was not invalid on ground that 18 USCS §§ 371, 1952 can no longer be basis of criminal conviction as they are violative of USCS Constitution, Amendment 5 privilege against self-incrimination since 18 USCS § 1084 was still enforceable. Dudley v State (1972) 228 Ga 551, 186 SE2d 875.

36. Discovery

Defendants, convicted of interstate gambling telephone operations and conspiracy to transmit wagers through an interstate wire operation, had no cause to complain of USCS Constitution, Amendment 4 violations when the trial judge, in an in camera proceeding, denied defendants standing to obtain federal transmission logs containing references to only unknown voices, physical surveillance notes of the FBI, and FBI's interoffice memoranda (airtils). United States v Kane (1971, CA5 Fla) 450 F2d 77, cert den (1972) 405 US 920, 30 L Ed 2d 790, 92 S Ct 947 and cert den (1972) 405 US 934, 30 L Ed 2d 810, 92 S Ct 954.

37. Evidence; admissibility

Testimony of witnesses relating to placement of bets with defendant by interstate telephone which occurred both before and after effective date of 18 USCS § 1084 was admissible and relevant to show "scheme or plan" by defendant to conduct gambling business using interstate telephone facilities and that violations charged were deliberate and not results of accident or inadvertence. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

Evidence obtained from telephone company's continued monitoring and tape recording of defendant's conversations after ample evidence had been secured of illegal use by defendant of company's facilities in violation of 18 USCS § 1084 was inadmissible. Bubis v United States (1967, CA9 Cal) 384 F2d 643.

Testimony of defendant, in prosecution for violation of, inter alia, 18 USCS § 1084, concerning application for wagering tax stamp and filing of returns showing wagering income was inadmissible as violative of USCS Constitution, Amendment 5 privilege against self-incrimination and was reversible error where testimony was extremely important part of Government's case. Nolan v United States (1968, CA5 Tex) 395 F2d 283.

Admissibility of secondary evidence is within broad discretion of trial judge; in prosecution under 18 USCS § 1084, introduction of toll records which were copies of originals was admissible and trial judge did not abuse discretion in ruling that testimony of security officer of telephone company that diligent search of office had not uncovered originals was sufficient foundation for introduction of identified copies. United States v Covello (1969, CA2 NY) 410 F2d 536, cert den (1969) 396 US 879, 24 L Ed 2d 136, 90 S Ct 150, reh den (1970) 397 US 929, 25 L Ed 2d 110, 90 S Ct 897.

Defendant was not entitled to have evidence seized by agents of Treasury Department excluded and search warrants retroactively invalidated upon dismissal of count charging defendants with failing to pay special tax imposed by 26 USCS §§ 4411, 4412, since defendant was also charged with violation of 18 USCS §§ 1084, 1952 which were totally unrelated to wagering tax provisions. United States v Armiento (1971, CA2 NY) 445 F2d 869, cert den (1971) 404 US 853, 30 L Ed 2d 93, 92 S Ct 94.

District Court properly denied motion to suppress evidence concerning violations of 18 USCS §§ 1084, 1952 even though the detailed affidavits predicating the search warrants partially concerned violations of wagering tax statutes subsequently rendered unenforceable by United States Supreme Court. United States v Armiento (1971, CA2 NY) 445 F2d 869, cert den (1971) 404 US 853, 30 L Ed 2d 93, 92 S Ct 94.

38. --Sufficiency

In prosecution under 18 USCS §§ 371, 1804, act of one conspirator is act of other, whether present or absent, if performed in furtherance of combination, separate wrongdoing of 2 codefendants was imputable to other and evidence was therefore sufficient to support both substantive counts as well as conspiracy. United States v McGowan (1970, CA4 Va) 423 F2d 413.

Deputy sheriff's single observation of defendant using ticker tape machine together with paper dropped by defendant at time of arrest containing notations identified as record of bet and slips with similar notations which had been scattered around ticker tape machine was sufficient to present to

jury issue whether defendant's use of ticker tape machine was with intent to carry on enterprise involving gambling. United States v Ippolito (1971, CA5 Fla) 438 F2d 417, cert den (1971) 402 US 953, 29 L Ed 2d 123, 91 S Ct 1620.

Evidence that substantial portions of defendant's income were from pari-mutual betting, a lawful activity sanctioned by state law, did not establish that defendant is in business of betting in violation of 18 USCS § 1084. United States v Donaway (1971, CA9 Cal) 447 F2d 940.

In prosecution for, inter alia, knowing use of a telephone for the interstate transmission of information assisting in the placing of bets and wagers on sporting events, in violation of 18 USCS § 1084, evidence that defendant was observed copying line in local sports book, and then drove to a public telephone and read contents of line sheet into telephone, and that within an hour, codefendant was arrested in Indianapolis and line sheet was found in his possession bearing posting identical to that copied and read by defendant, was sufficient to support jury's conclusion that defendant completed telephone call to Indianapolis and relayed day's line information. United States v McLeod (1974, CA7 Ind) 493 F2d 1186.

Defendants' conviction of violation of 18 USCS § 1084 was supported by sufficient evidence where, on record, jury could find that: (1) defendants were engaged in business of betting or wagering, (2) telephone conversations were made across state lines, and (3) in each call, information assisting in placing of bets was transmitted. United States v Florea (1976, CA6 Ohio) 541 F2d 568, cert den (1977) 430 US 945, 51 L Ed 2d 792, 97 S Ct 1579, reh den (1977) 431 US 925, 53 L Ed 2d 240, 97 S Ct 2201.

Defendant was improperly convicted of violating 18 USCS § 1084 even though evidence showed his awareness of certain interstate gambling activity, his discussion of merits of certain wagers with co-defendant who lived in same state, his placing of substantial bets with such co-defendant, and his collection of line information on phone, since no evidence was introduced relative to requirement that defendant was actually in "business of betting or wagering," and fact that record indicated defendant was friend of convicted co-defendant with whom he regularly bet did not establish his status as aider and abettor. United States v Anderson (1976, CA7 Wis) 542 F2d 428.

Evidence was sufficient to sustain conviction for conspiring to violate 18 USCS § 1084 where tape recordings contained conversation clearly referring to organized gambling operations in which defendants were participants. United States v Barletta (1977, CA8 Mo) 565 F2d 985, 2 Fed Rules Evid Serv 676.

Evidence was sufficient to sustain defendant's conviction for violation of 18 USCS § 1084 where it was shown that defendant furnished line information to person who operated substantial bookmaking business in Minneapolis area, that person relied on this information, that some sort of financial arrangement existed between defendant and person, that defendant was fully aware of person's bookmaking operation, and that accurate and up-to-date line information is of critical importance to any bookmaking operation. United States v Scavo (1979, CA8 Minn) 593 F2d 837, 4 Fed Rules Evid Serv 62.

Defendant's telephone toll records introduced at trial which indicated 728 calls to 2 codefendants and 139 calls from codefendants in period from May 1977 through January 1978, testimony of witnesses that they were betting with defendant in 1977, along with racing form and line sheets seized during defendant's arrest was sufficient evidence from which jury could conclude defendant was engaged in continuous activity characterized as business of betting or wagering within meaning of 18 USCS § 1084; there is no requirement that defendant be proved to have exclusively engaged in business of betting or wagering; evidence of telephone records indicating that calls were placed from telephone service in defendant's name and fact that records for period did not reflect any request for credit for calls is sufficient to establish that defendant placed calls; despite defendant's contention that information received could not have assisted in placing of bets or wagers on sports events, where testimony of New York and Los Angeles services testified that service provided sports scores of games in progress, final scores, overnight wrap-up stories and general late breaking sports news was adequate to show that recorded information could have assisted defendant in placing and accepting of bets and wagers. United States v Reeder (1980, CA8 Ark) 614 F2d 1179, 5 Fed Rules Evid Serv 1324.

39. --Prejudicial effect

Mere presence of unconstitutional counts in indictment charging violation of 18 USCS § 1084 is not prejudicial and was not tantamount to improper comment upon defendant's failure to testify where

only proof adduced on unconstitutional counts which was not independently admissible on permissible counts as well was stipulated testimony of records witnesses offered to show defendant's failure to register to pay wagering tax which had no tendency to establish that he was gambler. United States v Kelley (1968, CA2 NY) 395 F2d 727, cert den (1968) 393 US 963, 21 L Ed 2d 376, 89 S Ct 391.

Error, if any, in failure to permit defendant to inspect, in prosecution for violation of, inter alia, 18 USCS § 1084, federal income tax returns of prosecution witnesses was not prejudicial since returns did not constitute "statements" of witnesses within meaning of Jencks Act [18 USCS § 3500]; filing of returns was unconnected with investigation of defendant's activities or criminal proceedings initiated against him, and returns were filed with entirely separate federal agency. United States v Covello (1969, CA2 NY) 410 F2d 536, cert den (1969) 396 US 879, 24 L Ed 2d 136, 90 S Ct 150, reh den (1970) 397 US 929, 25 L Ed 2d 110, 90 S Ct 897.

Any error arising from jury's rehearing of portions of tape recording which had not been admitted into evidence was harmless in prosecution under 18 USCS § 1084 and did not prejudice defendants in any manner where only issue at trial was whether defendants used telephone in interstate commerce. United States v Sellers (1973, CA5 Ala) 483 F2d 37, 25 ALR Fed 233, reh den (1973, CA5 Ala) 485 F2d 688 and cert den (1974) 417 US 908, 41 L Ed 2d 212, 94 S Ct 2604 and (ovrld on other grounds by United States v McKeever (1990, CA5 Tex) 905 F2d 829).

40. Witnesses

Witness who was granted immunity from prosecution had no right under USCS Constitution, Amendment 5 and corresponding immunity from prosecution derived therefrom to protect other parties and was not entitled to claim privilege of silence in order shield associates or those with whom he had dealings. Marcus v United States (1962, CA3 Del) 310 F2d 143, cert den (1963) 372 US 944, 9 L Ed 2d 969, 83 S Ct 933.

41. Instructions

In prosecution under 18 USCS § 1084, trial court properly refused Defendant's requested instruction that government was required to prove that defendant had proprietary interest in wagering business in which he engaged and shared in profits and losses. Cohen v United States (1967, CA9 Cal) 378 F2d 751, 5 ALR Fed 147, cert den (1967) 389 US 897, 19 L Ed 2d 215, 88 S Ct 217.

Failure of court to give specific intent instruction in prosecution for violation of 18 USCS § 1084 was harmless error; trial court properly rejected defendant's offer of instruction limiting application of phrase "engaged in the business of betting or wagering" to "bookmakers". United States v Scavo (1979, CA8 Minn) 593 F2d 837, 4 Fed Rules Evid Serv 62.

42. Speedy trial

Where there had been a delay of six years because there was a novel question of law as to whether the transmission of wagering information which was prohibited under 18 USCS § 1084 involved tips on horse races and not communicating results directly to bookies, there was no reasonable justification and defendant was prejudiced and did not waive his right to speedy trial. United States v Baron (1971, SD NY) 336 F Supp 303.

Chicago Tribune, July 1, 2000

July 1, 2000 Saturday, CHICAGOLAND FINAL EDITION

SECTION: News; Pg. 1; ZONE: N

LENGTH: 1343 words

Unwanted Gaze - Material

HEADLINE: CLINTON OKS E-SIGNATURES AS PART OF PRIVACY PUSH

BYLINE: By Frank James, Washington Bureau.

DATELINE: WASHINGTON

BODY:

President Clinton on Friday signed legislation making electronic documents bearing digital signatures as legal as their old-fashioned pen-and-paper counterparts.

Companies will be able to execute contracts to buy and sell goods, and consumers will be able to sign mortgages and car loans online, as Clinton noted in a Philadelphia ceremony. And they will be able to do so with a high level of security. Digital signatures use encryption, which scrambles computer communications to keep them private and accessible only to the sender and recipient.

The signing of the bill, which takes effect Oct. 1, was just another step by Clinton to enhance Americans' privacy, especially on the Internet. In the second half of his presidency, privacy has become his passion.

In a recent commencement address at Eastern Michigan University, Clinton referred no fewer than 14 times to the importance of protecting privacy, especially now that a person's medical and financial data can be transmitted instantly across the globe.

This speech was another occasion where Clinton emphasized the important role government can play in safeguarding individual privacy. He also urged the private sector to do more.

"In this Information Age, we can't let new opportunities erode old fundamental rights," Clinton said in Ypsilanti, Mich. "We can't let breakthroughs in technology break down walls of privacy."

With technology changing rapidly, Clinton has been forced to confront the issue and, some experts say, he has become the strongest privacy advocate to occupy the White House. Yet privacy rights experts and civil libertarians say Clinton's current stand contrasts sharply with his earlier seeming indifference. Some observers wonder whether the president's own loss of privacy during the Monica Lewinsky scandal heightened his sensitivity to the issue.

Vice President Al Gore, the presumptive Democratic nominee for president, has also picked up on the

privacy theme. Gore recently announced legislation to stop the commercial sale of Social Security numbers as a way to enhance individual privacy.

Meanwhile, Texas Gov. George W. Bush's campaign has yet to decide how to address Americans' privacy concerns.

"The governor does feel strongly about and has spoken out about the importance of protecting people's privacy," said Ray Sullivan, a campaign spokesman. "We're examining that complicated issue in more detail right now."

Early in Clinton's administration, though, reviews from privacy advocates were not glowing. "If you asked most privacy advocates in Clinton's first term, or even before impeachment, I think they would have said Clinton was one of the worst presidents on privacy in the postwar period," said Jeff Rosen, a professor at George Washington University Law School.

"It's true . . . after his impeachment, Clinton seems to have found religion," Rosen said.

"Whether he's been chastened by his own experience at the hands of the independent counsel is hard to say," said Rosen, who wrote "The **Unwanted Gaze,**" a new book that looks at eroding privacy rights in America. "If a conservative is a liberal who has been mugged, maybe a privacy advocate is a president who's been impeached after having his privacy invaded," Rosen said.

Clinton has mentioned the need for greater privacy in his last two State of the Union speeches, and last year he appointed Peter Swire as the White House's chief privacy counsel.

The president has acted on several fronts. He signed an executive order to ban the use of genetic information by federal employers in hiring and other work-related decisions. He lobbied for stronger consumer privacy provisions in a financial modernization bill he signed earlier this year. And the Health and Human Services Department has drafted rules to protect the privacy of electronic medical records.

However, the White House was recently embarrassed by disclosures that its National Drug Control Policy Office had quietly placed small bits of computer code known as "cookies" on the computer hard drives of visitors to the agency's Web site.

Many privacy advocates consider cookies a privacy intrusion because they are typically used to track pages a visitor looks at on a Web site.

The discovery caused the White House to order all executive branch agencies to review privacy practices and agency heads to approve use of cookies. As a show of its seriousness, the administration said if agencies violated the new rules, their budgets would be cut.

As for electronic commerce, the president and administration have largely resisted calls for legislation to protect individuals, preferring to let Commerce Secretary William Daley, who will be departing soon, jawbone the private sector in policing itself. Some critics saw this policy as negative for privacy.

"This whole self-regulation has really been a slowdown of privacy and a naive approach," said Robert Ellis Smith, a privacy expert. "The Commerce Department is not at all pushing for privacy."

The other president who stressed privacy would likely surprise many Americans: President Richard Nixon.

Nixon signed the Privacy Act, which attempts to protect the records of individuals from misuse by federal bureaucrats. He also had a White House privacy committee headed by his vice president, Gerald Ford.

In his 1974 State of the Union speech, his last before he resigned in disgrace, Nixon said: "One measure of a truly free society is the vigor with which it protects the liberties of its individual citizens. As technology has advanced in America, it has increasingly encroached on one of those liberties--what I term the right of personal privacy.

"Modern information systems, data banks, credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another--all these have left millions of Americans deeply concerned by the privacy they cherish," Nixon said.

It was a huge irony for a president whose operatives repeatedly violated the privacy of Americans through infamous break-ins of Democratic Party offices at the Watergate building and a psychiatrist who had treated a critic of the administration's Vietnam policy.

Privacy advocates bristled at the Clinton administration's support for strict controls on encryption software, the technology that keeps computer communications and data secret by scrambling them.

The administration argued that the need to battle criminals and terrorists who use computers to commit crimes required authorities to have access to digital "keys" and a ban on the export of the best encryption software.

After considerable pressure from the industry, Congress and privacy advocates, the White House largely relented.

"Nobody was tougher to talk to when we started talking about safety and security on the Internet, and this was back in 1994," said Sen. Conrad Burns (R-Mont.). "They just didn't want to talk about this issue at all," he said of the White House.

Supporters of strong privacy protections also pointed to Clinton's support in 1996 of a so-called roving wiretap law. It allowed "federal agents and police to tap not only a particular phone, but any phone the target of an investigation comes close to," said James Dempsey, senior staff counsel for the Center for Democracy and Technology, a Washington-based group that advocates on behalf of technology and privacy issues.

"All of these are examples of a president who repeated the inclinations he showed as governor in Arkansas, which was to be much more concerned about being tough on crime than about civil libertarian concerns," Rosen said. "He'd never been much of a civil libertarian either in Arkansas or for most of his presidency."

The privacy issue was raised recently when a federal judge found Clinton guilty of violating the Privacy Act by releasing personal correspondence he received from Kathleen Willey, the former White House volunteer who claimed the president groped her. Clinton, his lawyers and outside legal experts have disagreed with the judge.

GRAPHIC: PHOTOPHOTO (color): President Clinton uses an electronic signature card Friday to sign a bill legalizing electronic documents with digital signatures. Reuters photo.

LANGUAGE: ENGLISH

LOAD-DATE: July 1, 2000

86 A.B.A.J. 86

July, 2000

86 A.B.A.J. 86

LENGTH: 1247 words

SECTION: Books

TITLE: Protect the Veils of Privacy: Gender harassment law and high tech combine for 'jurisprurience'; THE **UNWANTED GAZE;** The Destruction of Privacy in America; By Jeffrey Rosen; Random House, 288 pages; $ 24.95

TEXT:

Reviewed by Steve France

For Jeffrey Rosen, legal editor of *The New Republic*, the Monica Lewinsky scandal was all about promiscuity. But not the sexual kind. In his new book, *The **Unwanted Gaze***, Rosen is concerned about what he sees as the indecencies of a computer age "jurisprurience."

Rosen says Monicagate exposed a legal system that routinely takes liberties with Americans' privacy, often using new types of high-tech evidence. Without wiretaps, bodywires, e-mail searches and DNA testing, the law might never have wrested confessions from President Clinton and his admirer.

Indeed, technology has changed and multiplied the ways we gaze at each other, in both wanted and unwanted ways, Rosen says. Life is an increasingly kaleidoscopic hall of mirrors, where we can see and hear others and be seen and heard in various newly configured bits and pieces.

Despite the dazzling technology, however, Rosen argues we can still carve out defensible boundaries of privacy in cyberspace. He even sees signs that the market will produce new technology and services to shield personal information.

Unfortunately, that won't do much good when it comes to the legal machinery that propelled Clinton's private life into court. There is nothing high-tech about a subpoena for a pen-and-ink diary, for example.

No Windows Into Souls

On that front, at least, nothing has changed since Queen Elizabeth I declared she did not want windows into men's souls. She meant that she would not use her power to force open the secrets of her subjects' religious and political beliefs. It was a great moment in the evolution of liberty, which only exists when the state refrains from entering the private recesses of human consciousness and

puts some limits on citizens' encroachment on others' privacy.

At the same time, as social animals, men and women are eager to open windows into their souls and look into those of others.

It's called communicating. In Elizabeth's time, new windows were being opened with abandon: Martin Luther had triggered a torrent of disturbing and inspiring public confessions; Michel de Montaigne invented a new literary form, the essay, that was the equivalent of thinking private thoughts aloud; and Shakespeare guided audiences deep into the private agonies and ecstasies of his characters.

But windows need curtains, Rosen says, especially to keep the state from peering in. He describes the threadbare condition of the legal veils that once shielded personal diaries and letters, and the way civil courts are stripping ordinary Americans of their privacy.

Personal communication is always a risky business. Tell a joke or make an overture that elicits a negative social response and the pain is sharp and lasting.

You can tell the joke; he, she or they can think that it's ugly and shun or shame you accordingly. But these days in the workplace such social control is not enough. The state has targeted a new kind of blasphemy, Rosen argues. In case after case, he shows how, when it comes to gender discrimination, the law's brooding gaze has become omnipresent.

The law hovers over workers because of worries that too many people will find certain jokes amusing or will not see the harm in clumsy overtures. The offended party is not encouraged to persuade others, even the perpetrator, by simple communication, that something was offensive; instead the power of the state is deployed.

Undaunted by Ambiguities

A fast-growing stack of books tells us how tricky it can be for us to understand one other. Yet, undaunted by such ambiguities, legal authorities gaze into the souls involved in workplace incidents with the narrow aim of classifying them as victims or offenders.

Efforts to apologize or explain and just get along are discouraged. Everyone in the organization is drafted into a legal drama where everything they say (or may have said) is evidence.

Rosen recounts how evidentiary rules have been re-engineered to promote complaints and amplify fallout. "The sexual history of the accuser [is] more or less off-limits, while that of the accused [can] be mined for damaging incidents," he says, regardless of the harm to third parties (e.g., Monica's friends).

The key, Rosen says, is that "harassment law has been designed to protect the reputation of women in general." The wrong is to create an environment where, as he quotes an EEOC Policy Guidance, "a message is implicitly conveyed that the managers view women as 'sexual playthings.'"

To fight that evil, the law forces employers to act as police. Simply by making private employers liable for the hostile environment their employees may create, the law has created an army of big brothers (and sisters) not subject to the constraints that limit government.

Rosen surveys the damage this regime does to workers' freedom to fashion their own social environment while doing their jobs, but he does not deny the need to protect individuals from harassment. Rather, he struggles to describe what is and what is not verboten in the workplace.

Exploring where consensual relationships fit in, for example, he notes, "A third of all romances begin at work." The romances often feature senior males and junior females. (Bill Gates, for example, dated Microsoft employee Melinda French for five years before they married.) But about a quarter of

the costly lawsuits involve "soured romances" that ended without marriage.

In the end, Rosen gives up on making sense of the current rules, thus joining many others in the work force who have concluded that any personal conversation between individuals is a minefield if it has any conceivable gender overtones. Case law and litigation economics drive otherwise easygoing employers to take absurd precautions. We all have silly or chilling stories to tell.

Although Rosen is indignant about these excesses, he still sees a need for legal controls in this area. He argues for treating most harassment cases under invasion of privacy doctrines, not discrimination law.

Those tort doctrines, Rosen notes, "focus on speech targeted at a particular woman that has the purpose or effect of insulting or humiliating her." They put the blame for inappropriate conduct on the perpetrator, not the employer or other workers, unless they participated. Only conduct that goes well beyond teasing or obtuseness is condemned.

Reasserting Boundaries

Rosen's approach would be bad news for litigators, who need deep corporate pockets, and for social activists, who need broad brushes. Employers once again could decide what the appropriate rules should be and how much freedom to allow their employees in working out issues among themselves. Debates about gender and sex would largely play out in the social sphere, not the courts.

In Clinton's case, without any lawsuits, Linda Tripp's tapes would have put him on the spot and sparked fierce debate about his fitness for office. As his boss, we might have driven him from office. Ironically, the debate and any chance that public opinion would turn against Clinton were preempted by public disgust with the legal shenanigans of the Paula Jones and Kenneth Starr teams.

Rosen says public support for the president was driven by a determination to "reassert the boundaries" between the public and private spheres. His book argues for reasserting those boundaries for the rest of us, too

Steve France is a lawyer and journalist in Washington, D.C.

LANGUAGE: ENGLISH

GRAPHIC: Photo 1, JEFFREY ROSEN; Photo 2, JEFFREY ROSEN Most harassment cases should be treated under invasion of privacy doctrines, not discrimination law., CHRISTOPHER BILRLEIN PHOTO

View: Cite | KWIC | **Full** | Custom PREVIOUS **5 of 51** NEXT Text Only | Download | Fax | Email
FOCUS™ - Narrow Results | Save As ECLIPSE | More Like This | More Like Selected Text

86 A.B.A.J. 86

Source: All Sources : / . . . / : **News Group File, All**
Terms: **unwanted gaze** (Edit Search)
View: Full
Date/Time: Wednesday, July 5, 2000 - 4:10 PM EDT

Search | Search Advisor | Get a Document | Check a Citation
ECLIPSE(TM) | History | Change Client | Options | Feedback | Sign Off | Help
About LEXIS-NEXIS | Terms and Conditions

The Detroit News, June 13, 2000

June 13, 2000, Tuesday

SECTION: Front; Pg. 1

LENGTH: 1106 words

HEADLINE: Granholm fights Net snoops
Precedent-setting lawsuit targets Web sites she says violate privacy of browsers online

BYLINE: Mark Hornbeck / Detroit News Lansing Bureau

DATELINE: LANSING

BODY:
LANSING -- Atty. Gen. Jennifer Granholm launched a first-of-its-kind legal crusade Monday against companies she says are violating the privacy of Michiganians who browse the Internet.

Granholm sent notice that she'll seek a precedent-setting lawsuit against four commercial Web site companies that allow the use of Internet "cookies" -- tiny bits of text that track a person's activities on the Web to develop profiles of potential customers -- without properly informing customers they're being watched.

Some businesses that get information from the Web bugs could pass it on to marketers and others on the Internet -- information that could wind up damaging the customers' relationships with insurers and employers, Granholm said.

The companies -- a medical site, a pornography site, a stock-trading site and a baby-clothing site -- have 10 days to respond before a lawsuit is filed.

At issue is whether these so-called Web bugs violate the Internet user's privacy, subject them to unwanted solicitations by advertisers and potentially put sensitive, private information in the wrong or unintended hands, Granholm said.

"It's similar to Big Brother, but I like to call it Big Browser," Granholm said. "People have no idea their thoughts and practices on the Internet are being tracked or policed. We're going after this secret, third-party surveillance."

Cookies have been a controversial issue in the Internet world for several years. Many major companies, including The Detroit News, use cookies to tailor their Web sites to the users' interests. But the News, like some companies, does not share the information.

The sharing of information from cookies is part of the growing concern about a loss of privacy on the

Internet and how commercial Web sites use information. "They are an invasion of privacy and do not always say how to delete them," said Pete Jimenez, 25, a party-store manager in Detroit who regularly surfs the Internet. "We should have privacy laws to protect us from them."

Granholm will use the Michigan Consumer Protection Act as her hammer. The act bars companies from "engaging in certain unfair, unconscionable or deceptive methods, acts and practices in the conduct of trade or commerce." The law allows for civil penalties up to $25,000 per violation.

Creative cookie cruncher

Jeffrey Rosen, George Washington University law professor and author of the book **Unwanted Gaze:** Destruction of Privacy in America, said Granholm may have hit on a creative way to attack Web privacy issues.

"Judges generally have ruled that any time you surrender information to a third party for one purpose, you abandon protection against having that information used for other purposes," Rosen said. "But if the Michigan law is carefully drafted, it might be an innovative and potentially useful way of combating a serious problem in this country."

The four companies selected -- Ortho Biotech Inc., a medical subsidiary of Johnson & Johnson in Raritan, N.J.; Intimate Friends Network, a pornography site in Lake Worth, Fla.; Stockpoint Inc., a stock-trading site in San Francisco; and AmericasBaby.Com Inc., a site in New York that sells baby clothing and furniture -- were chosen simply because they are representative of the electronic marketplace, Granholm said. They're not the only or even the most serious violators of privacy rights, she said.

"We know this is the tip of the iceberg," Granholm said. "We're holding up these four as examples."

The companies can avert a lawsuit by promising within 10 days to write "true, accurate, clear and conspicuous privacy policies" that inform customers about the Web bugs and how to delete them, Granholm said.

Fighting for consumers

Granholm has staked out consumer protection as a critical mission of her office, just as her predecessor Frank Kelley did for decades. State attorneys general have taken a stronger hand in dealing with societal problems in recent years, most notably the class-action suit against the big tobacco companies. Michigan will receive $8 billion from the companies over the next decade under terms of the settlement.

Defending her cookies campaign, Granholm said Internet users can erase the cookies, but most aren't sophisticated enough to know how to do it, and these companies tend to make it more difficult.

A spokesman for Johnson & Johnson said the action by the attorney general is misdirected.

"Our privacy policy promises that any information gathered from users of our Web site will be anonymous and it will not be shared with anyone," said John McKeegan, spokesman for the New Jersey-based company.

McKeegan said the company's PROCRIT.COM site does contract with DoubleClick Inc., a leading on-line services company that uses cookies. But the information collected is used only by Ortho Biotech to determine the characteristics of its audience and the effectiveness of the Web site, he said.

Granholm said questions on the site ask users whether they take AZT, a drug used by some patients with AIDS. That information could be damaging if sold to a prospective employer or health insurance

company that refuses to write polices for people with HIV or AIDS, she said.

She added that people who browse the Intimate Friends Internet site probably are unaware they're being tracked and labeled by advertisers as pornography users. That information could be passed on to a prospective employer who could use it in hiring decisions, Granholm said. She added that she is unaware of any such cases in Michigan.

Attempts to contact WebPower, the company that operates the site, were unsuccessful.

Stockpoint Inc. said it intends to cooperate with Granholm.

"We support the privacy rights of consumers using the Internet," the company said in a statement. It said its privacy policy is currently not posted on its site because it is undergoing internal review. But the policy will soon be posted, it said.

Detroit News Staff Writer Santiago Esparza contributed to this report.

Internet privacy debated

Cookies are information about a user planted by Web sites onto the hard drive of the user's computer, for the site to access each time the person visits. Sites sometimes share that information, sparking the following debate:

Pro

* Cookies enable marketers to tailor advertising to the specific interests of Web users.

* Targeted marketing saves time for advertisers and consumers.

Con

* Cookies invade the privacy of Internet users and subject them to unsolicited advertising.

* A Web user's private, personal information could be sold to other interested parties, such as employers or insurers.

GRAPHIC: Granholm

LOAD-DATE: June 13, 2000

View: Cite | KWIC | **Full** | Custom PREVIOUS 12 of 51 NEXT Text Only | Download | Fax | Email
FOCUS™ - Narrow Results | Save As ECLIPSE | More Like This | More Like Selected Text

Source: All Sources : / . . . / : **News Group File, All**
Terms: **unwanted gaze** (Edit Search)
View: Full
Date/Time: Wednesday, July 5, 2000 - 4:12 PM EDT

Search | Search Advisor | Get a Document | Check a Citation
ECLIPSE(TM) | History | Change Client | Options | Feedback | Sign Off | Help
About LEXIS-NEXIS | Terms and Conditions

The New York Times, June 7, 2000

June 7, 2000, Wednesday, Late Edition - Final

SECTION: Section A; Page 31; Column 2; Editorial Desk

LENGTH: 982 words

HEADLINE: My Child, Mine to Protect

BYLINE: By Jeffrey Rosen; Jeffrey Rosen, an associate professor at the George Washington University Law School, is the author of "The **Unwanted Gaze:** The Destruction of Privacy in America."

BODY:

On a sharply divided Supreme Court, the principle that liberal and conservative justices increasingly seem to agree on is the right to privacy. This principle was affirmed in two decisions on Monday, strengthening the right of parents to raise their own children and the right of individuals to conceal their private papers.

It may seem odd that this court would affirm the right to privacy. Most of the current justices were appointed by Republican presidents who insisted that the court had erred in the 1960's and 70's, when it discovered a constitutional right to privacy in cases like Griswold v. Connecticut and Roe v. Wade. But these cases, which established the rights, respectively, to use contraception and to choose abortion, were not really about privacy. The court was using the concept of privacy as an imprecise way of establishing the right to sexual autonomy.

In the most recent Supreme Court cases, by contrast, the justices are resurrecting a different concept of privacy, with explicit constitutional roots in the Fourth and Fifth Amendments: the right of people to protect the privacy of their "persons, houses, papers, and effects" from unreasonable state scrutiny.

On Monday, by 6 to 3, the court held that a Washington State law went too far by allowing a judge to grant "any person" rights to visit a child over a mother's objections. Declaring that parents have a "fundamental right to make decisions concerning the care, custody and control" of their children, Justice Sandra Day O'Connor's plurality opinion held that the state court had injected itself "into the private realm of the family" when it ordered visitation rights for grandparents without evidence that the mother was unfit.

The court reaffirmed decisions from the early 20th century that found that parents had the right to send their children to private school and to teach them foreign languages. In the process, the court reaffirmed the right of parents, rather than the state, to define the boundaries of the home.

In the other case decided on Monday, the court, voting 8-to-1, rejected the effort by Kenneth Starr,

the independent counsel, to indict Webster Hubbell for tax evasion after he had issued a subpoena for Mr. Hubbell's private papers and promised him immunity from prosecution.

When the Constitution was drafted, the search of a private diary was considered the quintessential example of an unreasonable search. In a majestic opinion in the late 19th century, the Supreme Court held that a subpoena for business papers violated both the Fourth Amendment, which prohibits unreasonable searches and seizures, and the Fifth Amendment, which prohibits compelled self-incrimination.

By the late 1980's, the court had whittled away at this crucial protection. In 1994, when Bob Packwood tried to conceal his diaries from Senate investigators, Judge Thomas Penfield Jackson concluded that the Fifth Amendment no longer protected the content of private papers from state scrutiny. The Supreme Court refused to review this decision, and when Kenneth Starr subpoenaed Monica Lewinsky's computer and resurrected her unsent electronic love letters, she had no legal recourse.

In the Hubbell case this week, the court breathed a little life into the tattered Fifth Amendment protections: the justices held in the opinion that when the government has "no prior knowledge of either the existence or the whereabouts" of private papers, it can't use subpoenas to go on fishing expeditions for possibly incriminating evidence and then indict citizens based on the papers that they are forced to produce.

In a bold concurring opinion, Justices Clarence Thomas and Antonin Scalia went further still, suggesting that they might be prepared to resurrect the 19th century principle that the Fifth Amendment protects the content of incriminating private papers from state scrutiny, whether or not the government knows of their existence in advance. If this position had been adopted earlier, the diaries of Bob Packwood and Monica Lewinsky might have remained private.

These decisions were only the most recent Supreme Court victories for privacy. In January, the court unanimously upheld the Driver's Privacy Protection Act, in which Congress forbade greedy state departments of motor vehicles from collecting personal information like names, addresses and medical data and then selling it to businesses without a driver's consent.

And in December, in a 7-to-2 decision, the court upheld a California law prohibiting commercial information services from obtaining some police records that are routinely available to journalists and others who agree not to use the information to sell a product or service.

What can explain the recent victories for privacy? Perhaps the justices, who guard their own privacy more zealously than other federal officials, are beginning to recognize how much is lost when citizens cannot record their thoughts and share intimate information without fear of exposure.

Perhaps they remember the crucibles of their own confirmation hearings; they may feel violated when their own deliberations are exposed.

Perhaps, regardless of their dramatically different views about abortion and contraception, both liberal and conservative justices are returning to the original understanding of the Fourth and Fifth Amendments, which had promised all Americans the right to control personal information.

Perhaps they were embarrassed by the Starr investigation, which showed just how dramatically traditional protections of privacy have been allowed to atrophy.

Regardless of the explanation, the court's rediscovery of the right to privacy is a cause for celebration. In an age when independent counsels, state legislatures, police forces and nosy employers are all too ready to violate privacy, it's a relief that the justices are beginning to defend it.

http://www.nytimes.com

GRAPHIC: Drawing

LANGUAGE: ENGLISH

LOAD-DATE: June 7, 2000

Federal News Service April 6, 2000, Thursday

April 6, 2000, Thursday

SECTION: PREPARED TESTIMONY

LENGTH: 3845 words

HEADLINE: PREPARED TESTIMONY OF JEFFREY ROSEN

BEFORE THE HOUSE JUDICIARY COMMITTEE SUBCOMMITTEE ON THE CONSTITUTION

SUBJECT - THE FOURTH AMENDMENT AND THE INTERNET

BODY:

My name is Jeffrey Rosen. I am an associate professor at the George Washington University Law School and legal affairs editor of The New Republic. It is an honor to submit to the Subcommittee on the Constitution this prepared testimony on "the Fourth Amendment and Internet," which is adapted in part from my book, The **Unwanted Gaze:** The Destruction of Privacy in America (Random House.)

Monica Lewinsky is an improbable spokesperson for the privacy on the Internet. But in her memoir, Monica's Story, Lewinsky confesses that she was especially unsettled by Kenneth Starr's decision to subpoena a Washington bookstore for receipts of all of her purchases since 1995. Lewinsky points to the bookstore subpoenas as one of the most invasive moments in the Starr investigation, along with the moment that prosecutors subpoenaed her home computer and retrieved from her hard drive the e-mails she had tried unsuccessfully to delete and the letters she had drafted to the president but never sent.

At the beginning of the twenty-first century, as thinking and writing increasingly take place in cyberspace rather than in the home, many Americans find that their intimate e-mail, Internet browsing, and electronic papers are similar vulnerable to being monitored, searched and exposed by public employers, government agents, or private parties. But rather than adapting to new technological threats to privacy, the constitutional protections for intimate personal information have been eroded by the courts in recent years. The subpoenas issued by Kenneth Starr were perfectly legal, but for most of American history, many of them would have been suppressed as clear violations of the Fourth Amendment to the Constitution. I would like in my prepared testimony to explore some of the reasons that constitutional protections for private papers and diaries and computer files, stored in real space and cyberspace, have evaporated during the past few decades. I will also suggest ways that they might be resurrected.

To appreciate how dramatically privacy protections for private papers have eroded, it's useful to compare the stories of two legislators-- John Wilkes, an eighteenth-century Englishman, and Bob Packwood, a twentieth-century American--who tried to conceal their personal diaries from

overreaching prosecutors, with very different results. Wilkes is largely forgotten today; but his suit against King George's minions for breaking into his London house, in 1763, and seizing his private papers was so galvanizing for the American revolutionaries that the Sons of Liberty in Boston--a group that included John Adams and John Hancock--insisted that "the fate of Wilkes and America must stand or fall together." Wilkes offended King George III by founding a Whiggish scandal sheet called the North Briton, a kind of eighteenth- century Drudge Report.

The King was especially offended by North Briton No. 45, a violent attack on a speech of his praising an obscure German peace treaty signed by Bute. Lord Halifax issued a general warrant authorizing the arrest of the printers, publishers, and authors of North Briton 45, without identifying them by name. After stopping by his printer's office, where he apparently destroyed the original manuscript, Wilkes returned to his house, where he was arrested and transported to the Tower. The King's minions then broke into his house, forced open the drawers of his writing desk, and seized his diaries and private papers. Wilkes sued the King's messengers for trespassing on his property, and he urged a number of other publishers and printers who had been arrested under general warrants to do the same. A jury awarded Wilkes one thousand pounds in damages -- a ruinous amount in its day. Later, Wilkes was elected Lord Mayor of London, and giddy American colonists named towns and infants -- from Wilkes-Barre, Pennsylvania, to John Wilkes Booth - in his honor.

More than two centuries later, when Bob Packwood, Republican from Oregon, tried to conceal his diaries from his fellow-legislators, he found that the legal protections for private papers had evaporated. Packwood served as a senator for twenty-six years, from 1969 to 1995.

More than two dozen former female employees and lobbyists accused him of making unwanted sexual advances during this time, but most of them described incidents that had occurred before the Supreme Court decision, in 1986, that definitely recognized sexual harassment as a civil offense. The exception was Packwood's former press secretary, who claimed that, in 1990, after an evening of drinking with colleagues, the Senator had made an unwanted advance but had retreated after being rebuffed. Summoned before the Senate Ethics Committee, Packwood tried to argue that the advance wasn't unwanted. On being asked to corroborate this claim, Packwood confessed that he had written about it in his diary.

This gave the ethics committee an opening to subpoena all of the diaries that Packwood had dictated between 1989 and 1993. Alarmed at the thought of his colleagues rummaging freely through his most private thoughts, Packwood suggested that the committee should instead appoint an "Independent Examiner" to review the diaries and decide which passages were relevant to the charges of sexual misconduct. (The former appellate judge whom Packwood recommended that the Senate appoint as Independent Examiner was Kenneth Starr.) Packwood's lawyers then contested the subpoenas, citing a famous opinion from 1886, Boyd v. U.S., in which the Supreme Court had recited the story of John Wilkes, and then announced that subpoenaing a defendant's private business papers in order to use them against him was both an unreasonable search and a form of compelled self-incrimination, violating both the Fourth and Fifth Amendments, which "run almost into each other." In a stirring conclusion, Justice Bradley announced that "any compulsory discovery by extorting the party's oath, or compelling the production of his private books and papers, to convict him of crime or to forfeit his property, is contrary to the principles of a free government. It is abhorrent to the instincts of an American."/1

Unmoved by Packwood's citation of the Boyd case, Judge Thomas Penfield Jackson of the U.S. District Court in Washington ordered him to turn over his diaries to the Senate. The nineteenth century right to privacy, Jackson noted, had been chipped away by subsequent Supreme Court decisions which were initially motivated by a single purpose: eradicating white collar crime. In the years leading up to the Progressive era, it became clear that if people could refuse to turn over their corporate records in response to grand jury subpoenas, then it would be impossible to enforce antitrust laws or railroad laws, and the regulatory state would come to a grinding halt. Well before the New Deal, the Court decided that the only way to investigate corporate crime would be to give prosecutors broad power to subpoena witnesses and to produce documents. And in 1948, the New Deal Court held that the Fifth Amendment wasn't violated by requiring someone to produce records

that the government had ordered him to keep, no matter how incriminating or embarrassing the records might be.

But the Warren and Burger Court went further still, delivering the coup de grace for constitutional privacy protections. In the sexual privacy cases leading up to Roe v. Wade, the Court waxed grandiloquent about "the sacred precincts of the marital bedroom." But the right to privacy in these cases turned out to be a confusing metaphor for a very different right to make personal decisions about procreation.

Meanwhile, in a series of less familiar criminal procedure cases, the Court dramatically expanded the power of the police to conduct intrusive searches and, in the process, threatened the ability of innocent people to control the disclosure of personal information in an age when so many of our intimate papers are stored outside the home.

These decisions were grounded on the legal test that Justice John Marshall Harlan proposed in the Katz case for determining what kind of surveillance activity should trigger the protections of the Fourth Amendment: a person must have an actual or subjective expectation of privacy, Harlan suggested, and the expectation must be one that society is prepared to accept as reasonable.

Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular. People's subjective expectations of privacy tend to reflect the amount of privacy they subjectively experience; and as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections. In a series of related rulings, the Court held that if you share information with someone else, you relinquish all "reasonable expectation of privacy" that the information will remain confidential. In the 1971 case that made it possible for Kenneth Starr to wire Linda Tripp, four justices said that a government informer carrying a radio transmitter could secretly broadcast his conversation with a suspected drug dealer to an agent waiting in a nearby room, because all of us, when we confide in our friends, assume the risk that our friends may betray us. And, in the cases that laid the groundwork for Kenneth Starr's subpoenas of Monica Lewinsky's book store receipts, the Burger Court decided, in the nineteen seventies, that we have no expectation of privacy in information such as bank records and telephone logs that we voluntarily mm over to a third party. The Court insisted, again, that when we share information with other people, all of us assume the risk that those people may disclose the information to the government.

In cases involving e-mail and other private papers stored on third party networks outside the home, the consequences of Harlan's test have been even more draconian. The Court has created an incentive for public employers to search and monitor the most private areas of the workplace - including Internet browsing and computer files stored on hard drives - as regularly as possible, in order to decrease their employees' expectation of privacy. The caselaw suggests that merely by adopting a written policy that warns employees that their e-mail may be monitored and restricted, employers will lower expectations of privacy in a way that gives them even broader discretion to monitor and restrict their employees' e-mail.

If employers were only permitted to monitor their employees' e-mail after clearly warning the employees in advance to expect monitoring, then the surveillance might be tolerated as an intrusive but freely accepted condition of employment. Unfortunately, judges today have adopted something like the opposite rule: even when employers promise to respect the privacy of e-mail, courts are upholding their fight to break their promises without warning. In cases involving e-mail sent from work, courts are increasingly holding that employees have very little expectation of privacy, mostly because of the tautological "expectation of privacy" test. As long as network administrators have the technical ability to read their employees' e-mail, employees should have no reasonable expectation that their e-mails aren't being read. In 1996, for example, police off-leers from Reno objected that their Fourth Amendment rights were violated when email messages they had sent over the department's internal message system were retrieved from a central computer. A court rejected their claim, quoting a commentator who noted that "an employee's privacy interest in E-mail messages"

would likely "fail the 'expectation of privacy' test since most users probably realize that a system administrator could have access to their Email."/2

But the fact that e-mail can be physically intercepted doesn't mean that it should be treated, for legal purposes, as if it were a postcard. In colonial America, letters from Europe were left at local taverns by ship captains, open for public inspection until they were claimed. And at the end of the eighteenth century, around the time of the Framing of the American Constitution, the mail was so insecure that Postmaster-General Benjamin Franklin and, later, Thomas Jefferson, thought that their own mail was being opened. (Indeed, Jefferson invented an extraordinary early encryption machine to address this problem.) To alleviate similar concerns, Congress in 1825 passed the Postal Act, which prohibited prying into other people's mail./3 And in 1878, the Supreme Court held that government needed a search warrant to open first class mail, regardless of whether it was sent from the office or from home. Instead of being passive in the face of technological determinism, we should demand similar privacy for e-mail.

The Court's reasoning - that a person who confides in someone else, or turns over information to a third party, abandons all expectations of privacy in intimate information - is simplistic at best: in the bank records case, the bank managers hadn't chosen to betray their confidences of their depositors. In fact, the government had ordered the bank to keep records of deposits and then forced the bank to disclose those records to a federal grand jury./4 If the Court meant what it said - "a person has no legitimate expectations of privacy in information he voluntarily turns over to third parties"/5 - then it would have to reconsider its holding in the wiretapping case, where it said that a person does have a legitimate expectation of privacy in information shared with a friend on the telephone. But the real problem with the Supreme Court's test for invasions of privacy is not empirical but conceptual. In many cases, people have an objectively valid expectation of privacy that the Court, by judicial fiat, has deemed unjustifiable.

In an important dissent in the bank records case, Justice Thurgood Marshall noted that constitutional protections for privacy shouldn't mm on subjective expectations, which necessarily diminish as technologies of surveillance permit the state to invade privacy in more efficient, but less detectable, ways: "Whether privacy expectations are legitimate," Marshall wrote, "depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."/6 A vision of privacy that took seriously the text of the Fourth Amendment might emphasize that there is an irreducible core of constitutional protection against unreasonable searches and seizures of persons, houses, electronic papers and effects that is necessary for freedom, regardless of how much or how little privacy people subjectively expect in these areas in the light of changing technologies of surveillance./7

When it comes to physical strip searches, courts today have no difficulty recognizing that invasions of privacy that might be reasonable in the investigation of serious crimes can be unreasonable in the investigation of less serious crimes. From 1952 until 1979, for example, police in Chicago routinely strip-searched female prisoners whom they arrested for minor traffic violations./8 Happily, times change: by 1986, the U.S. Court of Appeals in New York had no hesitation in concluding that it was unconstitutional for the police to subject a woman to a strip search after they arrested her for the misdemeanor of filing a false crime report./9 But when confronted with mental strip searches, judges have relinquished the tools to distinguish between violent crimes and thought crimes. The law no longer encourages them, as it should, to balance the intrusiveness of the search against the seriousness of the offense.

To restore this balancing test, Congress might consider listing the crimes that are serious enough to justify the search of private papers and e-mail, although congressional lists are hardly insulated from political pressure. In 1968, for example, Congress recognized that wiretapping posed such a serious threat to privacy that it could only be justified for especially serious crimes, such as espionage, treason, and crimes of violence. But although wiretapping was authorized for only 26 crimes in 1968, there were 95 crimes on the list in 1996. In that year, 71% of all the wiretaps authorized involved drug cases rather than crimes against the state./10

Another alternative might be for Congress to create new legal institutions for protecting privacy. Perhaps special grand juries could be empaneled to evaluate the reasonableness of subpoenas and warrants, balancing the intrusiveness of the search against the seriousness of the crime Subpoenas are ordinarily considered less threatening to privacy than warrants, because they allow the recipient to surrender the specified items, rather than permitting an officer of the state to rummage freely through a home or office. But a broad subpoena that allows prosecutors to retrieve all the data on a suspect's hard drive looks uncomfortably like a general warrant, which authorizes an unconstrained fishing expedition without specifying the areas to be searched or the things to be seized. The fact that private information on computers is extremely hard to delete - in her grand jury testimony, Monica Lewinsky confessed that she had tried unsuccessfully to erase her private e-mails at home, without realizing that prosecutors could retrieve them - makes the threat to privacy in cases involving computer searches all the more acute.

Arguably, the courts could require some kind of filtering mechanism to prevent prosecutors from riffling through a great deal of innocent documents in search of potentially incriminating ones, even with a warrant or subpoena. Rather than allowing Kenneth Starr to scrutinize Lewinsky's computers, for example, Judge Norma Holloway Johnson could have insisted on reviewing the files herself, and disclosed to the prosecutors only material that was clearly relevant to their investigation and didn't unreasonably threaten Lewinsky's privacy. Or, if Judge Johnson didn't feel that she had the time to undertake such an extensive review, she could have appointed a special privacy master to play the role that Bob Packwood had asked Congress to assign to Kenneth Starr during the investigation of Packwood's diaries, sifting through the hard drive and separating relevant from irrelevant material.

In civil cases involving the seizure of computer hard drives, in which innocent and potentially incriminating documents are hopelessly intermingled, some courts have suggested that the officers should hold the computers until a magistrate specifies the conditions under which they may be searched./11 When large quantities of information are seized, these courts have suggested, the officers should apply for a second warrant, to ensure that the search will be focused only on relevant documents./12 By ensuring that a neutral magistrate carefully monitors the scope of computer searches, this approach avoids the dangers of general rummaging through private papers that the Framers of the Fourth Amendment were determined to prohibit. Similar filtering mechanisms might be extended to more general searches of private papers stored in cyberspace.

As for particular statutes, I gather that my fellow witnesses will discuss the possibilities of adopting general privacy protections, along the lines of the European Union, which holds that information gathered for one purpose shall not be disclosed for another without the consent of the individual concerned. I know that there is strong opposition to such a law, especially from ecommerce interests, and that it faces an uphill battle. But I would like to close by suggesting that law may not be the most effective way of restoring in the age of the Internet the same privacy protections that citizens took for granted in the eighteenth century. Forms of technological selfhelp: including self-deleting e-mall, providers of anonymous browsing, and technology to erase postings in chat room, may be more effective than broad Congressional statutes.

There is no single solution to the erosion of privacy in cyberspace: no single law that can be passed or single technology that can be invented to restore Fourth Amendment protections in cyberspace. The battle for privacy must be fought on many fronts -- legal, political, and technological -- and each new assault must be vigilantly resisted as it occurs. There is nothing inevitable about the erosion of privacy in cyberspace, just as there is nothing inevitable about its reconstruction. We have the ability to rebuild some of the private spaces we have lost. But do we have the will?NOTES

FOOTNOTES:

1. Boyd v. United States, 116 U.S. 616, 630-32, 6 S.Ct. 524, 532-33, 29 L.Ed. 746 (1886).

2. Bohach v. Reno, 932 F. Supp. 1232,1234 & n.2 (1996) (quoting Laurie Thomas Lee, Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop", 28 J. MARSHALL L. REV. 139, 148 (1994).

3. Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (Cambridge, MA: MIT Press, 1998), pp. 128-29.

4. Albert W. Alschuler, Interpersonal Privacy and the Fourth Amendment, 4 N. ILL. L. REv. 1, 24 (1983).

5. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (emphasis removed).

6. Id. at 750. See also United States v. Miller, 425 U.S. 435,455 (1976) (Marshall, J., dissenting) (citing California Bankers Assn. v. Shultz, 416 U.S. 21, 96 (1974) (Marshall, J., dissenting)).

7. See Alschuler, supra note 17, at 6-8 & n. 12. Alschuler stresses that when the government intrudes on property interests in persons, houses, papers, and effects, with or without physical trespass, judges shouldn't have to inquire into cultural expectations of privacy. They should only speculate about cultural expectations, he argues, when evaluating invasions of privacy that take place outside this property- based Fourth Amendment core.

8. DAVID BRINN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 69 (1998).

9. In a desperate effort to get the police to respond to an attack on her son, the woman told a dispatcher he had been shot rather than beaten. See Weber v. Dell., 804 F.2d 796, 798-99 (2d Cir. 1986).

10. See, e.g., James X. Dempsy, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 ALB. L.J. ScI.& TECH. 65, 75 (1997).

11. Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 HARV. J.L. & TECH. 75, 105-106 (1994) (citing United States v. Tamura, 694 F.2d 591,595-96 (9th Cir. 1982)) (discussing the Intermingled Records Doctrine in the Tamura and Steve Jackson Games cases). See also United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987).

12. Winick, supra note 15, at 107.

END

LANGUAGE: ENGLISH

LOAD-DATE: April 7, 2000

View: Cite | KWIC | **Full** | Custom PREVIOUS 41 of 51 NEXT Text Only | Download | Fax | Email
FOCUS™ - Narrow Results | Save As ECLIPSE | More Like This | More Like Selected Text

Source: All Sources : / . . . / : **News Group File, All**
Terms: **unwanted gaze** (Edit Search)
View: Full
Date/Time: Wednesday, July 5, 2000 - 4:23 PM EDT

Search | Search Advisor | Get a Document | Check a Citation
ECLIPSE(TM) | History | Change Client | Options | Feedback | Sign Off | Help
About LEXIS-NEXIS | Terms and Conditions

Los Angeles Times

View Related Topics

June 27, 2000, Tuesday, Home Edition

SECTION: Part A; Part 1; Page 1; Financial Desk

LENGTH: 1324 words

HEADLINE: GENOME MILESTONE: CRACKING THE CODE;
DECODING RAISES A DOUBLE-EDGED SWORD ON ETHICS

BYLINE: MARLENE CIMONS, TIMES STAFF WRITER

DATELINE: WASHINGTON

BODY:

The first draft of the entire human genome ultimately will bring a wealth of scientific knowledge about ourselves. But it could also bring a heap of trouble.

Controversial advances that push society to the edge of the scientific frontier frequently pose ethical dilemmas before public policy has had a chance to address them, bioethicists say.

In the case of public and private scientists' announcement Monday that they had compiled all the genetic pieces of a human being, the complex and sobering ramifications will be impossible to ignore.

"It is an amazing scientific accomplishment," said Art Caplan, director of the University of Pennsylvania bioethics center. "But, sadly, the potential value of this monumental achievement may be delayed or even lost if we do not move public policy and the law forward to respond to what science has achieved."

Repeatedly Monday, even in the blush of triumph, world leaders--and indeed the scientists themselves--raised the potential for abuse and urged that society and decision makers wrestle with these issues before it is too late.

"As we consider how to use new discovery, we must also not retreat from our oldest and most cherished human values," President Clinton said during a White House ceremony celebrating the achievement. "We must ensure that new genome science and its benefits will be directed toward making life better for all citizens of the world, never just a privileged few."

Clinton also warned about privacy violations and discrimination. "Increasing knowledge of the human genome must never change the basic belief on which our ethics, our government, our society are founded. All of us are created equal, entitled to equal treatment under the law."

British Prime Minister Tony Blair, trumpeting his own country's role in the research, emphasized the responsibility to use it wisely.

"We cannot resist change," Blair said, "but our job--indeed, our duty--is to make sense of change, to help

people through it, to seize the massive opportunities for better health and a better quality of life and then, with equal vigor, to minimize the threats such developments pose."

The impact of the choices that society finally makes--or fails to make--will be felt in a broad range of arenas: **medical privacy,** employment, advertising and even reproduction.

Some of the implications still sound like the stuff of science fiction. In this category is the specter of designer babies: What is to stop potential parents from inserting selected genes into embryos to make a "perfect" child?

"Many people would be repulsed by the idea of optimizing embryos to have tall, handsome, thin, athletic, intelligent babies who will be able to predict the stock market," said Mildred Cho, senior research scholar at Stanford University's Center for Biomedical Ethics. "But it's a private matter. And that would be hard to regulate."

More immediate are threats of genetic discrimination and invasion of genetic privacy. "There is nothing to stop those who have tissue samples or biological materials stored from going out and looking at them to see what they can learn" about the donors, Caplan said.

Even the dead are vulnerable. Although they have no legal rights, Caplan said, "their relatives and descendants have interests. There may be personal or sensitive information that they do not want revealed, such as that they were adopted, that they were born out of wedlock, that they have an unknown African American grandparent, that they are prone to depression."

Advertisers and marketers would almost certainly be tempted to bombard consumers with promotions seeking to exploit their inevitable fears about their own genetic secrets.

"The possibility of creating anxiety and panic is not hypothetical," Caplan said. "Are you Irish, Native American, Latvian or Korean, or do you have an ancestor who lived in Central Africa or northern Iran? Then you need to be screened to see if you are at risk of cystic fibrosis, cancer, hives, depression or muscular dystrophy."

Many worry that new genetic information will be used by insurers to discriminate, making coverage inaccessible to those who need it the most. But some experts point out that having this information could instead prompt an overhaul of the industry to redesign the very way in which it assigns risk.

"The current premise is that you don't know what kind of risk you bring to the pool," said Erik Perens of Hastings Center, a research organization in Garrison, N.Y., that specializes in ethics. "This new information will take us down the road toward knowing in advance what risk we bring. So it explodes the concept of risk-based insurance."

Cho, the Stanford ethicist, points out that genes that are close together on their chromosomes tend to be inherited together.

"What if we find out that the gene for melanoma or colon cancer is right next to the gene for red hair?" she said. "It could be that they are linked together genetically and tend to travel together."

And that, she said, could influence the impression that people make: "You see someone with red hair and you think, 'Hmmmmm.' "

On its most cosmic level, the debate raised by this stunning accomplishment could transform the way in which individuals shape their very lives.

Is genetics destiny? Will who we are--and all we are to be--ultimately be seen as based solely on billions of bits of DNA instead of on free will--our power to choose?

"In this country, we have been committed to the notion that what you do and who you become has a lot to do with the goals you set for yourself and the way you behave," said Alex Capron, professor of law and medicine at USC. But in the new age of genetics, he said, this could be replaced by the concept that our fate "instead is sealed at the moment of fertilization."

"It seems so neat, so clean, so seductive--and so false," said Capron, who fears that "the full manifestation of ourselves as human, psychological organisms, living in a complex environment, with so many aspects of ourselves that arise from interactions," will be lost, "reducing us to a string of DNA."

Celera Genomics President J. Craig Venter, who shared in the achievement, said at the White House ceremony Monday that this psychic transformation is unlikely.

"The complexities and wonder of how the inanimate chemicals that are our genetic code give rise to the imponderables of the human spirit should keep poets and philosophers inspired for the millenniums," Venter said.

Some genetic anthropologists also have raised the intriguing possibility that racial and ethnic distinctions, now largely based on superficial physical characteristics, will dissolve once society realizes the genetic similarities and differences within and between groups.

"We could find that we are much more related to each other than we think we are, and that there is much more variation within a group that is socially defined--like Asians or African Americans--than between the groups," Cho said. "How will people react to that? I'm not sure."

Decision makers will have to grapple with how best to handle what ultimately is revealed--the good, the bad and the ugly. And the time to do so has now become short.

"There is every reason to celebrate the triumph of humanity deciphering the component parts of its own biological programming," Caplan said. "But if we are going to enjoy the medical and public health benefits that this work can bring, we must get moving quickly to build ethical and legal protections that will ensure that this knowledge will be put to good use."

*

More on Genome

* A BEGINNING--Devising actual cures based on the human genome will involve years of research. A12

* THE ENTREPRENEUR--Celera Genomics' J. Craig Venter has both his fans and his detractors. A12

* TEAM LEADER--The head of the public genome project is a man of contradictions, determination. A12

Milwaukee Journal Sentinel

June 16, 2000 Friday FINAL EDITION

SECTION: NEWS; Pg. 19A

LENGTH: 682 words

HEADLINE: Will government stamp out cybersnoops?

BYLINE: WILLIAM SAFIRE The New York Times

BODY:

Because Al Gore stands an even chance of becoming our next president, I thought it would be a good idea to nail down his position on a sleeper issue in this campaign: the abuse of computer technology to invade personal privacy.

The opportunity arose to put the privacy question to the vice president this week at an on-the-record session with New York Times editors in New York.

To show that entrapment with a trick question on a complex issue was not my intent, I prefaced my query with a brief explanation of the two key words used by both sides in the controversy.

The word "choice" is used by banks, hospitals and Internet companies to conceal their intrusions into the personal lives of their customers. They offer us a "choice" to tell them not to share our most intimate secrets with others -- but the burden of that decision is on the customer, who can be manipulated by a bribe of a gift or a threat of refusal of business. The intruders know that most people can't be bothered to choose to "opt out" -- to take the initiative to defend themselves.

The word "consent" is used by those opposed to the placement of " cookies" (spying bugs to track your every online movement) in your computer. We want to place the burden of seeking your express, informed consent on the marketers; this means you must first be made aware of who will get what information about you and be told explicitly whether it will be sold or given to some other company or division for a different purpose. Only if you affirmatively "opt in" -- give your permission -- can they then track your tastes and habits.

The difference is day and night. "Choice" is the misleading word used to cover a phony pass at a privacy policy, which retailers, insurers and banks are now touting, while consent is your valuable power to say "yes" that they are desperate to deny customers. In the sellout engineered last year by the Clinton Treasury secretary, Larry Summers, and the GOP Senate Banking chairman, Phil Gramm, the banking lobby won; your consent is not required.

So, Mr. Vice President, how come you spoke of providing choice in your speech about privacy? Would you support legislation requiring companies to first obtain the consumer's consent?

"Along with 270 million other Americans," he replied, "I use words more carelessly than Bill Safire. And in choosing the word 'choose,' I did not inform myself of the deeper, more subtle meanings -- which I now see clearly."

Then Gore got serious: "I don't think an unfair burden should be placed on the users of the Internet to affirmatively go out and protect their own privacy." He added: "I think there should be procedures commonly accepted which protect them more or less automatically unless (the Internet users) take affirmative steps to surrender their privacy."

That spells consent, but I pressed him on legislation to protect financial privacy, where his administration has been weak.

"I can tell you what the ideas are that I believe in," he said. "I think that we should have absolute protection of financial privacy as well as **medical privacy.** I do not think that your bank account and the history of what checks you write, and to whom, ought to be marketable."

Gore warmed to the subject: "I think that people ought to have a right to expect that will remain private unless they affirmatively give up that right for whatever reason. And I don't think the current law goes far enough in protecting them. Does that answer your question?"

Sure does. He also touched my button with " It should be illegal to trade in Social Security numbers. That's the single key fact that is most useful in compiling dossiers."

At that very moment, Sen. John McCain was holding Commerce Committee hearings to expose "online profiling," the turning of Net users into ripe selling targets. Industry snoops are suddenly promising self-policing -- anything to avoid asking consent.

Gore's stand on the right to privacy is forceful. Next is for one of us to pin down George W. Bush.

William Safire is a columnist for The New York Times.

LOAD-DATE: June 16, 2000

The Plain Dealer

June 16, 2000 Friday, FINAL / ALL

SECTION: EDITORIALS & FORUM; Pg. 9B

LENGTH: 669 words

GORE'S STAND ON PRIVACY

BYLINE: By William Safire

BODY:

Because Al Gore stands an even chance of becoming our next president, I thought it would be a good idea to nail down his position on a sleeper issue in this campaign: the abuse of computer technology to invade personal privacy.

The opportunity arose to put the privacy question to the vice president this week at an on-the-record session with New York Times editors in New York.

To show that entrapment with a trick question on a complex issue was not my intent, I prefaced my query with a brief explanation of the two key words used by both sides in the controversy.

The word "choice" is used by banks, hospitals and Internet companies to conceal their intrusions into the personal lives of their customers. They offer us a "choice" to tell them not to share our most intimate secrets with others - but the burden of that decision is on the customer, who can be manipulated by a bribe of a gift or a threat of refusal of business. The intruders know that most people can't be bothered to choose to "opt out" - to take the initiative to defend themselves.

The word "consent" is used by those opposed to the placement of "cookies" (spying bugs to track your every online movement) in your computer. We want to place the burden of seeking your express, informed consent on the marketers. This means you must first be made aware of who will get what information about you, and be told explicitly whether it will be sold or given to some other company or division for a different purpose. Only if you affirmatively "opt in" - give your permission - can they then track your tastes and habits.

The difference is day and night. Choice is the misleading word used to cover a phony pass at a privacy policy, which retailers, insurers and banks are now touting, while consent is your valuable power to say "yes" that they are desperate to deny customers.

In the sellout engineered last year by the Clinton Treasury secretary, Larry Summers, and the GOP Senate Banking chairman, Phil Gramm, the banking lobby won: Your consent is not required.

So, Mr. Vice President, how come you spoke of providing choice in your speech about privacy? Would you support legislation requiring companies to first obtain the consumer's consent?

"Along with 270 million other Americans," he replied, "I use words more carelessly than Bill Safire. And in choosing the word choose,' I did not inform myself of the deeper, more subtle meanings - which I now see clearly."

Then Gore got serious: "I don't think an unfair burden should be placed on the users of the Internet to affirmatively go out and protect their own privacy." He added: "I think there should be procedures commonly accepted, which protect them more or less automatically unless they (the Internet users) take affirmative steps to surrender their privacy."

That spells consent, but I pressed him on legislation to protect financial privacy, where his administration has been weak.

"I can tell you what the ideas are that I believe in," he said. "I think that we should have absolute protection of financial privacy as well as **medical privacy.** I do not think that your bank account and the history of what checks you write, and to whom, ought to be marketable."

Gore warmed to the subject: "I think that people ought to have a right to expect that will remain private unless they affirmatively give up that right for whatever reason. And I don't think the current law goes far enough in protecting them. Does that answer your question?"

Sure does. He also touched my button with "It should be illegal to trade in Social Security numbers. That's the single key fact that is most useful in compiling dossiers."

At that very moment, Sen. John McCain was holding Commerce Committee hearings to expose "online profiling," the turning of Net users into ripe selling targets. Industry snoops are suddenly promising self-policing - anything to avoid asking consent.

Gore's stand on the right to privacy is forceful. Next is for one of us to pin down George W. Bush.

LANGUAGE: ENGLISH

LOAD-DATE: June 17, 2000

MAY 15, 2000

SECTION: Vol. 18, No. 20; Pg. 7; ISSN: 87502100

B&H-ACC-NO: 54043739

DOC-REF-NO: MAHT-2174-9

LENGTH: 687 words

HEADLINE: Baltimore uses CyberTrust for a **medical privacy** program

BODY:

Baltimore Technologies, an Irish company that acquired GTE's Needham CyberTrust Solutions business earlier this year, will provide electronic security software to four Bay State health care companies in an innovative privacy pilot program.

Officials at Baltimore's new local division said last week it has been selected by the Massachusetts Health Data Consortium (MHDC) as the source of digital certificates used to ensure medical data e-mailed between health care providers and insurers is secure.

Internet transmission is expected to help reduce the cost and increase the efficiency of shuffling medical paperwork like claim forms, said Dean Coclin, business development manager for Baltimore. Health care organizations, however, have been leery of e-mail and other Web-based products since data can be intercepted and viewed by unauthorized parties. What's more, hospitals and payers will soon face federal guidelines that require them to protect patient information.

"HHS (the U.S. Health and Human Services department) said it expects the regulations to be final before the end of the calendar year," MHDC Executive Director Elliot Stone said. "Then, once the final regulations are issued, companies have 26 months to comply."

At issue is the transfer of medical data that includes a patient's identity, whether it is a name, a social security number or other so-called "individually identifiable" information. According to planned federal guidelines, organizations transmitting this sort of medical data over public networks, like the Internet, will be required make sure it is protected from unauthorized viewers.

The MHDC is gearing up for the impending regulations with a pilot program involving four member companies: Blue Cross Blue Shield of Massachusetts, Tufts Health Plan, Children's Hospital and Care Group Inc. To meet data security requirements it has enlisted Baltimore, which through the CyberTrust purchase provides Public Key Infrastructure (PKI) software. The PKI technology is designed to issue, renew, revoke and otherwise manage digital certificates - electronic IDs that vouch for the identity of an individual or company.

'We feel that PKI is a technology that is mature enough to handle the security needs facing health care companies," Coclin said. "Most people are drawing that conclusion."

Baltimore already has large clients like MasterCard and American Express that use its digital certificate technology The Bay State pilot program is one of its first forays into the health care sector, and company executives believe it is a sector ripe for PKI technology.

"Right now we are just seeing the consortium idea of groups banding together in the health care area to think about security, largely because the legislation is looming," said public relations manager Mike Yaffe.

Between 20 to 25 people inside each of the pilot organizations will receive digital certificates allowing them to transmit and receive data. Stone said the program will focus on low-volume transactions like claims questions and consumer service information.

"The idea is simply to replace the normal non-secure communications with secure ones," Stone said. "Right now it may be talking over the phone or sending faxes with individually identifiable information. The pilot aims to tighten that all up."

Once the pilot is over, the MHDC will evaluate the program and use the results to educate its other member companies on the use of PKIs and digital certificates. Coclin said Baltimore hopes being involved early will mean big exposure among MHDC members and the chance to expand its client base in the health care community.

"It is already getting talked about at their meetings, conferences and in the newsletter," he said.

Baltimore Technologies is a network security firm headquartered in Dublin, Ireland. Its local office, based in Needham, was formed by Baltimore's purchase in March of GTE's CyberTrust in a stock deal worth $150 million. CyberTrust developed PKI software.

According to Jaffe, the company has 700 employees worldwide, including roughly 200 in its Needham office.

LANGUAGE: ENGLISH

LOAD-DATE: June 23, 2000

Los Angeles Times

View Related Topics

May 15, 2000, Monday, Home Edition

SECTION: Health; Part S; Page 1; View Desk

LENGTH: 1441 words

HEADLINE: ER DOCTORS OFTEN FACE A SHORTAGE--OF PATIENT INFO; TECHNOLOGY: NEARLY INSTANT ACCESS TO **MEDICAL** HISTORIES IS SOUGHT. BUT **PRIVACY** CONCERNS HAVE SLOWED THE PROCESS.

BYLINE: JANE E. ALLEN, TIMES HEALTH WRITER

BODY:

The hunt for important medical and personal information was well underway by the time paramedics wheeled the semiconscious 78-year-old construction worker into the emergency room. They already had logged his vital signs, learned his name and assessed injuries he suffered in a 10-foot fall from a ladder.

The patient was unable "to tell us where he hurt or any subtleties of his mental status," said Dr. Edward Newton, co-director of the emergency room at Los Angeles County-USC Medical Center's General Hospital.

So the doctors and nurses did what they usually do when patients arrive in the ER with no medical history and unable to communicate: They flew blind, relying on standard procedures and experience.

Expressing some reluctance with his own analogy, Newton likened the task of evaluating a patient who can't tell doctors what's wrong to "a veterinary exam."

On this particular night, they studied a gash on the patient's head and looked for indications of a broken neck or back. Under a spotlight's eerie bluish glow, technicians performed X-rays that could reveal damage or why he fell.

Having medical information in hand is often a luxury in hospital emergency rooms. This is especially true at inner-city hospitals such as County-USC, which treat large numbers of uninsured, working poor and transients, who may lack regular medical attention. Yet such information could speed the doctors' job--or possibly save a life by averting drug reactions or other complications.

For example, if doctors knew a patient with chest pain was severely allergic to aspirin, a standard treatment, they might choose a substitute and save the time involved in reversing a potentially deadly reaction. If they knew a patient with an inflammatory disease such as colitis was taking steroids, they could avoid medicines that further compromise the body's fight-or-flight system, Newton said.

Both private industry and the medical profession have begun some small-scale efforts to address the problem.

And a handful of doctors and hospitals are encouraging patients to carry at least a bare-bones health record and an emergency contact, even if it's scribbled on a scrap of paper.

"As an emergency physician, if I can get anything with a patient's history on it--an old chart, a write-up from a board-and-care, or a medical information access card, I am already five minutes ahead of the game," said Dr. Robert Realmuto, medical director of Orange Coast Memorial Medical Center in Fountain Valley, which provides a plastic card with medical history, emergency contacts and insurance eligibility free to the community.

The American College of Emergency Physicians supports medical information cards and wants parents of special-needs children to keep medical histories at school and on the refrigerator where baby-sitters and others can grab them. If doctors knew a child with breathing trouble had an underlying heart condition, they might avoid antihistamines that make the heart race, said M.J. Fingland, a spokeswoman for the organization.

Without a medical card or other information, hospital workers scramble to gather what they can about a patient. If paramedics haven't yet searched the patient's clothing and wallet, social workers or ER staff may track down next of kin. They'll check hospital records. They may ask law enforcement to visit the neighborhood where the person was found, in hopes of locating a friend or neighbor.

For sure, an engraved medical alert bracelet--hard to miss during the physical examination, can reveal drug allergies or conditions such as epilepsy or diabetes that might explain a coma or seizure. The bracelet links emergency health workers to a phone number they can call to get more information on the wearer. But fewer than 5% of people passing through County-USC Medical Center's emergency rooms wear one, says Dr. Gail V. Anderson Sr., emergency department chairman.

Only the rare patient carries a wallet-sized card with medical information that might reveal dementia or other conditions that could explain the patient's difficulties communicating.

As Anderson and others say, you can't make people tattoo the information on their foreheads. Requiring that everyone's medical records go into a large database raises privacy concerns. High-tech solutions that link personal medical histories to the Internet or scannable cards that reveal sensitive data could compromise careers or insurance if the information fell into the wrong hands.

"Everybody is worried about Big Brother," said Dr. Gail V. Anderson Jr., medical director of Harbor-UCLA Medical Center in Torrance and the son of County-USC's Anderson. A spokesman for the emergency physicians' college, he thinks the group needs to push voluntary ways of providing access to medical history, such as bracelets and medical information cards, until privacy issues can be addressed.

Advocates of high-tech databases say a good information system could make emergency health care more efficient and eliminate redundancies in the often overburdened health care system. Dr. Marie Russell, an ER attending physician at County-USC, favors a card in which doctors could quickly learn what medical tests patients have had and their results: "Has somebody had a stress test before? Do they have coronary disease?"

A few organizations have fledgling efforts to provide such information. Precis Smart Card Systems of Oklahama City is test-marketing a wallet-size card in which the patient's medical record is embedded on a microchip. The product, called the Instacare Emergency Card, must be read with a portable hand-held device. And the Medic-Alert Foundation, a Turlock, Calif.-based nonprofit group that provides identification bracelets and pendants for people with serious allergies and medical conditions, is

collaborating with San Diego-based Humetrix.com on an electronic card that would allow doctors to obtain members' medical records through the Internet.

Meanwhile, some hospitals and doctors are encouraging the simpler solutions, such as alert bracelets or printed cards. But even those methods require verification. Some drug abusers obtain diabetic alert bracelets to try to fool police in case they are ever detained, said Dr. Chris Johnson, a resident at County-USC.

Nearly 100,000 patients who live in Los Angeles and Orange County communities now are carrying medical information cards provided by Memorial Health Services, a Fountain Valley-based health care company that operates five hospitals in the region, including Long Beach Memorial and Orange Coast Memorial Medical Center.

The wallet-size cards are printed with basic personal and medical information and also have a magnetic strip that can be swiped to show information about the patient's medical insurance and medical history--data that the person has provided voluntarily.

A Beverly Hills cardiologist has taken that idea a step further by including a miniaturized tracing of a patient's electrocardiogram on a wallet-sized card. If a heart patient is treated by an unfamiliar doctor, the card provides a critical piece of information.

"The EKG can show, for example, that a patient with atypical chest pain isn't having a heart attack because it provides a baseline for what's normal in that patient," said Dr. Yzhar Charuzi.

The card contains the name of the patient's doctors, along with allergies, other medical conditions and a list of past medical tests and procedures. Charuzi, who charges patients $ 20 to cover the cost of the cards, said one of them recently came in handy for a patient who became seriously ill during a trip to Romania.

As the medical system sorts out long-term solutions for the sharing of medical information, his card-carrying patients are prepared. In a health crisis, he said, what matters is "whatever you have on the spot."

*

Residents of Los Angeles and Orange counties may order a free emergency information card from Memorial Health Services through its web site at http://www.memorialcare.org or by calling toll-free, (877) 446-4406, regardless of whether they use its hospitals.

* A free Medical I.D. Pocket Pal, as well as a blank personal medical history, consent-to-treat and emergency-information form for children with special health care needs, can be obtained by writing to the American College of Emergency Physicians at 1111 19th St. NW, Suite 650, Washington, DC, 20036, by calling (800) 320-0610, Ext. 3006, or by going to http://www.acep.org.

* To obtain MedicAlert tags, contact the MedicAlert Foundation at (800) 432-5378 or go to http://www.medicalert.org.

GRAPHIC: PHOTO: When patients aren't able to speak for themselves, hospital staff must scramble to find facts or the family members who might have them. PHOTOGRAPHER: GINA FERAZZI / Los

The Buffalo News

May 5, 2000, Friday, CITY EDITION

SECTION: BUSINESS, Pg. 6B-

LENGTH: 584 words

HEADLINE: LAFALCE BILL GIVES **PRIVACY** PROTECTION FOR FINANCIAL; **MEDICAL** RECORDS

BYLINE: DOUGLAS TURNER; News Washington Bureau Chief

DATELINE: WASHINGTON

BODY:

Warning the Democrats are "drawing a line in the sand" on consumer protection, Rep. John J. LaFalce on Thursday unveiled a White House-backed bill granting broad privacy protection on financial services and medical records.

The Tonawanda Democrat, joined by House Minority Leader Dick Gephardt, D-Mo., and Treasury Secretary Lawrence Summers, told a press conference his party will finish the job they said was blocked by congressional Republicans last year.

"When we passed the financial services deregulation act," LaFalce said, "the Democrats forced the issue on privacy and made a significant start."

During the voting on the omnibus banking bill, LaFalce charged, Republicans killed further reforms by casting party line votes in the House Banking Committee, in the House Rules Committee, and in the Senate-House conference last year.

LaFalce is the top Democrat on the committee, meaning that if the Democrats win the House this fall, he will be the likely chairman.

The Democrats new bill would require that any financial institution covered by federal law must get specific permission from any consumer before medical or other personal information could be distributed.

Their bill gives the government stronger enforcement powers, and allows consumers to comparison shop for services and privacy protection.

David Runkel, spokesman for Banking Chairman Jim Leach, R-Ind., said LaFalce's claim of party line votes by the committee on consumer protection was "not accurate." Runkel noted many Democrats joined the GOP in a committee vote to defeat a similar Democratic measure in 1999.

Republican Sen. Phil Gramm, R-Texas, said "Congress approved the most important protections of financial privacy in U.S. history."

Gramm, Senate banking chairman, said "the rules to put those protections in place are still being written by regulators. We need to give customers and their financial institutions time to absorb those new rules before we consider changing them."

In advance of the new regulations, some banks are sending customers documents outlining new privacy policies. However, many consumers have complained the mailings are complex and impossible to understand.

Democrats said they think consumer protection will be a big issue in their quest to regain the House majority.

"Every time I go home, I go door-to-door and people ask me about this," said Gephardt.

Rep. Edward Markey, D-Mass., insisted that the privacy issue "should animate the fall elections."

Summers said "we made an important start last year but . . . we did not go far enough."

LaFalce said "there is no valid reason our Republican colleagues cannot join us in a serious effort to" pass tougher protections. His Financial Privacy Act would give financial consumers a chance to "opt out" before one firm can share private data with anyone, even an affiliate under the same conglomerate umbrella.

Under last year's bill, this sharing is possible. LaFalce's bill requires that a consumer affirmatively consent before any financial firm could have access to medical information from a health insurance company. Also, the bill prohibits any financial firm lacking specific consent to share credit-card data about where a customer spends money and what they buy.

"It creates new rights for consumers to know what information a financial institution is collecting about them, and to correct or delete inaccurate information before making decisions permitting disclosure," LaFalce said.

LANGUAGE: ENGLISH

LOAD-DATE: May 16, 2000

FOCUS™
Search: General News;headline (Medic! and Privacy)

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

Milwaukee Journal Sentinel

April 30, 2000 Sunday FINAL EDITION

SECTION: NEWS; Pg. 05A

LENGTH: 592 words

HEADLINE: Financial **privacy** legislation promoted;
White House plan would restrict sharing of **medical,** personal spending data

BYLINE: STEPHEN LABATON New York Times

BODY:

Washington -- The Clinton administration is preparing legislation to protect the financial privacy of consumers by limiting how banks, insurers and other companies share sensitive consumer information such as personal spending habits, medical files and insurance records.

Administration officials said that President Clinton would describe the plan today at a commencement address at Eastern Michigan University in Ypsilanti and that it was strongly endorsed by Vice President Al Gore.

But the package has already been denounced by the financial services industry, which has chafed over less restrictive proposed regulations authorized by a banking law passed last year. It has also been criticized by leading Republicans in Congress who stripped some provisions similar to the new plan from last year's legislation.

Opponents of the new privacy legislation say it will cost companies too much and will discourage the consolidation of banks, insurers and securities firms, which the law passed last year was intended to promote through deregulation.

The White House proposal would prohibit affiliates of large financial conglomerates, say an insurance company and a bank, from sharing information such as medical records without a customer's consent when the customer applies for a loan.

It also would restrict the ability of banks to divulge the spending habits of their customers that may be gleaned from checking accounts, or credit or debit cards.

It would give consumers a new right to review their credit and financial information and correct errors. And it would force companies to provide consumers with special new privacy notices upon request, to enable them to shop for the most protective institutions.

"To further the Clinton-Gore commitment to protecting consumer privacy, the president is taking strong steps to enhance financial privacy protections," a senior administration official said. "The president believes that firms should not be able to share especially sensitive medical information, or information on personal spending habits, unless the consumer affirmatively consents."

While the plan's prospects for passage by Congress this year are dim, it appears certain to have deep resonance in the presidential campaign, particularly as public opinion polls show the issue to be of growing

importance to voters and consumers who are increasingly relying on both the Internet and on large financial conglomerates to do banking, buy consumer goods and trade stocks.

Gore and other leading Democrats have allied themselves with the plan. Gov. George W. Bush's aides said he had not articulated a position, although many senior Republicans in Congress and supporters of Bush have been equally vociferous against taking any further steps to increase the privacy protections of consumers because they say they are too burdensome for the financial services industry.

"It's very clear that this a political act and the president is playing to the traditional base of the party," said Kenneth Guenther, a lobbyist for the Independent Community Bankers Association, which represents many of the smaller banks and savings associations and opposes the new measure.

"This is going to be a humongous issue, particularly since there is nothing in the law that right now prevents companies such as the Travelers, a unit of Citigroup, from sharing medical records with Citibank. But the issue is not going to be resolved now, not with with this Congress, which at this late date is not going to touch this with a 10-foot pole."

LOAD-DATE: May 16, 2000

THE ARIZONA REPUBLIC

March 24, 2000 Friday, Final Chaser

SECTION: FRONT; Pg. A20

LENGTH: 938 words

HEADLINE: A PRESCRIPTION FOR **MEDICAL PRIVACY;**
NEW FEDERAL RULES WOULD LIMIT ACCESS TO ELECTRONIC RECORDS

BYLINE: By Julie Appleby, USA Today

BODY:

Most patients assume that what they tell their doctor is confidential.

But it might not be.

Blame the loss of privacy on the Internet or on the growing use of computer records. Blame it on cost-conscious managed care insurance companies that demand justification for treatment. Blame it on a desire to reduce medical errors.

Just don't assume that no one knows about your health except you and your doctor.

"In many respects, the battle for health privacy has already been lost," said Robert Gellman, a Washington, D.C., privacy consultant and member of the National Committee on Vital and Health Statistics.

"Of all the records about you that are maintained by third parties, health records are the most widely circulated, more than financial records, school records, even video rental records."

Although that's long been true, patient advocates now fear the growing use of computerized medical records compounds the loss of medical privacy.

"Once you put the medical record in a computer, it can wind up anywhere," said HMO industry critic Jamie Court of Consumers for Quality Care. "That's the direction we're going, and it's frightening, especially when you talk about genetic information."

The recent hacker attacks on such high-profile Internet sites as Yahoo! and Amazon.com highlight the concern: If hackers can disrupt major players in the e-commerce world, how safe is your doctor's Web site?

Properly encrypted and password protected, it might be safer than paper files left lying on a counter or in a storeroom, some advocates say. But sometimes things go wrong.

In February, for example, medical records of several thousand patients at the University of Michigan Medical Center were inadvertently placed on the Internet, where they sat for two months. A student doing an online search discovered the files, which included names, addresses, Social Security numbers and other data. The site was promptly shut down.

Even before medical records went online, patient information was anything but private. Some patients have learned that the hard way:

*An HIV-positive Pennsylvania man employed by a state transit agency sued in 1995 after the agency learned of his condition through a review of prescription drug records. A federal Appeals Court ruled against him. The court's decision said that because the employer paid for the drug plan, it had a right to see the information.

*An Atlanta truck driver lost his job in early 1998 after his employer learned from an insurance company that he had sought treatment for drinking problems.

*After a state review of a doctor in Kentucky, an investigator called one patient's employer - the FBI - to say the man was being treated for depression. As a result, the FBI took the employee's gun away and ordered him to undergo a two-day psychiatric exam, which found him fit for duty.

Researchers, public-health officials, police and others can get medical records. Apply for life insurance and your health problems might go on file at the Medical Information Bureau, an insurance industry clearinghouse with files on more than 15 million Americans and Canadians.

Insurers often demand detailed information from providers, including mental health counselors and doctors, in order to justify continued treatment.

"Managed care companies are requesting much more information than they need to make coverage decisions," including "comments about suicide attempts, extramarital affairs, job-related problems and drug or alcohol abuse," said Paul Appelbaum, vice president of the American Psychiatric Association.

Employers - the very group most patients fear will get their private information - are able to get medical information from insurers and others, said Janlori Goldman of the Health Privacy Project at Georgetown University.

"Employers may say, 'You just doubled our premium, what's going on?' There's no federal law that prevents the insurer from giving that information to employers," she said.

The first federal standards aimed at guarding electronic medical records are now under review by the Department of Health and Human Services, which received more than 40,000 comments on the draft proposal. The proposed privacy safeguards don't cover paper records.

If upheld as written, the standards would reduce access by employers, allow patients to get copies of their own records and require permission from patients in certain circumstances to release information.

No consent, however, would be needed to release information related to medical treatment, payment or health care operations, such as auditing, checking credentials of staff or quality assurance work. (Patients often give consent to release information, sometimes unknowingly, whenever they sign up for health insurance or fill out forms at doctors' offices).

Some patient advocates say the standards don't do enough to prevent abuses, while insurers fear the proposed standards are too costly and burdensome. Congress could pass broader legislation, but so far has not done so.

'Right now, once information leaves a doctor's office, there are no federal regulations that protect the

privacy of that information," said Goldman of Georgetown University.

Medical information routinely leaves doctors' offices: After a patient sees a doctor or fills a prescription, claims are sent to insurers and third-party bill collectors.

In turn, that information is sometimes given to drug companies or marketers. Insurers can mine prescription data, looking for patients with chronic health conditions such as asthma, diabetes or heart failure to enroll them in special programs.

LANGUAGE: ENGLISH

LOAD-DATE: March 25, 2000

THE ORLANDO SENTINEL

February 6, 2000 Sunday, METRO

SECTION: INSIGHT; Pg. G1

LENGTH: 1276 words

HEADLINE: MEDICAL PRIVACY QUESTIONS ABOUND

BYLINE: By Michael Freeny, Special to the Sentinel

BODY:

There are some interesting questions buzzing throughout Washington regarding the privacy of your medical records.

For example:

Should the police be able to snoop through your private medical records without your knowledge, consent or even a search warrant?

Should insurance companies have expanded powers to use, transmit, share or profit from your medical records as long as the data is used for treatment, payment or "health-care operations"?

Should your employer have access to your medical records to monitor employee-subsidized health care.

Should the federal government give itself the right to obtain your medical records without your consent or knowledge?

These and other important questions are provisionally answered by the Department of Health and Human Services draft regulations that propose revolutionary rules to govern use of electronic medical records.

The need for such rules is long overdue. Medical information is now routinely stored, transmitted and retrieved by computers. The traditional paper chart is fading into history as databases of symptoms, treatments, payments, procedures and authorizations create the "virtual chart."

Unlike a unwieldy paper chart, which can only be at one place at a time, the Electronic Patient Record can be everywhere, viewed simultaneously by providers and insurers in different states.

Today there is simply no way to deliver efficient, precise and timely medical care without computers.

However, the convenience of instant access to a patient's medical data must be balanced against the traditional right to privacy, consent and protection.

Your trust of the confidentiality in a health-care setting may dramatically affect your willingness to tell the truth about sensitive subjects, such as substance abuse, sexual diseases, depression or marital problems.

Historically, such information was held in private confidence between doctor, patient and medical chart. Today, sensitive information and even clinical photographs are routinely shared with many health-care

players, increasingly via the Internet.

In the past, medical-records privacy has been a matter of state regulation. However, there is currently little consistency from one state to another. With so many national health-maintenance organizations managing patient care, the need for national standards has become urgent.

Richard Coorsh, vice president of the Health Insurance Association of America, said that his group supports the federal attempt to preempt state privacy laws.

"This will help us in the efficient delivery of care and allow physicians and payors to communicate freely," Coorsh said.

Congress actually granted itself the power to develop such rules in 1996, then missed its own August 1999 deadline to develop them.

The task then fell to Health and Human Services, which posted the draft privacy rules in November 1999 and will accept public comment on them through Feb. 17 before issuing final rules.

The proposed rules stray from a number of strong standards in medical privacy. Laws have long required patients to sign a "consent to release" information form, even for such routine tasks as allowing a physician to bill an insurer or to communicate with other health-care providers.

The proposed Health and Human Services rules do away with this requirement. The use of identifiable health information requires no patient consent or notice if it is "compatible with or directly related to treatment, payment, or health care operations."

This is like a "don't ask, don't tell" policy, allowing a hospital physician to look at the records of other patients with similar illnesses or even other family members without asking or telling anyone. Similarly, insurers, regulators, case managers, claims managers, data processors, and a host of others in the system will also have equal access. The patient has no right to demand an accounting of all medical record disclosures. The regulations also allow for law-enforcement agencies to issue administrative orders for medical information without going through the courts and without seeking the patient's consent.

As part of an investigation, the police could peek into your medical symptoms and treatments in search of criminal evidence to determine what medical evidence would correlate with drug use, child abuse, domestic violence or sexual diseases. Banking and payment processors will enjoy similar rights to examine your medical data without informing you, as long as it's "the minimum amount of protected health information necessary to complete a banking or payment activity." That likely would include medical information about the who, what, when, where and how of your medical care.

HHS spokeswoman Lorrie McHugh says that their proposed regulations "try to address the issue of consent by strengthening the information consumers must get about how their information is used and dsclosed."

But Paul Appelbaum MD, vice president of the American Psychiatric Association, said of the proposed regulations, "The approach is that the confidentiality of medical records can be set aside for any reason at all."

Doesn't the patient have a right to restrict access to their own medical data?

Unfortunately, no, the regulations do allow the individual "to request" that uses or disclosure be restricted.

However, the regulations state that the provider, "is not required to agree to the requested restriction." So it's their call, not yours. Also, an individual may not even request restriction of disclosure to a variety of government agencies.

What if you suffer personal damage from an inappropriate disclosure of medical information?

The regulations establish civil and criminal penalties for violations, but can only be enforced if an entity "knowingly" violated the privacy standards.

It would be up to the consumer to first discover the violation and then request HHS to prove that the use of a person's health care data was not related to "health care operations," a nearly insurmountable burden of proof for HHS, according to James Pyles, Washington, D.C., legal counsel for the American Psychoanalytic Association.

The patient has no right to sue for punitive or actual damages under these rules. These regulations are about government standards, and violations and fines would go to HHS. The patient would need to pursue litigation at his own expense.

Because these regulations are to be managed by HHS, the agency has granted itself broad powers to investigate and even confiscate records if they believe entities are out of compliance.

Think about this: When the Nixon White House burglars wanted to get Daniel Ellsberg's psychiatric records, they had to actually go to the doctor's office to steal them. Under the draft regulations, HHS could simply "suspect" that the good doctor was out of compliance and get copies of all this records to investigate. Of course, under the law-enforcement provision, the FBI also could request the records as evidence.

The regulations strip away most of the accepted checks and balances of informed consent and patient notification. There is no right or presumption of privacy, a staggering change in patient's rights that consumers and health-care professionals should examine closely. HHS may need to know that a major part of our privacy rights serve to protect against government intrusion. The federal government learned this recently when OSHA tried to extend its workplace standards to home office workers - giving itself and employers rights to inspection and enforcement in your own home.

Fortunately, public outrage squashed those rules within 24 hours.

LANGUAGE: ENGLISH

LOAD-DATE: February 7, 2000

The Detroit News

View Related Topics

June 11, 2000, Sunday

SECTION: Opinion; Pg. 6

LENGTH: 832 words

HEADLINE: Internet needs to get serious about **privacy** issues

BYLINE: Nolan Finley / The Detroit News

BODY:

How would you react if you discovered someone was secretly following you around the shopping mall, jotting down on a clipboard all the stores you visit, what windows you stop to gaze through, what you purchase and whether you use cash, check or credit card?

There would probably be a racket right there in the middle of The Gap, right?

But that's more or less what happens each time you browse the Internet. Visit a website that carries advertising and you'll likely come away with a "cookie" file on your computer. A cookie is a directional arrow that web sites place on your hard drive to track your online behavior. Some cookies simply record your activity within the site, noting how long you stay and what you look at while there. Others are more intrusive, tailing you wherever you go on the Internet, compiling information that is used to deliver highly targeted advertising.

Those are the cookies that leave a bad taste in the mouth of Michigan Atty. Gen. Jennifer Granholm.

She describes cookies as being "like a bar code on your back" and worries that Internet surfers are unwittingly opening a portal into their personal habits and preferences.

Granholm is leading a campaign for stronger privacy commitments from Internet companies. A recent Federal Trade Commission report found that only 20 percent of major Internet companies have adequate privacy protections. The report is fueling a push for federal legislation to regulate web privacy. A bill introduced in the Senate last week would require very clear notification when cookies are placed on a computer, make it simpler for consumers to reject cookies, allow them to see the data collected and mandate that sites secure the harvested information.

"Most people aren't aware they are being tracked and don't realize they have the option of refusing the cookies," Granholm says. "Unless a company has a privacy policy, they can take your personal information and sell it, or share it with others you have no control over."

Consumers, of course, can program their computers to reject cookies. But Granholm notes that many computer users either don't know about cookies or aren't technically savvy enough to dive into the bowels of their computer and purge them.

That would be me.

After talking with Granholm and getting considerable help from techno savants, I checked my own computer for cookies and, sure enough, found enough to keep a Girl Scout troop going door-to-door for months.

It was maddening to think of all those electronic bugs watching my every Internet move.

The dangers are obvious. Few people would care if a database somewhere had on file that they visited, say, amazon.com. But most wouldn't want their permanent cyber-record to reveal that they tarried for a while at nakedbabes.net.

No one is monitoring how the Internet dossiers can be used. Is it possible, for example, that an employer might find out a job applicant once ordered anti-depressants from a pharmaceutical site? Or might voters someday learn that a political candidate has a major shoe fetish he sates on the web?

The debate is whether the industry, responding to consumer pressure, is best able to police itself on privacy matters. Granholm contends that before the marketplace can exert sufficient pressure on Internet companies, consumers must be fully informed about cookies and the potential they present for abuse.

One remedy she suggests is uniform privacy practices posted in a conspicuous place on the web site and prohibiting the collection of personal information without permission. She is also talking with Microsoft Corp. about setting computers to automatically reject cookies, unless the user agrees to accept them.

In the meantime, she urges consumers to program their computers to notify them when cookies are being placed and to understand that information sent out on the Internet is not always private.

"You've got all these web sites saying 'Get a prize, register here, free free free,' in exchange for filling out a 25 question questionnaire," Granholm says. "Nothing is free. You are giving up your personal information. And there is nothing to prevent them from selling that information.

"Data mining is the gold of advertising. Why wouldn't they sell it?"

The attorney general doesn't want to ban cookies altogether. They can be a useful tool in personalizing the Internet experience.

"I want the Internet to be an exciting and dynamic place," she says. "I don't want to slow commerce. I just want consumers to be protected and feel comfortable."

For the Internet to thrive, it must be as unencumbered as possible by government regulation. But Americans hold privacy sacred and have an ingrained fear of being watched by Big Brother, whether he emerges in the form of big government or big business.

If the industry fails to self-regulate, it not only invites legislative intervention, it risks being shunned by consumers who have too many other choices to tolerate cyber-snooping.

GRAPHIC: Nolan Finley

LOAD-DATE: June 11, 2000

June 15, 2000, Thursday, Home Edition

SECTION: Editorial; Pg. 22A

LENGTH: 418 words

HEADLINE: Pass law to protect **Internet privacy**

BYLINE: Staff

SOURCE: CONSTITUTION

BODY:
Internet executives are supposed to be bright people who are helping to remake the world as we know it. But sometimes you have to wonder.

For example, e-commerce hasn't been the sudden success that many New Economy gurus had been predicting, and partly as a result, a lot of dot-com companies have been struggling to stay afloat. And when Internet users are asked in surveys why they don't like to shop or execute financial transactions over the Internet, the No. 1 reason is always the same: Fear that their information won't be secure or that their privacy will be invaded.

Given that problem, you might expect that companies that have bet their futures on the Internet would be eager for some means to ensure consumer privacy on the Web. If so, you would be wrong. Internet officials instead are lobbying hard in Washington to avoid any type of government regulation that would bar companies from using and selling consumer information gathered over the Internet.

The nature of that information is potentially very intimate. Already, companies have the ability to record if John Smith has sought information about impotence, or if Mary Smith has been visiting Web sites about menopause. How widely such data is used or disseminated is a matter of dispute.

In testimony this week before the Senate Commerce Committee, Internet officials are warning that government regulation will hamstring the Internet from fulfilling its potential, arguing that their industry should be allowed to regulate itself on privacy issues.

The very concept is ludicrous. Expecting Internet companies to regulate themselves on the Internet is like leaving a dozen 10-year-old boys alone in a room with a Playboy magazine. You might tell them not to look at it, but sooner or later one of them will take a peek. And once one of them succumbs to the temptation, they'll all do it.

In essence, the companies are demanding the right to peer over our shoulders as we navigate the Web, and they expect us to take their word for it that the information they gather in their spying won't be used inappropriately. And unfortunately, they are backing up that demand by flooding congressional races and political-party coffers with campaign donations.

However, campaign cash won't protect members of Congress who can't summon enough courage to protect their constituents' personal privacy. This is an important issue, and the public is not going to accept the

solutions that Internet executives have proposed so far.

LOAD-DATE: June 15, 2000

FOCUS™
Search: General News;headline (Internet w/5 Privacy)

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

The Dallas Morning News

View Related Topics

June 22, 2000, Thursday THIRD EDITION

SECTION: NEWS; Pg. 2A

LENGTH: 472 words

HEADLINE: SOMEBODY'S WATCHING;
White house drugg offices use of **Internet** tracker raises **privacy** concerns

SOURCE: Scripps Howard News Service

DATELINE: WASHINGTON

BODY:

WASHINGTON - The White House Office of National Drug Control Policy has taken its anti-drug message to the Internet, and it is secretly tracking those who find it in the process.

Search for drug terms such as "grow pot" on some Internet sites, and an ad banner that pops up from the drug office may drop a "cookie" in your computer that tracks your online activities.

"It's sort of spooky," said Internet consultant Richard Smith, a privacy advocate and former software engineer.

Despite what one critic called Big Brother tactics, the White House drug office says there's nothing surreptitious going on. The computer cookies are simply tracking its anti-drug media campaign.

"Cookies" are personal identifiers used to track the Web sites that computer users visit and what they buy. They identify Internet surfers by the service they are using to get access to the Internet and can be matched with other information online to provide personal identification.

Mr. Smith said he inadvertently discovered the government cookies while doing Internet research for pharmaceutical companies.

White House ads offering information on marijuana pop up when Internet users search for certain words connected to drugs on Internet search engines such as AltaVista or Lycos. The banner ads steer users to the anti-drug site www.freevibe.com, which is operated by the White House drug office. A tracking cookie is inserted into the user's personal computer as the site is activated.

Although Freevibe's privacy notice states that "no information, including your e-mail address, will be sold or distributed to any other organization," the site is connected to Doubleclick.com. Officials of Doubleclick, a New York advertising firm that is one of the largest companies gathering data on Internet user use, told the Senate Commerce Committee last week it is developing products that will profile more than 40 million Internet users.

Freevibe's site says that the White House drug office will collect the e-mail address "only so we can

identify your submission." It doesn't disclose its use of cookies.

Donald Maple, senior policy analyst with the White House drug office, said the cookie programs are part of a banner advertising campaign run through the New York advertising firm Ogilvie and Mather.

"We have a specific agreement with Ogilvie and Mather that they will not provide personal identification," he said.

Mr. Maple admitted that one of the anti-drug sites operated by the White House drug office and visited by 240,000 parents a month seeking information on drug abuse is inserting cookies into the computers of visitors. He said the drug office didn't know this until a reporter pointed it out.

This week it was to be disabled. "We didn't know it was there," Mr. Maple said. "It won't be shortly."

GRAPHIC: CHART(S): (DMN) WATCHING AND LEARNING

LANGUAGE: ENGLISH

LOAD-DATE: June 23, 2000

Chicago Tribune

View Related Topics

May 23, 2000 Tuesday, CHICAGO SPORTS FINAL EDITION

SECTION: Business; Pg. 1; ZONE: N

LENGTH: 599 words

HEADLINE: FTC SEEKS **INTERNET PRIVACY** LEGISLATION; CONGRESS UNLIKELY TO ACT ON REQUEST

BYLINE: By Frank James, Washington Bureau.

DATELINE: WASHINGTON

BODY:

Amid severe election-year opposition on Capitol Hill and little support from the Clinton administration, the Federal Trade Commission on Monday asked Congress for regulations to protect the privacy of consumers who use the Internet.

The majority of commissioners of the independent agency approved the action after the FTC's latest survey of the privacy practices--a random sample of commercial Web sites--indicated only 1 in 5 met minimum standards.

The call for new legislation was a reversal for the FTC. Until now it had advocated giving companies the chance to police themselves. But the failure of so many companies to enact comprehensive policies caused the commission to change its stance.

Mozelle Thompson, an FTC commissioner, said the commissioners did not think they were being premature in their decision because the commission has studied on-line privacy since 1997, a lengthy period in the Internet's evolution. During that time, the public's concern has grown as many companies have underreacted.

"If you take a look at what's happening out there in the world, consumers have not become less concerned, they've become more concerned about this issue," Thompson said. "We're getting the sense that the issue may indeed be larger than industry itself can solve."

While the regulations the FTC is seeking are given little chance of passage this year, Internet privacy is growing as a concern for consumers and businesses alike.

An FTC survey found that only 20 percent of a random sample of Web sites had already implemented four privacy-related practices recommended by the FTC. The percentage among the 100 most popular sites was significantly better at 42 percent, but still disappointing to FTC officials.

The survey also found that just 8 percent of the random sites displayed a privacy seal, while 45 percent of the most popular sites did. Privacy seals, which industry has promoted, are akin to the Good Housekeeping Seal of Approval, a symbol meant to raise consumer confidence.

The FTC's report released Monday recommended Congress pass legislation that would ensure "basic standards of practice for the collection of information on-line." The legislation would mandate consumer-oriented sites that use the Internet to gather personally identifiable information from or about individuals to conform to four FTC-recommended practices.

The companies would have to notify a consumer that certain information is routinely collected and allow the consumer to say no. They would also have to provide access to the personal information so an individual could correct mistakes, as well as provide security to keep the information out of unauthorized hands.

But prominent members of Congress see little chance that lawmakers will embrace the regulations anytime soon.

"It's doubtful that Congress will enact any sweeping privacy legislation this year," said Ken Johnson, a spokesman for Rep. Billy Tauzin (R-La.). Tauzin chairs a House Commerce subcommittee with responsibility for Internet matters.

"The quickest way to kill the Internet is to regulate it to death," Johnson said. Tauzin "has been encouraged by the progress made by the on-line industry to safeguard personally identifiable information."

The Clinton administration refrained from openly criticizing the FTC's recommendation. But it made clear it viewed the FTC's action as premature.

"The administration will continue its dialogue with the private sector and with consumer groups on effective mechanisms to ensure privacy on-line," said Commerce Secretary William M. Daley in a statement.

LANGUAGE: ENGLISH

LOAD-DATE: May 23, 2000

June 30, 2000

SECTION: News Review; ISSN: 1099-9248

LENGTH: 426 words

HEADLINE: Data Privacy: Get It Right to Get Users

BYLINE: Tim Kridel

BODY:

Although few attendees probably knew it, Wireless Agenda 2000 opened the same day that the Federal Trade Commission released a gloomy report to Congress on **Internet privacy:** Self-regulation alone isn't adequately protecting consumers, so legislation is a necessary supplement to guarantee basic protections.

That's food for thought, considering CTIA President & CEO Tom Wheeler's keynote proclamation that wireless data is the second Internet revolution, one that "promises to make the first pale in comparison." But Wheeler tempered that optimism by cautioning against claiming victory prematurely when three defining issues remain unresolved: insufficient spectrum, the cancer scare and subscribers' rights.

"If e-commerce is to morph into wireless commerce, we have to have a relationship of trust with customers," Wheeler said. "Our challenge is to do something about that now. We have the opportunity to deal with something before it deals with us."

For its part, CTIA will release a consumer code of ethics, and it's suing the FBI over plans to use E-911 location technology to track suspects. But at the show, it was clear that each wireless provider, vendor and application provider also will have to do its part. One recommendation: Every company should have a chief privacy officer, who would ensure that all technology and business practices protect users' privacy.

"The future of your company depends on people's acceptance of the technology," said Ray Evertt-Church, Alladvantage.com director of wireless-Internet applications.

Cautionary tales abound. Earlier this year, privacy watchdogs howled over the Pentium III, which includes an embedded serial number that Intel said would be used only to validate e-commerce transactions. Meanwhile, DoubleClick lost a third of its market cap over three days following the

· flap over its collection of Web surfers' profiles.

Wireless privacy is an even taller order because of location technology, which could be a public-relations nightmare despite a service provider's best efforts. Alan Davidson, Center for Democracy & Technology CTO, warned against keeping historical logs of users' locations because they could be subpoenaed even if the user isn't a suspect. Global roaming makes the lines even fuzzier because privacy laws vary widely.

It's enough to cloud the otherwise rosy predictions for advertising that makes its pitches based on the user's location.

"To many people, that's not a utopian vision," Davidson said. "That's an Orwellian vision."

LANGUAGE: ENGLISH

LOAD-DATE: June 28, 2000

May 5, 2000

SECTION: Vol. 51, No. 38; Pg. 1A; ISSN: 08937745

B&H-ACC-NO: 53820280

DOC-REF-NO: DENV-2288-2

LENGTH: 1228 words

HEADLINE: Privacy concerns mounting

BODY:

Colorado considers itself far ahead of other states when it comes to dealing with the hot **financial privacy** issues facing banks and other financial services companies.

The state Legislature passed a bill, HB 1395, just last month that creates a task force to look at all aspects of consumer privacy in Colorado. The law is undergoing minor tinkering and should go to Gov. Bill Owens for his blessing anytime now.

But financial industry analysts are concerned that most financially oriented companies aren't tacking privacy problems fast enough. Some companies are waiting for a canned, one-size-fits-all solution. Others are just waiting to see how a new federal privacy law works.

Analysts, however, don't expect dealing with the issue to be that simple.

"Folks seem a little lethargic about moving on this," said Kimberly Aaron, a senior manager at financial services firm KPMG in Dallas. "Most of the solutions to privacy problems are technological ones, and there's not a lot of time between now and next November to address them. People need to look at this today."

Time is key because in November of this year a federal law enacted in November 1999 - the Gramm-LeachBliley Act - goes into effect. That law's final regulations should be completed by the end of this month, and financial services companies will have until the fall to implement them.

At that time, Americans are expected to be flooded with some 2 billion questionnaires - that's an average of 20 per household - from banks, credit card companies, insurance companies, stock brokerage firms and even travel agencies asking how they want their personal information handled.

Consumers will have three choices. They can "opt in," or allow data about them, from their Social Security number to their home address, to be disseminated only with their OK, They can "opt out," and data will be shared unless they say no. Finally, there's the "do nothing" alternative, which allows the bank or other financial service source to do what it wants to.

But since Gramm-Leach-Bliley passed, how fast and how deeply privacy issues are addressed have become

controversial. The financial services industry generally has a wait-and-see-attitude, wanting to see how the law works before considering more restrictions. Consumer advocacy groups, on the other hand, want people to be able to prohibit the sharing of personal information sooner rather than later. As the federal law stands now, data can be shared whether the consumer says yes or no.

President Bill Clinton, who's had privacy-protection issues of his own, falls in the latter category. This week, he told Eastern Michigan University's newest graduates that the new information age shouldn't erode old, fundamental rights. To that end, he proposed toughening the law by giving consumers the outright ability to block the sharing of their personal information - particularly health-related data - not just have a say about how their information is used.

Aaron thinks banks that already have a computerized customer relationship management system in place won't have much problem digesting the responses to those questionnaires. They've already assembled their customer information in a single, central file. It should be relatively easy to add to that file a customer's preference for how its personal information should be shared.

But if firms and government agencies don't already have such a system, they will have to create one by November. Many financial institutions may have systems for managing client data, but because of the many mergers and acquisitions that have occurred in that industry, there's also a lot of duplication. One customer's name may appear in a couple of systems that haven't been combined yet.

Another reason for the sense of urgency among some in, and outside, the financial industry is that privacy issues are complicated, hugh and should continue to be of great concern for several years. The advent of the Internet has made swapping data as easy and fast as hitting "return" on a computer keyboard. They only start with the banking industry.

An especially complex part of the privacy debate is the definition of personal information itself. Is it only nonpublic data, or is it anything that can identify a particular person? A consumer's address is personal information, for example, but if it's in the telephone book, it's also public information.

"This issue has crept up on us as a society," said Don Childears, president of the Colorado Bankers Association. "It's so complex in every way."

Privacy waters get muddied further for banks because they need to protect clients' privacy to keep those customers, but they also want to sell them more services. Banks. further contend that some sharing of information with outside companies helps customers, and that privacy protections should be upheld by those third parties.

"When a customer comes in to open a checking account, we need to share their name, address and account number with the check company," said John Jackson,, president of VectraBank in Colorado Springs and past chairman of the Colorado Bankers Association. "Most customers consider that a convenience. We have to allow for convenience and protect privacy."

Some customers, on the other hand, are tired of being hounded by their bank to buy its insurance and use its credit cards. They're also afraid their addresses, account numbers and even health information - their identities - could be stolen electronically.

"People were fairly relaxed about that kind of information before the surge in technology, which is where the risk is coming from," Jackson added. "Things are shared so fast and broadly because of it. There's definitely a real risk; people ought to be concerned."

Added Joe Morford, a financial services analyst at Dain Rauscher Inc. in San Francisco: "Most people underestimate what their banks know about them. You know what you give them, but they can get more."

But banks are only the tip of the privacy iceberg. Several industries, for example, are expected to be represented on Colorado's **financial privacy** study team.

Childears put together a list that includes government agencies, which have vast amounts of private information for everything from driver's licenses to property liens; health care providers; and e-commerce companies that sell products on the Internet. It continues with telemarketing and direct marketing companies; media, from newspapers to cable TV, and stores like Colorado's King Soopers grocery chain and Wal-Mart, the country's largest retailer, which track everything customers buy through their purchasing cards and can sell that information. Even employers, charities and colleges and universities have a wealth of personal information.

After banking, the telecommunications business is expected to be next focus of interest regarding privacy Phone companies can monitor private calls, learning who calls where and how long the call lasts.

If a person places a five-minute phone order to Land's End, for example, the phone company watches that call and calculates how much merchandise the caller probably bought. It can then sell that information to a Land's End competitor like Eddie Bauer.

"It's astonishing what information is available if you know where to look for it and how to get it," concluded Kimberly Aaron.

LANGUAGE: ENGLISH

LOAD-DATE: June 15, 2000

FOCUS™
Search: General News;financial privacy

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

May 5, 2000

SECTION: Vol. 51, No. 38; Pg. 1A; ISSN: 08937745

B&H-ACC-NO: 53820280

DOC-REF-NO: DENV-2288-2

LENGTH: 1228 words

HEADLINE: Privacy concerns mounting

BODY:

Colorado considers itself far ahead of other states when it comes to dealing with the hot **financial privacy** issues facing banks and other financial services companies.

The state Legislature passed a bill, HB 1395, just last month that creates a task force to look at all aspects of consumer privacy in Colorado. The law is undergoing minor tinkering and should go to Gov. Bill Owens for his blessing anytime now.

But financial industry analysts are concerned that most financially oriented companies aren't tacking privacy problems fast enough. Some companies are waiting for a canned, one-size-fits-all solution. Others are just waiting to see how a new federal privacy law works.

Analysts, however, don't expect dealing with the issue to be that simple.

"Folks seem a little lethargic about moving on this," said Kimberly Aaron, a senior manager at financial services firm KPMG in Dallas. "Most of the solutions to privacy problems are technological ones, and there's not a lot of time between now and next November to address them. People need to look at this today."

Time is key because in November of this year a federal law enacted in November 1999 - the Gramm-LeachBliley Act - goes into effect. That law's final regulations should be completed by the end of this month, and financial services companies will have until the fall to implement them.

At that time, Americans are expected to be flooded with some 2 billion questionnaires - that's an average of 20 per household - from banks, credit card companies, insurance companies, stock brokerage firms and even travel agencies asking how they want their personal information handled.

Consumers will have three choices. They can "opt in," or allow data about them, from their Social Security number to their home address, to be disseminated only with their OK, They can "opt out," and data will be shared unless they say no. Finally, there's the "do nothing" alternative, which allows the bank or other financial service source to do what it wants to.

But since Gramm-Leach-Bliley passed, how fast and how deeply privacy issues are addressed have become

controversial. The financial services industry generally has a wait-and-see-attitude, wanting to see how the law works before considering more restrictions. Consumer advocacy groups, on the other hand, want people to be able to prohibit the sharing of personal information sooner rather than later. As the federal law stands now, data can be shared whether the consumer says yes or no.

President Bill Clinton, who's had privacy-protection issues of his own, falls in the latter category. This week, he told Eastern Michigan University's newest graduates that the new information age shouldn't erode old, fundamental rights. To that end, he proposed toughening the law by giving consumers the outright ability to block the sharing of their personal information - particularly health-related data - not just have a say about how their information is used.

Aaron thinks banks that already have a computerized customer relationship management system in place won't have much problem digesting the responses to those questionnaires. They've already assembled their customer information in a single, central file. It should be relatively easy to add to that file a customer's preference for how its personal information should be shared.

But if firms and government agencies don't already have such a system, they will have to create one by November. Many financial institutions may have systems for managing client data, but because of the many mergers and acquisitions that have occurred in that industry, there's also a lot of duplication. One customer's name may appear in a couple of systems that haven't been combined yet.

Another reason for the sense of urgency among some in, and outside, the financial industry is that privacy issues are complicated, hugh and should continue to be of great concern for several years. The advent of the Internet has made swapping data as easy and fast as hitting "return" on a computer keyboard. They only start with the banking industry.

An especially complex part of the privacy debate is the definition of personal information itself. Is it only nonpublic data, or is it anything that can identify a particular person? A consumer's address is personal information, for example, but if it's in the telephone book, it's also public information.

"This issue has crept up on us as a society," said Don Childears, president of the Colorado Bankers Association. "It's so complex in every way."

Privacy waters get muddied further for banks because they need to protect clients' privacy to keep those customers, but they also want to sell them more services. Banks. further contend that some sharing of information with outside companies helps customers, and that privacy protections should be upheld by those third parties.

"When a customer comes in to open a checking account, we need to share their name, address and account number with the check company," said John Jackson,, president of VectraBank in Colorado Springs and past chairman of the Colorado Bankers Association. "Most customers consider that a convenience. We have to allow for convenience and protect privacy."

Some customers, on the other hand, are tired of being hounded by their bank to buy its insurance and use its credit cards. They're also afraid their addresses, account numbers and even health information - their identities - could be stolen electronically.

"People were fairly relaxed about that kind of information before the surge in technology, which is where the risk is coming from," Jackson added. "Things are shared so fast and broadly because of it. There's definitely a real risk; people ought to be concerned."

Added Joe Morford, a financial services analyst at Dain Rauscher Inc. in San Francisco: "Most people underestimate what their banks know about them. You know what you give them, but they can get more."

But banks are only the tip of the privacy iceberg. Several industries, for example, are expected to be represented on Colorado's **financial privacy** study team.

Childears put together a list that includes government agencies, which have vast amounts of private information for everything from driver's licenses to property liens; health care providers; and e-commerce companies that sell products on the Internet. It continues with telemarketing and direct marketing companies; media, from newspapers to cable TV, and stores like Colorado's King Soopers grocery chain and Wal-Mart, the country's largest retailer, which track everything customers buy through their purchasing cards and can sell that information. Even employers, charities and colleges and universities have a wealth of personal information.

After banking, the telecommunications business is expected to be next focus of interest regarding privacy Phone companies can monitor private calls, learning who calls where and how long the call lasts.

If a person places a five-minute phone order to Land's End, for example, the phone company watches that call and calculates how much merchandise the caller probably bought. It can then sell that information to a Land's End competitor like Eddie Bauer.

"It's astonishing what information is available if you know where to look for it and how to get it," concluded Kimberly Aaron.

LANGUAGE: ENGLISH

LOAD-DATE: June 15, 2000

FOCUS™
Search: General News;financial privacy

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

June 1, 2000

SECTION: No. 6, Vol. 189; Pg. 29 ; ISSN: 0021-8448

IAC-ACC-NO: 62761700

LENGTH: 3688 words

HEADLINE: Lawmakers tackle privacy.

BYLINE: Pugliese, Anthony; Kravitz, Peter M.

BODY:

Tech growing pains are giving privacy issues a high profile. Technology allows the easy accumulation and distribution of personal financial data as well as the theft of these data. The growing demands and interrelatedness of the marketplace have increased companies' need for profiling the purchasing habits and financial situations of consumers. A few companies made headlines last year for their poor stewardship of customer information. This notoriety helped to make consumer **financial privacy** an urgent issue for Congress, the public and the business community.

For example, U.S. Bancorp of Minnesota sold confidential customer financial information from its files to third-party marketers. The story made national news, causing U.S. Bancorp and several other financial institutions to stop the practice and prompting the Minnesota attorney general to file suit against U.S. Bancorp. In another major privacy story, Amazon.com profiled its customers' most popular book and music purchases, named the companies employing those customers making the purchases and published the information on its Web site. Customers' reaction caused Amazon.com to immediately stop publishing it. But Amazon still retains the data.

According to USA Today, only 20 of the 100 biggest online retailers have privacy policies that restrict the use of customer information to completing transactions. Although some e-commerce companies have seals--such as the WebTrust[SM] seal--to indicate the company's privacy policy, consumer groups and many on Capitol Hill believe that regulating the use of private financial information is necessary, and that disclosure and consumer choice regarding privacy policies are not enough to protect consumer privacy.

This is an area where the CPA's expertise puts him or her in an excellent position to help financial institutions to implement, maintain and monitor the privacy policies and systems they will have to create.

WAKE-UP CALL

In early January details about the first major theft of consumer financial information from an e-commerce company flashed into the news. A computer hacker had broken into the system of CD Universe and copied 300,000 customer credit card files. The hacker attempted to extort money from CD Universe in exchange for returning the information, When CD Universe refused to submit to extortion, the hacker posted the names, addresses and credit card numbers of 25,000 customers on a Web site. Although this theft happened

to an e-company, confidential financial information can be stolen from any company that maintains such records.

Although federal law essentially shields consumers from any loss due to the unauthorized use of their credit cards (there is a $ 50 dollar limit on a credit card), this incident heightened concern over the privacy and security of data stored in computers. Ultimately, all consumers will foot the bill for these losses when companies pass the charges to their customers in the form of higher costs.

NEXT?

Since the accounting profession's stock-in-trade is confidential financial information, it is conceivable that the Federal Reserve Board could adopt a regulation subjecting CPAs in public practice to the privacy rules applicable to financial institutions, which require periodic disclosures to clients about the privacy and integrity of confidential data. However, the proliferation of current and upcoming privacy statutes and regulations also opens up business opportunities for the profession and at the same time could subject CPAs to tougher requirements.

To mitigate risks, companies will seek assurance services that test the efficacy of their privacy systems. Clearly, of the act and what WebTrust achieves for e-commerce and SysTrust[SM] for any business are pioneering efforts in this area (see sidebar, "AICPA Assurance Service institutions." Programs That Address Privacy Issues," page 31). Privacy consulting--both creating privacy policies and systems as well as internal controls--is also an area where the accounting profession's expertise can put CPAs front and center in the effort to guard public and business interests.

THE HARDWARE STORE AS FINANCIAL INSTITUTION

The privacy provisions of the 1999 Financial Services Modernization Act apply to financial institutions and their treatment of nonpublic personal information. The act defines a financial institution as "any institution the business of which is engaging in financial activities," and the Federal Reserve Board is given the authority to determine what activities are financial. Once an activity is determined to be financial in nature, then companies that engage in such an activity are subject to the privacy provisions of the act, whether or not the company is affiliated with a financial holding company.

Such a broadening of the term financial institution heaps compliance burdens on an enormous number of businesses that before this development would not have been considered part of the financial arena. For example, a local mom-and-pop store could be a financial institution because it extends store credit to its customers. Stretching the concept further, it also is possible that accounting firms could be considered financial institutions for purposes of the privacy law--preparing tax returns is arguably a financial service.

Businesses will face challenges: (1) they must comply with the provisions of the act and/or (2) they must ensure they do not lose customer loyalty because their systems are not secure and reliable.

With the growing prominence of privacy issues, CPAs operating in various roles in industry, especially in financial institutions, should take notice of the privacy issues that affect their employers in both the online and offline worlds. These issues might take the form of new laws and regulations, such as those required by the act and/or the best practices that are being followed by industry to ensure that customer confidence and trust are kept at the highest levels possible (see sidebar, "Best Practices" page 32). Best practices include accepted industry standards and practices such as posting privacy policies on a Web site in a conspicuous place or having internal controls to ensure that privacy policies are not violated. For more information on best practices for banking and other industries, the CPA working in industry might look to the AICPA

WebTrust program.

CPAs who work in public practice should know the requirements of the act and inform clients how the requirements will affect day-to-day operations, especially businesses that might not think of themselves as "financial institutions" but are now considered such. In addition, the recent focus on privacy creates a wealth of service opportunities for the practitioner in his or her role as adviser to clients. As more and more clients migrate to e-commerce environments or engage in information-sharing practices, the need for consultative advice and assurance on all aspects of operations affected by these changes becomes paramount to clients and potential clients. Sometimes it's not the details that clients are aware of that add the most value to CPA services but, rather, the things they are not aware of.

The Financial Services Modernization Act of 1999

The privacy law imposes burdens on all "financial institutions," whether or not they transmit nonpublic personal information to third parties.

The law prohibits

* The transmission of private personal information to nonaffiliated third parties without prior notice to the customer and without a customer option to prevent it.

* The transmission of an account number "or similar form of access number or access code" to a nonaffiliated third party that wants to use the information for marketing purposes.

The law requires all financial institutions to

* Notify their consumer customers of the privacy policy at the onset of the relationship and annually thereafter.

* Disclose the affiliate sharing notice and the opt-out opportunity for affiliate information sharing.

What it doesn't do

* The act does not regulate the sharing of information between a financial institution and its affiliates.

* The act does not ban all third-party transmissions. It provides for some exceptions, allowing the transmission of nonpublic personal information to third parties such as accountants and auditors without the necessity of customer disclosure and the opt-out choice.

* The act does not provide for private rights of action for violations. Enforcement is given over to the federal financial regulators for banks, thrifts and credit unions; to the SEC for brokers, dealers, investment companies and advisers; to state insurance regulators for insurance companies; and to the FTC for everyone else.

* The act does not amend the Fair Credit Reporting Act, which provides an opportunity for customers to opt out of a company's sharing "nontransaction" financial information, such as a credit report, with an affiliate.

EXECUTIVE SUMMARY

* E-COMMERCE PRIVACY ISSUES ARE HIGH PROFILE in Washington. Technology allows the easy accumulation and distribution of personal financial data as well as the theft of these data, and security must be ensured.

* INCIDENTS THAT CAUGHT THE ATTENTION OF Congress were a bank selling confidential information to third-party marketers; a major Internet company publishing customer data; and a hacker who tried to extort money from a company to stop publication of stolen credit card numbers.

* IMPORTANT ACTION IS UNDER WAY, Look at the list of bodies promulgating regulations that will affect financial institutions: the Federal Reserve Board, the FDIC, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the SEC, the FTC and the National Credit Union Administration.

* WHAT CONSTITUTES A FINANCIAL INSTITUTION? The act's definition goes far beyond traditional labels. It defines one as an entity engaging in an activity that is financial in nature or incidental or complementary to a financial activity, and it empowers the Federal Reserve Board to determine which businesses fit the definition. That description could include a local merchant that extends consumer credit or a CPA firm that prepares tax returns.

* THE FINANCIAL SERVICES MODERNIZATION ACT of 1999 bans the dissemination of consumer information to third parties without a customer option to prevent it. It also requires financial institutions to disclose to consumers their privacy policy at the outset of the relationship and annually thereafter. Enforcement is solely the province of federal financial regulators.

RELATED ARTICLE: AICPA Assurance Service Programs That Address Privacy Issues

WebTrust[SM]

WebTrust addresses the fundamental privacy concerns of both the business community and the online customer. The WebTrust seal informs potential customers that a CPA has evaluated a Web site's business practices and controls to verify they conform with the WebTrust principles and criteria for business-to-consumer electronic commerce. WebTrust is the only online privacy seal program that provides for independent verification and the only Internet service that reviews security of financial information maintained by e-commerce companies.

As e-commerce becomes the global and preferred way of conducting business, countries around the world are setting standards to assure citizens that their information is kept private. The European Union privacy directives for the European market took the lead in this area. In the United States, the Online Privacy Alliance, a coalition of businesses, is leading an initiative to demonstrate that the government does not need to be involved. WebTrust meets or exceeds all these key organizations' critical requirements regarding privacy, as well as the key requirements of the Financial Services Modernization Act of 1999.

WebTrust requires online businesses to make privacy disclosures and testing in the following areas:

* The specific kinds and sources of private information that is being collected and maintained; the use of the information; and third-party distribution of the information.

* Choices regarding how identifiable private information collected from an individual online may be used and/or distributed.

* The business transaction consequences of an individual's refusal to provide private information or of his or her decision to opt out of a particular use of such information.

* How individually identifable private information collected can be reviewed and, if necessary, corrected or removed.

* If a Web site uses cookies (files placed on a consumer's computer by an online business that allow it to track information on sites visited and buying habits), how they are used and the business transaction consequences of an individual's refusal to accept a cookie.

For a complete copy of the CPA WebTrust principles and criteria, refer to www.aicpa.org/Webtrust/index.htm.

SysTrust[SM]

In a SysTrust engagement, a CPA firm issues an attestation report that evaluates whether management of an e-business has maintained effective controls to ensure that its systems function reliably within a specified period of time.

Developments in information technology make far greater power available to companies at far lower costs. The systems supported by this technology range from tools for bookkeeping to running businesses, producing products and services and dealing with customers and business partners. Among the concerns of customers and business partners is the reliability of conducting business in a manner that protects private or confidential information from unintended or unlawful uses.

A reliable system is defined as one that is capable of operating without material error, flaw or failure during a specified period of time in a specified environment. A SysTrust report on a reliable system is underpinned by four essential principles--the benchmarks of reliability:

* Availability--the system is available for operation and use.

* Security--the system is protected against unauthorized access.

* Integrity--the system processing is complete, accurate, timely and authorized.

* Maintainability--the system can be updated when necessary.

SysTrust is the only attestation service available for signifying whether a company's privacy systems have effective controls that enable the system to function reliably. For more information on the CPA SysTrust services and to review the SysTrust principles and criteria, refer to www.aicpa.org.

RELATED ARTICLE: Best Practices for Building Consumer Trust

In response to growing concerns from online shoppers about security and privacy protection, and in light of recent high-profile breaches of public trust at several brand-name Web sites, the AICPA offers several tips to Web merchants to help them build consumer trust and confidence.

Maintain a High Level of Security

E-commerce sites must use the most reliable security controls and tools and communicate that they do so to

their customers in easy-to-understand language. This includes the latest SSL encryption technology, digital certificates, secure server technology and authentication to ensure that personal customer information is safe. The site should be independently verified to ensure that its security controls adequately protect its customers from risk of security breaches.

Build Online Credibility and Legitimacy

Brand names are important on the Internet. They help shoppers make choices when they have a limited range of knowledge about quality and functionality. If an e-commerce site lacks its own recognizable consumer brand name, it can sell branded products from other manufacturers, partner with an established brand, offer samples of its services through low-risk trials and creative offers or use a CPA to independently verify that it is a legitimate business. Whichever strategy is used, it is important to be consistent and adhere to the highest set of standards so that customers trust the site.

Maintain a High Standard of Integrity With All Transactions

Web sites have to maintain a high degree of integrity with every transaction and they should be independently tested for compliance against a stringent set of standards. Many a Web site loses sales when the buyer has to struggle to complete a transaction. Nothing alienates shoppers more often than order-entry glitches that cause the loss of entered information, computer freezes or being bounced off the site. A site's lack of full disclosure regarding actual costs is also a big turnoff. Online shoppers want to know all costs before going through detailed registration in order to avoid surprises and significant changes to the online price. An order-tracking system that allows online shoppers to review orders and/or maintain addresses and credit card information is also very helpful in building trust in a site.

Fully Disclose Policies and Make the Site Easy to Navigate

Online shoppers want to know how a site will handle their personal information, so Web merchants must explain how they collect and handle consumer data and must post easy-to-read privacy statements. Some customers are not willing to buy online without assurance from independent third parties that their confidential information will be protected. The design and content of a site are also critical elements in attracting potential customers.

Support Online Consumer-to-Consumer Dialogue

E-commerce sites can build additional trust when they encourage their customers to contact and inform each other about a site's products and services: A chat group sponsored by the site allows its customers to question each other about their purchasing experiences. The online business can also provide links to other independent sites that allow customers to obtain feedback and ratings.

Empower Consumers to Take Control of Decisions

Online shoppers will trust a site when they know that they control access to their personal information. Web sites that ask permission to obtain customers' personal details are taking the smartest approach. Some companies, for example, discuss the benefits provided by cookies on a user's hard drive (the cookie ensures that preferred settings appear without the customer logging in each time) and then asks the user for permission to place a cookie. The online shopper is fully informed and empowered to make the decision whether to allow the cookie onto the hard drive. Many e-commerce sites are beginning to ask consumers to serve on panels that independently audit their privacy policies, the integrity of their transactions and their fulfillment records.

RELATED ARTICLE: What's Happening in D.C.?

Privacy was not an issue during the first four years of debate on the Financial Services Modernization Act of 1999 (the GrammLeach-Bliley act). This changed when the U.S. Bancorp story broke. Concerns about privacy helped spur Congress to adopt as part of the act the first comprehensive federal privacy provisions applicable to financial institutions.

According to Gary Gensler, treasury undersecretary for domestic finance, the Clinton administration will offer new privacy legislation this year. The Treasury will also finish a wide-ranging study of privacy issues by the end of 2000, which could lead to additional privacy proposals. In February Senator Richard Shelby (R-Ala.) and Congressman Edward Markey (D-Mass.) announced the founding of a bipartisan Congressional Privacy Caucus. Its purpose is to fight for tougher consumer **financial privacy** laws.

Regulations defining the exact scope of the privacy provisions will be promulgated by several federal agencies. The federal banking agencies, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision have issued a joint proposal and will adopt identical regulations. Also adopting regulations will be the Securities and Exchange Commission, the Federal Trade Commission, and the National Credit Union Administration. It is expected that these regulations will be similar to each other in some aspects but will differ in others.

An example of how they may differ in treatment is the definition of nonpublic personal information. The modernization act defines personally identifiable financial information as information that is provided by the consumer to the financial institution. Excluded is information that is publicly available through sources such as the telephone book, tax records or land records. It is possible to determine that a customer's name and address are nonpublic because the financial institution receives them from the customer. Contradictorily, since this information is also available from the telephone book, tax records and other public records, it could be determined to be public information.

The act allows states to adopt privacy policies that provide consumers with even more protections. If the states ultimately adopt different privacy laws, financial institutions operating across state lines will need to have multiple privacy policies and disclosures.

The federal banking agencies, NCUA and the FTC issued their proposed regulations in February, the SEC in March. The modernization act provides that the regulations be made final by May 12, with an effective date six months later. Federal regulators are empowered to set an effective date that is later than November 12.

PETER M. KRAVITZ is director of congressional/political affairs at the AICPA. His email address is pkravitz@aicpa.org. ANTHONY PUGLIESE, CPA, is director of assurance services at the AICPA. His email address is apugliese@aicpa.org. The authors are both employees of the American Institute of CPAs and their views, as expressed in this article, do not necessarily reflect the views of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation.

LANGUAGE: ENGLISH

IAC-CREATE-DATE: June 20, 2000

LOAD-DATE: June 21, 2000

Money

June, 2000

SECTION: MONEY.COM/BETTER FINANCES THROUGH TECHNOLOGY; Pg. 161

LENGTH: 1465 words

HEADLINE: Protecting Your **Financial Privacy;**
YOUR FINANCES ARE LESS SECURE THAN YOU THINK. BUT THE WEB CAN HELP YOU FIGHT BACK.

BYLINE: Amy Feldman

BODY:

Internet customization definitely has its benefits. Those targeted offers from Amazon.com for books you might want to read based on your earlier purchases are often eerily on target. And it's hard not to like the convenience of tracking your portfolio or paying bills online. But if you're like most people, you're also increasingly edgy about how little control you have over your own data--particularly sensitive medical and financial information.

This is the devil's bargain of the Web: In pursuit of effortless surfing, shopping and investing, we turn over huge stores of valuable details about ourselves. And once such information is out there, it can be sold, shared and crunched, often without our knowledge or our consent. While financial companies have long bought and sold their customers' data for marketing purposes, the Web makes the issue of **financial privacy** even more problematic, since many of us now routinely give away intimate financial details to websites we know next to nothing about.

Want to try that cool portfolio tracker that you just heard about (from, perhaps, a magazine like this one)? No problem. Just take a few moments to register with your name, address, phone number, e-mail address, income and, of course, the contents of your entire portfolio. What happens to your data thereafter is anybody's guess--unless you read the site's privacy policy (assuming there is one), approve of what it says and trust that the site is true to its word. And portfolio trackers are just the beginning. Every time you shop for a mortgage,get a life insurance quote or apply for a credit card online,you are placing trust where it may or may not be deserved.

Why be concerned with the widespread dissemination of your

financial data? First, there's the intrusive advertising. Companies you already have a relationship with may "bombard you with information because they think they know something about you," says George Simeone, a partner at Deloitte & Touche. But the other, more troubling use that companies find for your information is to sell it to third parties.

Last year, in a case that became a touchstone for **financial-privacy** awareness both online and off, Minnesota prosecutors sued U.S. Bancorp for renting, in violation of its stated privacy policy, customers'private financial info (including credit-card numbers) to a telemarketer. In the subsequent settlement,U.S. Bancorp CEO Jack Grundhofer called such data marketing an "industrywide practice." Minnesota attorney general Mike Hatch, who says he's pursuing several other similar cases, agrees: "We thought it was an outlier, but it is not."

But don't look for sweeping reform to happen any time soon. New rules passed as part of last year's financial modernization bill purport to protect privacy but really only demonstrate how little control we have over our own info. Expected to go into effect later this year, these rules require financial firms to tell customers about their privacy policies and to allow customers to bar their personal information from being sold to or shared with unaffiliated marketers. But only a small percentage of people currently choose to "opt out," as the lingo has it, and critics argue that the new rules don't go far enough to safeguard consumers. "The potential for misuse is way too high for the benefits," says Andrew Shen, policy analyst at the Electronic Privacy Information Center.

If the prospect of your information floating from bank to marketer and beyond concerns you, here are a few things you can do online to try to protect yourself.

SEE WHAT'S AT STAKE. Check out the free online resources of the Electronic Privacy Information Center, the Privacy Rights Clearinghouse and other privacy groups for a briefing on current issues and privacy trends, plus a complete rundown on what rights you have--and what rights you don't have. (For more details on these and other privacy-related sites, see the table below.)

WATCH WHERE YOU TREAD. Most commercial websites now post their privacy policies online. These legalistic statements detail what the company will and will not do with the data it collects on you. To get a better handle on how online privacy policies compare, head to Enonymous.com, which uses a four-star system to rate more than 30,000 sites. Just a minuscule 3.5% get Enonymous.com's highest rating. "Consumers want to know what a

site will not do, so if the site rules out certain behaviors, it gets a higher rating," says Enonymous.com co-founder Tim Kane. Likewise, be wary of turning your financial info over to any site (even if it's just to compare auto-loan rates) without first finding out whether the company is reputable and knowing what it will do with the data.

OPT OUT OFTEN. In most cases, if you want to be excluded from data sharing, you have to ask. If you want to minimize all those e-mails and phone calls touting products, then opt out every chance you get. Often you can do so online; sometimes, however, you still will have to write a letter. Under the new regulations, your bank, your brokerage and your insurer (whether online or off) will also be required to remind you each year how to say no.

And if you're committed to taking your fight for privacy one step further, head to the preferences menu of your Web browser. Both Internet Explorer and Netscape Navigator can be configured to block all "cookies," those bits of software that can track your surfing habits without your knowledge. Be warned, though, that such blocking could also bar you from certain websites and disable many other sites' best customization options.

No matter what you do, unfortunately, many of your financial details are already irretrievably public. But rather than simply wishing for a return to a simpler era, you can take these precautions to protect yourself from further erosions of your privacy.

--AMY FELDMAN
amy_feldman@moneymail.com

BOX STORY:

INSIDE

taxes

NET INVESTOR 168
Do small investors make good venture capitalists?

BOX STORY:

PRIVACY RESOURCES ONLINE

If you're worried about online privacy, here's where you can turn for help and information.

NAME ADDRESS(WWW.)
WHAT YOU'LL FIND

Center for Democracy and Technology cdt.org
Privacy resources and information;
special opt-out section at opt-out.cdt.org

Electronic Frontier Foundation eff.org
Information about electronic privacy
and freedom of expression

Electronic Privacy Information Center epic.org
Clearinghouse for online privacy with news,
resources and publications

Junkbusters junkbusters.com
Information on how to get off targeted
marketing lists and block online "cookies"

Privacy Choices privacychoices.org

Instructions from online ad placement firm
DoubleClick on how to opt out of targeted ads

Privacy Ratings privacyratings.org
Four-star rating system for privacy policies,
run by Enonymous.com

Privacy Rights Clearinghouse privacyrights.org
Fact sheets and issue papers on a variety of
privacy issues; special section on identity theft

U.S. Public Interest Research Group pirg.org/consumer/

privacy/index.htm
Details on **financial privacy** and links to other
sites from the well-known consumer advocacy group

Sources: The websites.

BOX STORY:

Number of shares of TheStreet.com Bear Stearns held in February: 1.6 million. Number it held in April: 53.

BOX STORY:

Number of cases of online auction fraud reported in 1997: 107.
Number of cases reported in 1999: 10,700.

BOX STORY:

Amount spent on Internet purchases outside the U.S.: $ 8.4 bil.
Amount spent in California alone: $ 5.9 bil.

GRAPHIC: COLOR PHOTO ILLUSTRATION: EDMUND GUY, COLOR PHOTO: RAOUL BENAVIDES, Privacy prosecutor: Minnesota's attorney general Mike Hatch

LANGUAGE: ENGLISH

LOAD-DATE: May 15, 2000

May 5, 2000

SECTION: No. 38, Vol. 51; Pg. 1A ; ISSN: 0893-7745

IAC-ACC-NO: 62206290

LENGTH: 1245 words

HEADLINE: Privacy concerns mounting; financial information privacy regulation

BYLINE: MOORE, PAULA

BODY:

Feds, state address keeping data secret

Colorado considers itself far ahead of other states when it comes to dealing with the hot **financial privacy** issues facing banks and other Financial services companies.

The state Legislature passed a bill, HB 1395, just last month that creates a task force to look at ill aspects of consumer privacy in Colorado. The law is undergoing minor tinkering and should go to Gov. Bill Owens for his blessing anytime now.

But financial industry analysts are concerned that most financially oriented companies aren't tackling privacy problems fast enough. Some companies are waiting for a canned, one-size-fits-all solution. Others are just waiting to see how a new federal privacy law works.

Analysts, however, don't expect dealing with the issue to be that simple.

"Folks seem a little lethargic about moving on this," said Kimberly Aaron, a senior manager at financial services firm KPMG in Dallas. "Most of the solutions to privacy problems are technological ones, and there's not a lot of time between now and next November to address them. People need to look at this today."

Time is key because in November of this year a federal law enacted in November 1999 -- the Gramm-Leach-Bliley Act -- goes into effect. That law's final regulations should be completed by the end of this month, and financial services companies will have until the fall to implement them.

At that time, Americans are expected to be flooded with some 2 billion questionnaires -- that's an average of 20 per household -- from banks, credit card companies, insurance companies, stock brokerage firms and even travel agencies asking how they want their personal information handled.

Consumers will have three choices. They can "opt in," or allow data about them, from their Social Security number to their home address, to be disseminated only with their OK. They can "opt out," and data will be shared unless they say no. Finally, there's the "do nothing" alternative, which allows the bank or other

financial service source to do what it wants to.

But since Gramm-Leach-Bliley passed, how fast and how deeply privacy issues are addressed have become controversial. The financial services industry generally has a wait-and-see-attitude, wanting to see how the law works before considering more restrictions. Consumer advocacy groups, on the other hand, want people to be able to prohibit the sharing of personal information. sooner rather than later. As the federal law stands now, data can be shared whether the consumer says yes or no.

President Bill Clinton, who's had privacy-protection issues of his own, falls in the latter category. This week, he told Eastern Michigan University's newest graduates that the new information age shouldn't erode old, fundamental rights. To that end, he proposed toughening the law by giving consumers the outright ability to block the sharing of their personal information --particularly health-related data -- not just have a say about how their information is used.

Aaron thinks banks that already have a computerized customer relationship management system in place won't have much problem digesting the responses to those questionnaires. They've already assembled their customer information in a single, central file. It should be relatively easy to add to that file a customer's preference for how its personal information should be shared.

But if firms and government agencies don't already have such a system, they will have to create one by November. Many financial institutions may have systems for managing client data, but because of the many mergers and acquisitions that have occurred in that industry, there's also a lot of duplication. One customer's name may appear in a couple of systems that haven't been combined yet.

Another reason for the sense, of urgency among some in, and outside, the financial industry is that privacy issues are. complicated, huge and should continue to be of great concern for several years. The advent of the Internet has made swapping data as easy and fast as hitting "return" on a computer keyboard. They only start with the banking industry.

An especially complex part of the privacy debate is the definition of personal information itself. Is it only non-public data, or is it anything that can identify a particular person? A consumer's address is personal information, for example, but if it's in the telephone book, it's also public information.

"This issue has crept up on us as a society," said Don Childears, president of the Colorado Bankers Association. "It's so complex in every way."

Privacy waters get muddied further for banks because they need to protect clients' privacy to keep those customers, but they also want to sell them more services. Banks further contend that some sharing of information with outside companies helps customers, and that privacy protections should be upheld by those third parties.

"When a customer comes in to open a checking account, we need to share their name, address and account number with the check company," said John Jackson, president of VectraBank in Colorado Springs and past chairman of the Colorado Bankers Association. "Most customers consider that a convenience. We have to allow for convenience and protect privacy."

Some customers, on the other hand, are tired of being hounded by their bank to buy its insurance and use its credit cards. They're also afraid their addresses, account numbers and even health information -- their identities -- could be stolen electronically.

"People were fairly relaxed about that kind of information before the surge in technology, which is where the risk is coming from," Jackson added. "Things are shared so fast and broadly because of it. There's definitely a real risk; people ought to be concerned."

Added Joe Morford, a financial services analyst at Dain Rauscher Inc. in San Francisco: "Most people underestimate what their banks know about them. You know what you give them, but they can get more."

But banks are only the tip of the privacy iceberg. Several industries, for example, are expected to be represented on Colorado's **financial privacy** study team.

Childears put together a list that includes government agencies, which have vast amounts of private, information for everything from driver's licenses to property liens; health care providers; and e-commerce companies that sell products on the Internet. It continues with telemarketing and direct marketing companies; media, from newspapers to cable TV; and stores like Colorado's King Soopers grocery chain and Wal-Mart, the country's largest retailer, which track everything customers buy through their purchasing cards and can sell that information. Even employers, charities and colleges and universities have a wealth of personal information.

After banking, the telecommunications business is expected to be next focus of interest regarding privacy. Phone companies can monitor private calls, learning who calls where and how long the call lasts.

If a person places a five-minute phone order to Land's End, for example, the phone company watches that call and calculates how much merchandise the caller probably bought. It can then sell that information to a Land's End competitor like Eddie Bauer.

"It's astonishing what information is available if you know where to look for it and how to get it," concluded Kimberly Aaron.

LANGUAGE: ENGLISH

IAC-CREATE-DATE: May 24, 2000

LOAD-DATE: May 25, 2000

To: Joshua Gottheimer

From: Lauren Steinfeld
(5-3647)

COMMERCE NEWS
UNITED STATES DEPARTMENT OF COMMERCE
Office of the Secretary • Washington, DC 20230 • www.doc.gov

FOR IMMEDIATE RELEASE
May 22, 2000

Contact: Morrie Goodman
(202)482-4883
Chuck Melley
(202)219-4287

STATEMENT BY U.S. SECRETARY OF COMMERCE WILLIAM M. DALEY ON ON-LINE PRIVACY PROTECTION

Today the FTC released a survey that shows that there has been significant improvement in the number of websites that tell their customers about company privacy policies. In June of 1998, the FTC surveyed the extent of privacy protection online and found that only 14% of commercial websites surveyed posted a privacy policy of any kind. In one year, we saw that number jump to 65%, and today -- as the FTC has just announced -- to 88%. "Seal of approval" programs – such as TRUSTe, BBBOnline, and CPA Webtrust – have emerged to offer companies guidance in assuring privacy protection and to assure consumer confidence that their personal information is being handled responsibly. Many industry leaders have pledged only to advertise on the websites of companies that post privacy policies. We are also seeing the power of new technologies to assure privacy protection online, such as the P3P platform.

Challenges remain in two primary areas. First, the quality of the website privacy policies still has a long way to go. Second, there are enforcement challenges -- how should industry be held accountable for protecting privacy?

We continue to believe that private sector leadership is a critical component to high-quality privacy protection online. Some have suggested that the challenges of ensuring high quality privacy policies and adequate enforcement warrant a legislation solution. However, legislation will not be sufficient on its own, given the pace of technological change; the emergence of privacy challenges that neither we nor Congress can anticipate today; and the innovative privacy solutions that only the private sector can develop. In addition, some self-regulatory programs are providing monitoring and dispute resolution procedures that can produce greater protections for consumers.

However, it is clear that there is still a significant "free rider" problem. By that, I mean that while some companies are behaving responsibly, others are successfully avoiding any scrutiny by not offering any privacy policy and thus escaping from FTC or any other enforcement authority. Still some other companies have a privacy policy, but do not offer a meaningful opportunity to opt-out of information collection.

-MORE-

The Administration will continue its dialogue with the private sector and with consumer groups on effective mechanisms to ensure privacy protection online. To the extent that the private sector can show how it will address the free rider problem and improve the quality of privacy policies, legislation would not be necessary. As we have long stated, if we do not see such progress, then we may eventually need to consider whether legislation would provide companies with the right incentives to have good policies and participate in an effective self-regulatory program. Of course, if in the coming months a dramatic increase in the quantity and quality of privacy policies were to occur, the shape of our response would change. I look forward to working with a full range of affected parties on these challenges.

In short, I believe that there are three core components to securing effective privacy protection online. First, there must be strong leadership by the private sector. Second, we must avoid unnecessary regulation. And third, regulation – if necessary – should be minimal, predictable, cost-effective and clear. It should recognize and provide incentives for self-regulation, such as by granting participants in effective self-regulatory programs a "safe harbor" from regulation. This approach is the optimal one to ensure that more people are offered more protection by more websites.

Finally, there are areas of privacy protection that deserve immediate legislative action. These areas include financial privacy, medical records privacy, and genetic discrimination, where we have a developing consensus on the need for and the feasibility of legislation.

###

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

April 5, 2000

TAB 24 pp

MEMORANDUM

TO: **JOHN PODESTA**

FROM: **SALLY KATZEN**
PETER SWIRE

RE: **CYBER-SECURITY LEGISLATION INITIATIVE**

In recent weeks, we have run a process at the staff and deputies levels for a possible cyber-security legislative package. We began with about 30 items for possible inclusion in the package. A number of these items have been dropped, and others have been substantially amended. Several are already "cleared" Administration policy, but new questions have been raised about them.

In the end, we have consensus or near-consensus that the following 18 items, considered individually, each makes good policy. We call these items "nominees" for a legislative package. A brief description of each nominee is contained in Attachment A. The nominees are:

1. Nationwide trap and trace orders.
2. Emergency exception to trap and trace for ongoing, felony-level computer attacks.
3. "Shall" to "may" language to add judicial discretion to trap and trace orders.
4. Computer Fraud and Abuse: damages less than $5,000 are a new misdemeanor.
5. Aggregate damages to $5,000 to prove felony-level computer fraud.
6. Restrict mandatory sentences for computer fraud to only serious felonies.
7. Replace outdated telephone-only language.
8. Authorize monetary assistance to state and local law enforcement.
9. Permit voluntary disclosure of traffic information for stored information.
10. Application to computers located outside of United States.
11. Elevate protections for "electronic" communications to be same as for "wire" communications.
12. Increase penalties for illegal interceptions.
13. Sentencing Commission to study penalty enhancement for offenses involving privacy.
14. Treat some juvenile offenders as adults for hacking.
15. Access to electronic data by civil investigators.
16. Criminal forfeiture of hacking tools.
17. Clean Hands Exception to Suppression Remedy: Use Against Illegal Interceptor (cleared).
18. Cyberstalking (cleared).

In addition to these items, there are four other proposals that are priority items for DOJ or other agencies but are controversial among the Deputies. They are:

19. Computer trespasser provision.
20. Privacy Protection Act (cleared).
21. Cable Act (cleared).
22. Other clean hands exception to suppression remedy: useable in court provided government was not involved in the interception (cleared).

The most important of these is the "computer trespasser" provision, which would allow a system owner to authorize interception of communications to and from a computer trespasser. DOJ and DOD consider this provision a priority, in order to allow law enforcement and national security officers to assist system owners in responding to computer attacks, when authorized by the system owner. The provision would not apply to any interception of communication other than those to or from the trespasser.

DOJ and DOD stress that the provision, taken together with the elevation of "electronic" communications to the protections offered to "wire" communications, would actually increase the level of protection against interception for ordinary, authorized users. A number of agencies and White House offices have expressed reservations about the provision, concerned either that its scope would be too broad or would be perceived publicly as "putting a cop on the Internet."

The computer trespasser exception and the three controversial but already-cleared items are discussed below.

In the first Deputies meeting, Jim Steinberg suggested that we prepare a Framework document that shows the range of Administration actions in the cyber-security area. Any legislative package could be presented in the context of these much broader Administration activities, thereby demonstrating that the legislative proposals are part of a balanced overall effort in the area. The Framework is attached as Attachment B.

As the discussions proceeded, support for some items on the "nominee" list became linked with inclusion of other items. First, although DOJ itself originally proposed to elevate protections for "electronic" communications to the stricter "wire" level, DOJ later indicated that its support for this change is contingent on including significant enough new authorities for law enforcement. Second, items 2 and 3 on the nominee list are linked-- the Deputies agreed to include item 2 (emergency exception to trap and trace for ongoing attacks) only if taken together with item 3 (adding judicial discretion in issuing trap and trace orders).

DECISION ON CONTROVERSIAL ITEMS

Before turning to the size and shape of a potential package, you will need to decide whether to support the computer trespasser provision and the other controversial items.

1. COMPUTER TRESPASSER PROVISION

DOJ and DOD assert that they cannot now respond to system owner requests for help when they are confronted with significant problems and unlawful intrusions. Current law requires either a Title III warrant or use of one of the exceptions to that requirement (none of which is apparently available in many unlawful intrusion scenarios).

The proposal. The proposal would allow a system owner or operator to authorize interception of communications to and from a computer trespasser. "Computer trespasser" means a person who has no reasonable expectation of privacy in any communications transmitted to, through, or from a protected computer because the person is accessing the protected computer without authorization. The proposal allows access to a "person acting under color of law," notably, for law enforcement and national security purposes. A Title III order is not required for communications intercepted under this proposal.

Interception would be permitted where there is:

(A) Written authorization by the system owner or operator, with an explanation of the basis for believing that the intrusion is unlawful;

(B) An ongoing investigation;

(C) Reasonable grounds to believe the content is relevant to an ongoing investigation; and

(D) No interception of communications other than those to or from the trespasser.

Rationale for the proposal. The provision fits within the theme that the legislation would update telephone-era authorities for the Internet age. In a telephone world, the large phone companies had a strong incentive and ability to protect against hacks, which were often theft-of-service. On the Internet, the much larger number of system owners often lack the know-how to protect their own systems and prevent their systems from being used as a base for attacks on others. The provision would allow computer system owners to authorize law enforcement to investigate hackers, while retaining current law for any communications involving authorized users.

Safeguards against abuse. Safeguards against abuse would likely include: (i) current criminal penalties for unlawful interception; (ii) statutory civil remedies of $10,000 for unlawful interceptions (a

nominee for inclusion in our proposal); and (iii) harmonizing "electronic" communications to the stricter "wire" standards, so that authorized computer users would have *greater* protections than currently while trespassers would be governed by the new proposal. A key point is that the provision would not change current law with respect to authorized users, requiring a Title III order unless consent or some other exception applied.

There was consensus that authorization by the system owner should be in writing by a named individual. ("Writing" should include e-mail or other electronic writing.) System owners, both public and private, would have discretion about who would be permitted to give authorization. There was discussion, but no final recommendation, about what sort of approval there should be from the law enforcement or national security side. One option is to require AUSA approval or some equivalent in other agencies.

An additional possible safeguard, opposed by DOJ, would be to set a time limit on the use of the computer trespasser exception, such as for 30 days. There was also discussion about whether there could be language that says that interceptions would not be used for unrelated investigations. As the number of restrictions increases, however, it is not clear that the provision would continue to provide the assistance to law enforcement and system operators that they have sought.

Notwithstanding the additional safeguards and restrictions, several offices are very concerned that support for this provision may well be perceived as willingness, indeed enthusiasm, for putting a cop on the Internet. Given what they expect to be a very adverse reaction from the privacy and Internet communities, they fear it will bring down whatever package it is attached to. DOJ insists industry wants this help and would not criticize our move in this direction.

Recommendation: The optics here are hard to answer and we fear the risk it will impose to the rest of the package is too great.

_____ *Agree* _____ *Disagree* _____ *Let's Discuss*

2. PRIVACY PROTECTION ACT

The Privacy Protection Act was originally enacted in 1980 to address the search of Stanford's student newspaper. The Act requires a subpoena rather than a search warrant for government access to the work product of publishers. With changing Internet technology, every web page might be considered a publisher, and the Act's strict provisions thus can be interpreted to apply far more broadly than before. The proposal would apply the Act's strict limits on searches of publishers' materials so that searches of work product "incidental" to a lawful search would no longer be covered.

DOJ makes a strong substantive case for changed circumstances. Critics, however, might take

advantage of the statute's title to criticize a "rollback of the Privacy Protection Act." Because the statute specifically concerns publishers, there is some chance that the press will give particular attention to any proposed change.

This proposal has been previously cleared by the Administration.

_____ *Include with Nominees* _____ *Exclude*

CABLE COMMUNICATIONS POLICY ACT AMENDMENTS

The Cable Communications Policy Act establishes a strict standard for access to personal information, including an adversary proceeding before a court in which the subscriber can dispute disclosure. Privacy advocates often cite the Cable Act as a model privacy statute. In addition, Senator Leahy has recently proposed raising the standards for intercepting satellite communications to equal the strict cable standards.

As cable companies have begun to offer Internet service, the strict standards under the Cable Act have created problems for law enforcement investigations that call for obtaining electronic evidence of crimes involving the Internet. The issue arises of how to treat Internet-type communications over cable networks. Current law would appear to apply the Cable Act. The proposal would be to apply the same ECPA standards that apply to the Internet generally. At the same time, the proposal would provide that the stricter cable standards continue to govern "records revealing customer cable television viewing activity."

Similar language has previously been cleared. The current text is materially more protective of privacy than the already-cleared language. Nonetheless, Commerce, White House Counsel, and OMB have expressed concerns about amending the Cable Act. One concern is the public reaction to a proposal to reduce the level of privacy protection for the affected cable subscribers.

_____ *Include with Nominees* _____ *Exclude*

CLEAN HANDS EXCEPTION WHERE GOVERNMENT NOT THE INTERCEPTOR

This clean hands exception has been previously cleared but was highly controversial among the Deputies. The provision would allow use of an interception in evidence when the interception was by a person not acting under color of law and the party seeking to introduce the contents did not participate in the interception.

DOJ has argued for giving this item priority treatment. It allows investigations to go forward, based on evidence from unlawful wiretaps, where law enforcement was not to blame. DOJ notes that the exception applies to evidence used either for the prosecution or for the defense. This exception is viewed by law enforcement as a necessary accompaniment for extending the suppression remedy to electronic communications.

In opposition, this exception could well give an incentive to encourage prosecution based on illegal interceptions. Law enforcement officials insisted that there would not be any such incentive to encourage use of illegal interceptions, but many of the non-law enforcement Deputies believe that the provision would play badly and point out that DOJ states the exception would be rarely used.

_____ *Include with Nominees* _____ *Exclude*

THREE OPTIONS FOR ADMINISTRATION ACTION

There are essentially three options for a legislative strategy: (1) propose most or all of the nominee items; (2) decide not to propose a legislative package; or (3) create a more modest package. To assist in considering a more modest package, we have attached a "Cyber Security Issues Grouping" (Attachment C) that clusters issues in ways that suggest some possible ways to expand or contract the scope of our effort.

Option 1: Propose Most or All of the Nominee Items.

Pro: (1) There is consensus or near-consensus that most of the items, considered one at a time, are good policy. A broad package, therefore, would do the most substantive good if enacted.

(2) Whether or not an updating package passes this year, affirmative Administration proposals lay the groundwork for eventual progress on the substantive questions of how to update law enforcement authorities for the Internet.

(3) Schumer and Kyl have introduced a bill that contains a half-dozen items, and Hatch and Leahy are reportedly working together on a related bill. Active Administration involvement would help us shape this process and increase the chances of its gaining momentum.

(4) The history is that the opportunity to update authorities in this area comes infrequently. DOJ thus wishes to make the most of an opportunity to make the full range of needed reforms.

Con: (1) A big package can also be a big target. As the number of provisions grows, so too may the

number of groups that have concerns about something in the package. The public attacks from those who oppose elements of the package may be more intense than public statements of support.

(2) A big package may be hard to square with the message from the Cyber Security Summit, where the Administration stressed private-sector leadership but did not emphasize a sweeping need to change law enforcement and national security authorities.

(3) In a short legislative year, there simply may not be time for Congress to handle a big, complicated package. In terms of getting new law enforcement authorities, more may actually be achieved with a modest package.

(4) As the package grows larger, it is harder to demonstrate that it is balanced among other goals of enhanced law enforcement powers and civil liberties.

Option 2: Don't Propose a Package.

Under this approach, there would be no Administration legislative package. We would still have to decide what input to provide through quiet technical assistance, and what we would say on each issue in Congressional testimony.

Pro: (1) There is a risk that any package will attract criticism both for being too weak on law enforcement *and* for threatening civil liberties.

(2) It enables us to provide technical assistance where we want without accepting ownership.

(3) We would only have to comment on the items that are raised on the Hill. We could thus postpone making decisions about what to say on all of the items on the list.

Con: (1) DOJ and FBI have said several times said that they are working on a legislative proposal to update law enforcement authorities for the Internet. We would thus need an explanation for why we did not offer a proposal.

(2) Because the Administration will likely be pushed over time to testify and otherwise make public statements about these issues; we may be better off affirmatively proposing a position and sticking to it. That way we can better frame and take credit for the positions that we will eventually take.

(3) Agencies may see this approach as a green light to push their pet proposals.

Option 3: Create a More Modest Package.

This option would create a more modest Administration proposal. Some possible ways to create a modest package are set forth below.

Pro: (1) As mentioned above, more may actually get through Congress with a modest package, and a more modest package fits more closely with the tone of the Cyber Security Summit.

(2) Supporting a modest package avoids the twin dangers of saying too much (a large package that draws criticism) and saying too little (we have testified that DOJ is studying the topic, and need to have something to say).

Con: (1) DOJ and the FBI believe that they need to have significant new authorities for law enforcement to make this effort worthwhile.

(2) Even a modest package may draw significant criticism from at least some vocal elements of the civil liberty and privacy community. (We would need to do more consultations to have a good feel of where industry would be.)

Possible Groupings in Creating a Modest Package.

For option 3, we have worked up a "Cyber Security Issues Grouping," which is attached (Attachment C). This document creates clusters of issues that naturally balance themselves. The groupings are:

- A trio of trap and trace authority changes, that both expand the ability to track possible wrongdoers and enhances judicial oversight over the process.

- A trio of changes to the Computer Fraud and Abuse Act, which expand the scope of the law while reducing the use of mandatory sentences.

- Some "pure updating" items that have consensus within the Deputies group and that do not seem controversial.

- The computer trespasser provision. Balancing can be done within this provision, by specifying how many and how strict the conditions would be on use of the new computer trespasser authority.

- Additional items that do not fit neatly within the other groups. The most important of these is likely the elevation of "electronic" communications to the set of protections afforded "wire" communications. For this and other privacy-oriented provisions, an open question is which and

how many of the other law enforcement proposals form a proper package.

- Already cleared items. The greatest consensus at the Deputies level was on the cyberstalking proposal and a proposal to allow introduction of intercepted communications to prove wrongdoing by the person who did the interception. The strategic question here is which already cleared items to include in an announcement of a cyber-security package.

ATTACHMENT A

NOMINEES FOR INCLUSION IN PACKAGE

TRAP AND TRACE PROVISIONS

1. Nationwide Trap and Trace (p. 52)

Trap and trace orders track a phone call or Internet session back to its origin. The proposal would expand a federal court's power to issue nationwide trap and trace orders. Orders would apply for "any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." The change responds to changing technology and industry structures. Instead of serving an order once on a unified Bell system, law enforcement today must cope with multiple phone providers and an Internet that often bounces communications through multiple nodes.

The Attorney General has already testified in favor of this idea. Hatch, Schumer, and Kyl all support. Some opposition is possible from civil liberties groups due to concerns about greater use of trap and trace orders and potential that prosecutors would forum shop to get the nationwide orders. White House Counsel would support contingent on raising "electronic" protections to the "wire" level.

2. Emergency Exception to Trap and Trace Requirement

DOJ has made this item one of its priorities. Currently, law enforcement can install a pen or trap device without a prior court order if there is an "emergency situation," defined as one involving conspiratorial activity or danger of death or serious bodily injury. HTCB would add a new emergency category for "an ongoing attack on the integrity or availability of a protected computer." To qualify, the attack must be punishable as a felony, i.e., cause over $5,000 in damage.

3. Increase Judicial Discretion for Trap and Trace Orders.

Current law states that a federal judges "shall" issue a trap and trace order upon the statutory showing. This amendment would say that a judge "may" issue such an order, thereby stating explicitly that the judge has the discretion to find that the statutory showing has not been made in a particular instance.

This provision would be seen as a significant move in the civil liberties direction. At the last Deputies meeting, support for this change was made a condition of the group accepting the emergency exception to the trap and trace requirement.

COMPUTER FRAUD AND ABUSE ACT AMENDMENTS

4. Removing the $5,000 Threshold for Computer Fraud (pp. 3, 5)

Under current law, a computer intrusion involving damage to a computer is only a federal offense for damages of $5,000 or more. The HTCB would remove this monetary threshold for misdemeanor offenses. DOJ has already testified in favor of this idea.

Government Views. The current system poses a problem for law enforcement investigations of computer intruders where prosecutors have found it difficult to prove monetary damage of $5,000. Eliminating the $5,000 threshold, for instance, would permit federal prosecutions of intrusions against individuals' computers, where monetary damage may be impossible to prove. It would also permit law enforcement to act early against a virus, before significant monetary damage occurs.

Outside Views. Privacy and civil libertarians might oppose this provision on the grounds that it eliminates a line that was intended to direct law enforcement against only the most serious attacks. A related concern would be to define what events should be federal, as opposed to state, crimes.

5. Aggregating Damage to Meet $5,000 Felony Computer Fraud Threshold (p. 3)

The HTCB would make it a felony where computer fraud causes loss to one or more persons during a one year period *aggregating* at least $5,000 in value. This provision responds to the way that computer crime is increasingly committed. Today, a criminal may launch a series of attacks on many computers and devices. Each attack may fall short of the $5,000 minimum, but together these attacks could add up to serious damage worthy of felony status.

6. Restrict Mandatory Sentences for Computer Fraud to only Serious Felonies (p. 8)

The HTCB would amend the Sentencing Guidelines so that certain offenses, including accessing a computer without authorization and recklessly or negligently causing damage, would not be subject to mandatory imprisonment. These changes are necessary to remedy the unfair punishment of imprisonment for negligent or reckless commissions of law violations.

PURE UPDATING

Some of these provisions fit comfortably within our theme of updating telephone-era laws for the Internet age. For instance, the current statute in some places uses the term "device" and seems to exclude software-based approaches. Other provisions are technical fixes, such as the voluntary disclosure of traffic information.

7. Replace outdated language

The HTCB would replace the term "electronic storage" with "interim storage." In the trap and trace area, it would replace "phone lines" with language that includes other facilities to which trap and trace devices may be applied. It would also replace "devices" with "processes" in the trap and trace area, to include software as well as hardware.

These linguistic changes may be of only modest substantive importance. By stressing the telephone-based language in some parts of the current statute, they may be quite useful in explaining our overall rationale for needing to update law enforcement authorities.

8. Assistance to State and Local Law Enforcement Agencies (p. 12)

To assist state and local law enforcement agencies that are falling behind in the cybercrime effort, the HTCB would authorize approximately $15 million FY 2001 funds for training and to establish regional computer forensic laboratories. Note that this is authorizing language for the grant funding in the President's FY 2001 budget request for DOJ.

9. Voluntary Disclosure of Traffic Information (p. 39)

The current Section 2702 concerns voluntary disclosure of "contents." The language does not explicitly permit voluntary disclosure of traffic information (such as phone or IP number), even though such information is widely understood to be less sensitive than the actual content of communication. Because of this anomaly in the current statute, providers are uncertain of their ability to disclose transactional records, and have in some cases refused to voluntarily turn over traffic information. Government instead has had to compel disclosure, thereby slowing or frustrating investigations.

The proposal would make this technical correction, and allow voluntary disclosure of traffic information under the same standards that have applied to contents.

10. Application to Computers Located Outside of United States (p. 4)

The offense of computer fraud, under the HTCB, would be extended to cover computers located outside of the U.S. It would allow the U.S. to prosecute a U.S. hacker intruding into a system in Japan. This provision is consistent with the President's commitment, through the G-8 Summit, that there should be no safe-haven for computer hackers.

The provision also fits our updating theme, because modern networks and network intrusions are so often international.

ADDITIONAL ITEMS

The following items do not fall into any neatly defined group. The most important of these is the decision to elevate the protections that currently apply to "wire" communications to "electronic" communications. If this provision is included, a key question is which and how many provisions that enhance law enforcement authorities should be included to keep the proper balance.

11. Elevating Protection for "Electronic" Communications to "Wire" (p. 25)

The HTCB proposes to elevate the protection of "electronic" communications to the level currently provided for "wire" communications. Interception of electronic communications would now be: (i) subject to high-level departmental approval; (ii) allowed only for listed felonies; and (iii) subject to the stricter statutory suppression rules.

This is a harmonization in favor of privacy protection and will be a substantial plus for the civil liberties side of the balance. DOJ has indicated that it would support this item only if other priority items are included. The provision would make law enforcement's job more difficult to comply with these stricter standards when intercepting electronic communications.

Treasury, late in the process, requested that we consider including a hate crime provision in the package. One way to do so would be to add hate crime criminal provisions to the list of predicates for a Title III order.

12. Increase Penalties for Illegal Interceptions

The DOJ proposal would increase penalties in three settings. These provisions are privacy enhancing, because they deter illegal interceptions, and also increase law enforcement authority.

- Raise penalties for unauthorized interceptions of wireless communications to the level for illegal intercepts of ordinary phone calls.

- Restore, per Congress's intent, statutory damages for violating the wiretap statute to $10,000.

- Raise penalties for unauthorized access to unopened e-mail.

13. Sentencing Commission to Study Penalty Enhancements for Offenses Involving Privacy violations (p. 13)

The HTCB would require the U.S. Sentencing Commission to study the adequacy of penalties for offenses that involve a substantial invasion of individual privacy and, if justified, provide for enhancements of such penalties. This provision is unobjectionable but is not likely to be considered very significant.

14. Special Provisions for Juvenile Offenders

DOJ proposes to make juveniles charged with serious hacking offenses eligible for prosecution in federal court as juveniles. (p. 51) It would allow juvenile violations of the statute to count as prior convictions for those who continue to violate the statute as adults. (p. 5)

This provision is in the Kyl-Schumer bill, and the FBI has made positive comments about it in testimony.

15. Permitting access to electronic data by civil investigators (pp. 40-42)

Civil investigators at the federal and state level can today get basic subscriber information through Section 2703(c)(1)(C). They can use an administrative subpoena to get open e-mail -- content -- under Section 2703(b). But they cannot get other transactional information such as log-in time, who e-mails were sent to, etc. The HTCB would allow such civil authorities, using the appropriate legal process, to obtain that other transactional information.

16. Criminal Forfeiture. (p. 6-7)

This provision would apply criminal forfeiture rules to equipment used in computer attacks. DOJ had proposed also including civil forfeiture, but that provision has been dropped due to the ongoing dispute with Rep. Hyde on that issue.

ALREADY CLEARED ITEMS - CONTINUED CONSENSUS

The following items have been previously cleared and there continues to be consensus on them.

17. Clean Hands Exception to Suppression Remedy: Use Against Illegal Interceptor

As discussed above, the proposal may extend the remedy of statutory suppression to electronic communications. At the same time, it could create a "clean hands" exception for statutory suppression involving electronic and voice communications in criminal cases. There was consensus in favor of one clean hands exception, to allow evidence obtained from an illegal interception to be introduced in court for use against the person alleged to have intercepted it.

18. Cyberstalking (p. 8)

The HTCB would make it a crime to use a telecommunications or computer device to transmit information with intent to cause physical injury or damage to property or fear of such injury or damage to property. This provision was cleared, in slightly different form, in the Administration's Cyberstalking Report, issued last fall. DOJ has pointed out that this provision should be considered as enhancing both law enforcement and privacy, because of the sanctions

against intrusive behavior.

Notably, in light of recent events, the same section of the HTCB prohibits duping others to participate in a denial of service attack.

April 4, 2000 **Attachment B**

A Framework for Building Trust and Security in Cyberspace

Introduction

A. Computers bring great opportunity for E-commerce and society more generally

B. Continued growth of digital society is founded on trust

1. Trust that goods and services will be available
2. Trust that users will have security and privacy online

C. Special obligation of government to protect digital information that citizens entrust with the Government

D. Challenges: earning and keeping that trust

1. Increased reliance on computers makes us increasingly vulnerable
2. Need greater attention to safety and security measures
3. Efforts to address safety must protect and strengthen other values including free speech and privacy

I. Theme 1: The Private Sector Should Lead in Protecting Private Systems and Networks, and in Ensuring that the Internet Remains a Trusted Place for Business, Education, and Communities

A. Most computers and networks that we rely upon are in private sector

B. Private sector has the responsibility to lead in security

1. The Internet and networked systems are not centrally managed, and government has a limited role at best
2. Companies know their own systems better than anyone else
3. Private sector role to develop and deploy strong security products and services
4. Private sector role to prevent activities by employees that impair security

C. Administration support of voluntary private sector action

1. Promoting voluntary information sharing among companies about threats, vulnerabilities, and needed security actions:
   a) federal support for CERT
   b) support for creation of Information Sharing and Analysis Centers – financial services in operation, electric power and others in process;

— announcement at Cyber Security Summit of industry support for computer systems ISAC

2. Encouraging sector-wide action in key sectors (banking and finance, transportation, information and communications, energy) (e.g. continuous dialogue with industry associations and leaders; designation of Lead Sector Coordinators for key infrastructures)
3. Privacy – support TRUSTe, BBBOnline, and other self-regulatory approaches to safeguarding personal information
4. Promoting adoption of standards and best practices for information security through NIST and the National Information Assurance Partnership (NIAP)

D. Using market mechanisms to increase security and privacy

1. Encouraging growth of private sector markets in insurance, auditing and other risk management products and services (White House cyber-security insurance conference)

E. Other steps to promote confidence and thus E-commerce

1. Develop "cyberethics" curricula, technological tools, and other efforts that educate and empower Internet users
2. Develop codes of conduct, technical standards, and best practices for privacy and consumer protection

II. Theme 2: The Government Should be a Model for Information Security and Privacy, and for Building Trust in the Digital Society

A. Government agencies must all protect their computer-controlled systems

B. Existing law and policy requires each agency to ensure its systems are secure

1. Computer Security Act, Paperwork Reduction Act, and Clinger-Cohen
2. OMB direction pursuant to Circular A-130
3. PDD-63: Protection of Critical Infrastructures
4. PDD-67: Continuity of Government

C. Administration actions: Empowered Process to Improve Security and Privacy within Federal systems

1. Operations assistance from CIO Council, NIST, and GSA (including FedCirc)

2. Creation of Expert Review Team – first ever permanent full time capability to assist agencies on cyber-security problems (FY01 budget initiative)
3. Departmental Plans developed to identify and address vulnerabilities
4. Role of CICG for critical infrastructure-specific issues
5. New budget process: OMB's security decision criteria for funding IT systems ("Lew's Lessons"); CICG/OMB/NSC budget process for cross-cutting initiatives
6. OMB, CIOs, and NIST – security performance measures and best practices
7. Chief of Staff's April 1 report to the President on distributed denial of service attacks

D. Administration actions: Investment in new technology

1. Install Firewalls and IDS systems to detect and block attacks
2. PKI – government must expand its own use of encryption: for DOD (implementation memo 1999); for civilian agencies (FY01 budget initiative)
3. Next generation Intrusion Detection Systems – for DOD: Joint Task Force-Computer Network Defense; for National Security agencies: NSERC; for Civilian agencies: Federal Intrusion Detection Network (FIDNet)

E. Administration actions: Investment in Personnel

1. Recruit, train, and retain information security experts through the Federal Cyber Service Program (FY01 budget initiative)

F. Devoting the necessary resources – FY 2001 budget proposals

1. Key New Initiatives
   a) Education: Federal Cyber Service: $25M
   b) Technology: FIDNet: $10 M
   c) Improving Government security: Expert Review Team: $5M
2. Substantial growth in budget – from $1.1B FY 98 to $2.0B FY 01
3. Increased emphasis on civilian agency cyber security: from 10% of budget FY00 to 25% FY01

G. Government must provide for security in its own systems

1. Thompson-Lieberman bill would codify existing security policies and practice, including the bifurcation of national security and non-national security policies and procedures. DOD would maintain authorities over the former; OMB the latter. The bill was passed unanimously by Senate Governmental Affairs committee on 3/23, largely including Administration views. House action will follow

H. Government must keep personal information of citizens private and secure

1. Appointment of first Chief Counselor for Privacy at OMB;
2. Privacy Act protection for many information collections, including online information collections
3. Privacy Impact Assessments for IT systems
4. Privacy policies on Federal websites – 100% compliance

III. Theme 3: The Federal Government Will Work in Partnership with the Private Sector -- Building Security and Trust in the Digital Society

A. Government can

1. Elevate awareness in industry of the business case for building security and trust
2. Help identify problems and solutions
3. Invest in R&D for long term solutions
4. Support education and prevention

B. Framework for Joint National Action

1. First ever National Plan for Information Systems Protection, released by POTUS in January
2. POTUS Cyber-security Summit with Internet leaders
3. Administration's "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet"

C. Structures for partnership

1. Establish a permanent Presidential Advisory panel on critical infrastructure protection issues – the National Infrastructure Assurance Council (NIAC) – underway, members to be announced soon

2. Develop a broad based government-industry "Partnership for Critical Infrastructure Security" – already launched with the participation of over 130 major companies

D. Structures for Information Sharing

1. Government support for Information Sharing and Analysis Centers (ISACs) in private sector ($1M in FY01 budget)
2. InfraGard – information sharing consortium – FBI, private sector companies, academic institutions, state and local governments
3. Consumer Sentinel – FTC database shared with over 220 law enforcement agencies

E. Investing in Research and Development

1. Create the Institute for Information Infrastructure Protection to facilitate research that fills gaps in the combined government and private sector research agenda; ($50M FY01 budget)
2. 30% increase in Federal R&D investment – to $606M in FY01

F. Investing in Education

1 Education partnership – DOJ and Information Technology Association of America ("ITAA")
2. Education partnership: creation four years ago (with government leadership) of the National Colloquium for Information Systems Security Education bringing together government, academia, industry

IV Theme 4: Law Enforcement and Defense Capabilities for the Internet Age

A. Updating telephone era laws: As the public and private sector have re-engineered their information systems and business models, we must examine possible re-engineering of the law

1. The recent release of the Administration's "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet" established principles that apply to the updating exercise:
   a. Online-offline consistency
   b. Technology neutrality
   c. Appropriate investigatory tools
   d. Consideration of other societal interests

2. Specific proposals to update the law from DOJ include:
   a. Eliminate telephone-specific language in legal rules
   b. To keep pace with crime that now takes place over many devices in many geographical regions, permit the tracing of criminal communications with a single order
   c. Punish cyberstalkers who might currently escape prosecution under federal law, because existing statutes do not address types of stalking that are new on the Internet
   d. Address hacking issues that do not exist in phone systems. Therefore, when permitted by a computer system owner, authorize law enforcement to watch a computer trespasser who has broken into the system and to gather evidence against him or her
   e. Harmonize the protections afforded Internet communications, eliminating any distinction based on whether the provider is only an Internet service provider or also a cable provider
   f. Amend a statute written to apply to traditional print media so that it does not prevent criminal investigations of all persons who happen to have a web page

B. Specialized resources and new organizational structures to address the evolving law enforcement and national security challenges of cyber-security and privacy

1. Creation of the National Infrastructure Protection Center within the FBI
2. Enhancing intelligence capabilities for cyber security threats.
3. Update resources, e.g., FY2001 budget proposal provided $37 million to DOJ to increase staffing, training, and technological capabilities to fight against cybercrime

C. Building new partnerships between law enforcement and the private sector

1. Attorney General's upcoming partnership conference at Stanford

V. Theme 5: Preserve Fundamental American Values

A. Protecting privacy and civil liberties; President's statement in Internet speech to make sure "that as government works to protect our citizens in cyberspace, it does not infringe on our civil liberties"

1. Self-regulation progress on Internet privacy
2. Medical records proposed regulations, for electronic records
3. Financial privacy legislation and new legislative proposal
4. Children's Online Privacy Protection Act of 1998

5. Steps to assure privacy of records held by government
6. In current cyber-security discussions
    a. Harmonize the treatment of wire (voice) and electronic (such as e-mail) communications, so that they receive similar levels of protection
    b. Other privacy-enhancing proposals, such as stricter penalties against interception

B. Improving the quality of life for all Americans

1. The growth of electronic commerce has improved Americans' ability to access wealth of information, products, services
2. The e-commerce industry has also created new jobs and opportunities for millions of American workers

C. Promoting free speech

D. Protecting children

E. Provide broad access to public information; such as e-government initiatives that increase public access.

April 4, 2000

Attachment C: Cyber Security Issues Grouping

Trap and Trace (*)

1. Nationwide trap and trace – **A**
2. Emergency exceptions to trap and trace for ongoing, felony-level attacks – **A**
3. "Shall" to "may" language to add judicial discretion to trap and trace orders – **B**

Computer Fraud (*)

4. Damages less than $5,000 are a new misdemeanor – **A**
5. Can aggregate damages for $5,000 to prove felony-level computer fraud – **A**
6. Restrict mandatory sentences for computer fraud to only serious felonies – **B**

Pure Updating (**)

7. Replace outdated telephone-only language
8. Assistance to state and local law enforcement – **A**
9. Permit voluntary disclosure of traffic information for stored information – **A**
10. Application to computers located outside of United States – **A**

Additional Items

11. Elevate protections for "electronic" communications to be the same as for "wire" – **B**
12. Increase penalties for illegal interceptions – **A, B**
13. Sentencing Commission to study penalty enhancement for offenses involving privacy – **B**
14. Treat some juveniles as adults for hacking – **A**
15. Access to electronic data by civil investigators – **A**
16. Criminal forfeiture – **A**

Cleared Items

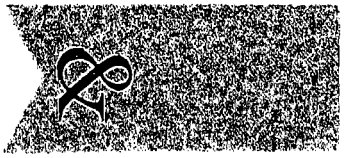
18. Clean Hands Exception to Suppression Remedy: Use Against Illegal Interceptor – **A, B**
19. Cyberstalking – **A, B**
20. Privacy Protection Act – **A**
21. Cable Act – **A**
22. Other Clean Hands Exception to Suppression Remedy: Useable in court provided government was not involved in the interception – **A**

Key:

- "*" indicates a possible cluster of issues balancing law enforcement and civil liberties
- "**" indicates unlikely to be controversial
- "A" – indicates provision primarily in the direction of providing law enforcement and national security authorities
- "B" – indicates provision primarily in the direction of privacy enhancement and/or less strict law enforcement authority

Disclaimers:

- The "A" and "B" notations are for the purpose of flagging the direction of each item in its own right. There is no suggestion that an eventual package would have an equivalent number of "A"s and "B"s. Items vary in their level of importance, and the overall substantive goal is to draft appropriate provisions, rather than to favor or oppose provisions simply because they are more or less strict.
- The descriptions of categories under "A" and "B" to group items was used in a prior Deputies meeting and there were no objections to using such categories.



U.S. Supreme Court

OLMSTEAD v. U.S., 277 U.S. 438 (1928)

277 U.S. 438

OLMSTEAD et al.
v.
UNITED STATES.
No. 493.

GREEN et al.
v.
SAME

No. 532.

McINNIS
v.
SAME.

No. 533.
Argued Feb. 20 and 21, 1928.
Decided June 4, 1928.

[277 U.S. 438, 439] Mr. John F. Dore, of Seattle, Wash., for petitioners Olmstead and others.

[277 U.S. 438, 441] Mr. Frank R. Jeffrey, of Seattle, Wash., for petitioner McInnis.

[277 U.S. 438, 445] Mr. Arthur E. Griffin, of Seattle, Wash., for petitioners Green and others.

[277 U.S. 438, 447] The Attorney General and Mr. Michael J. Doherty, of St. Paul, Minn., for the United

States.

[277 U.S. 438, 452] Messrs. Charles M. Bracelen, of New York City, Otto B. Rupp. of Seattle, Wash., Clarence B. Randall, of Chicago, Ill., and Robert H. Strahan, of New York City, for Pacific Telephone & Telegraph Co., American Telephone & Telegraph Co., United States Independent Telephone Ass'n and Tri-State Telephone & Telegraph Co., as amici curiae.

[277 U.S. 438, 455]

Mr. Chief Justice TAFT delivered the opinion of the Court.

These cases are here by certiorari from the Circuit Court of Appeals for the Ninth Circuit. 19 F.(2d) 842, 53 A. L. R. 1472, and 19 F.(2d) 850. The petition in No. 493 Was filed August 30, 1927; in Nos. 532 and 533, September 9, 1927. They were granted with the distinct limitation that the hearing should be confined to the single question whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wire tapping, amounted to a violation of the Fourth and Fifth Amendments. 276 U.S. 609, 48 S. Ct. 207, 72 L. Ed. -.

The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act (27 USCA) by unlawfully possessing, transporting and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors. Seventy-two others, in addition to the petitioners, were indicted. Some were not apprehended, some were acquitted, and others pleaded guilty.

The evidence in the records discloses a conspiracy of amazing magnitude to import, possess, and sell liquor un- [277 U.S. 438, 456] lawfully. It involved the employment of not less than 50 persons, of two sea-going vessels for the transportation of liquor to British Columbia, of smaller vessels for coastwise transportation to the state of Washington, the purchase and use of a branch beyond the suburban limits of Seattle, with a large underground cache for storage and a number of smaller caches in that city, the maintenance of a central office manned with operators, and the employment of executives, salesmen, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney. In a bad month sales amounted to $176,000; the aggregate for a year must have exceeded $2,000, 000.

Olmstead was the leading conspirator and the general manager of the business. He made a contribution of $10,000 to the capital; 11 others contributed $1,000 each. The profits were divided, one-half to Olmstead and the remainder to the other 11. Of the several offices in Seattle, the chief one was in a large office building. In this there were three telephones on three different lines. There were telephones in an office of the manager in his own home, at the homes of his associates, and at other places in the city. Communication was had frequently with Vancouver, British Columbia. Times were fixed for the deliveries of the 'stuff' to places along Puget Sound near Seattle, and from there the liquor was removed and deposited in the caches already referred to. One of the chief men was always on duty at the main office to receive orders by the telephones and to direct their filling by a corps of men stationed in another room-the 'bull pen.' The call numbers of the telephones were given to those known to be likely customers. At times the sales amounted to 200 cases of liquor per day.

The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers. Small [277 U.S. 438, 457] wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.

The gathering of evidence continued for many months. Conversations of the conspirators, of which refreshing stenographic notes were currently made, were testified to by the government witnesses. They revealed the large business transactions of the partners and their subordinates. Men at the wires heard the orders given for liquor by customers and the acceptances; they became auditors of the conversations between the partners. All this disclosed the conspiracy charged in the indictment. Many of the

intercepted conversations were not merely reports, but parts of the criminal acts. The evidence also disclosed the difficulties to which the conspirators were subjected, the reported news of the capture of vessels, the arrest of their men, and the seizure of cases of liquor in garages and other places. It showed the dealing by Olmstead, the chief conspirator, with members of the Seattle police, the messages to them which secured the release of arrested members of the conspiracy, and also direct promises to officers of payments as soon as opportunity offered.

The Fourth Amendment provides:

> 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

And the Fifth:

> 'No person ... shall be compelled in any criminal case to be a witness against himself.' [277 U.S. 438, 458] It will be helpful to consider the chief cases in this court which bear upon the construction of these amendments.

Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524, was an information filed by the District Attorney in the federal court in a cause of seizure and forfeiture against 35 cases of plate glass, which charged that the owner and importer, with intent to defraud the revenue, made an entry of the imported merchandise by means of a fraudulent or false invoice. It became important to show the quantity and value of glass contained in 29 cases previously imported. The fifth section of the Act of June 22, 1874 (19 USCA 535), provided that, in cases not criminal under the revenue laws, the United States attorney, whenever he thought an invoice, belonging to the defendant, would tend to prove any allegation made by the United States, might by a written motion, describing the invoice and setting forth the allegation which he expected to prove, secure a notice from the court to the defendant to produce the invoice, and, if the defendant refused to produce it, the allegations stated in the motion should be taken as confessed, but if produced the United States attorney should be permitted, under the direction of the court, to make an examination of the invoice, and might offer the same in evidence. This act had succeeded the act of 1867 (14 Stat. 547), which provided in such cases the District Judge, on affidavit of any person interested, might issue a warrant to the marshall to enter the premises where the invoice was and take possession of it and hold it subject to the order of the judge. This had been preceded by the act of 1863 (12 Stat. 740) of a similar tenor, except that it directed the warrant to the collector instead of the marshal. The United States attorney followed the act of 1874 and compelled the production of the invoice.

The court held the act of 1874 repugnant to the Fourth and Fifth Amendments. As to the Fourth Amendment, Justice Bradley said (page 621 (6 S. Ct. 527)):

[277 U.S. 438, 459] 'But, in regard to the Fourth Amendment, it is contended that, whatever might have been alleged against the constitutionality of the acts of 1863 and 1867, that of 1874, under which the order in the present case was made, is free from constitutional objection, because it does not authorize the search and seziure of books and papers, but only requires the defendant or claimant to produce them. That is so; but it declares that if he does not produce them, the allegations which it is affirmed they will prove shall be taken as confessed. This is tantamount to compelling their production; for the prosecuting attorney will always be sure to state the evidence expected to be derived from them as strongly as the case will admit of. It is true that certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting, and to this extent the proceeding under the act of 1874 is a mitigation of that which was authorized by the former acts; but it accomplishes the substantial object of those acts in forcing from a party evidence against himself. It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution, in all cases in which a search and seizure would be; because it is a material ingredient, and effects the sole object and purpose of search and seizure.'

Concurring, Mr. Justice Miller and Chief Justice Waite said that they did not think the machinery used to get this evidence amounted to a search and seizure, but they agreed that the Fifth Amendment had been violated.

The statute provided an official demand for the production of a paper of document by the defendant, for official search and use as evidence on penalty that by refusal he should be conclusively held to admit the incriminat- [277 U.S. 438, 460] ing character of the document as charged. It was certainly no straining of the language to construe the search and seizure under the Fourth Amendment to include such official procedure.

The next case, and perhaps the most important, is Weeks v. United States, 232 U.S. 383 , 34 S. Ct. 341, L. R. A. 1915B, 834, Ann. Cas. 1815C, 1177, a conviction for using the mails to transmit coupons or tickets in a lottery enterpise. The defendant was arrested by a police officer without a warrant. After his arrest, other police officers and the United States marshal went to his house, got the key from a neighbor, entered the defendant's room, and searched it, and took possession of various papers and articles. Neither the marshal nor the police officers had a search warrant. The defendant filed a petition in court asking the return of all his property. The court ordered the return of everything not pertinent to the charge, but denied return of relevant evidence. After the jury was sworn, the defendant again made objection, and on introduction of the papers contended that the search without warrant was a violation of the Fourth and Fifth Amendments, and they were therefore inadmissible. This court held that such taking of papers by an official of the United States, acting under color of his office, was in violation of the constitutional rights of the defendant, and upon making seasonable application he was entitled to have them restored, and that by permitting their use upon the trial the trial court erred.

The opinion cited with approval language of Mr. Justice Field in Ex parte Jackson, 96 U.S. 727 , 733, saying that the Fourth Amendment as a principle of protection was applicable to sealed letters and packages in the mail, and that, consistently with it, such matter could only be opened and examined upon warrants issued on oath or affirmation particularly describing the thing to be seized.

In Silverthorne Lumber Co. v. United States, 251 U.S. 385 , 40 S. Ct. 182, 24 A. L. R. 1426, the defendants were arrested at their homes and [277 U.S. 438, 461] detained in custody. While so detained, representatives of the government without authority went to the office of their company and seized all the books, papers, and documents found there. An application for return of the things was opposed by the district attorney, who produced a subpoena for certain documents relating to the charge in the indictment then on file. The court said:

> 'Thus the case is not that of knowledge acquired through the wrongful act of a stranger, but it must be assumed that the government planned or at all events ratified the whole performance.'

And it held that the illegal character of the original seizure characterized the entire proceeding and under the Weeks Case the seized papers must be restored.

In Amos v. United States, 255 U.S. 313 , 41 S. Ct. 266, the defendant was convicted of concealing whisky on which the tax had not been paid. At the trial he presented a petition asking that private property seized in a search of his house and store 'within his curtilage' without warrant should be returned. This was denied. A woman, who claimed to be his wife, was told by the revenue officers that they had come to search the premises for violation of the revenue law. She opened the door; they entered and found whisky. Further searches in the house disclosed more. It was held that this action constituted a violation of the Fourth Amendment, and that the denial of the motion to restore the whisky and to exclude the testimony was error.

In Gouled v. United States, 255 U.S. 298 , 41 S. Ct. 261, the facts were these: Gouled and two others were charged with conspiracy to defraud the United States. One pleaded guilty and another was acquitted. Gouled prosecuted error. The matter was presented here on questions propounded by the lower court. The first related to the admission in evidence of a paper surreptitiously taken from the office of the defendant by one acting under the direc- [277 U.S. 438, 462] tion of an officer of the Intelligence Department of the Army of the United States. Gouled was suspected of the crime. A private in the

United States Army, pretending to make a friendly call on him, gained admission to his office, and in his absence, without warrant of any character, seized and carried away several documents. One of these, belonging to Gouled, was delivered to the United States attorney and by him introduced in evidence. When produced it was a surprise to the defendant. He had had no opportunity to make a previous motion to secure a return of it. The paper had no pecuniary value, but was relevant to the issue made on the trial. Admission of the paper was considered a violation of the Fourth Amendment.

Agnello v. United States, 269 U.S. 20 , 46 S. Ct. 4, 51 A. L. R. 409, held that the Fourth and Fifth Amendments were violated by admission in evidence of contraband narcotics found in defendant's house, several blocks distant from the place of arrest, after his arrest and seized there without a warrant. Under such circumstances the seizure could not be justified as incidental to the arrest.

There is no room in the present case for applying the Fifth Amendment, unless the Fourth Amendment was first violated. There was no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the Fourth Amendment.

The striking outcome of the Weeks Case and those which followed it was the sweeping declaration that the Fourth Amendment, although not referring to or limiting the use of evidence in court, really forbade its introduction, if obtained by government officers through a violation of the amendment. Theretofore many had supposed that under the ordinary common-law rules, if the tendered evidence was pertinent, the method of obtaining it was [277 U.S. 438, 463] unimportant. This was held by the Supreme Judicial Court of Massachusetts in Commonwealth v. Dana, 2 Metc. 329, 337. There it was ruled that the only remedy open to a defendant whose rights under a state constitutional equivalent of the Fourth Amendment had been invaded was by suit and judgment for damages, as Lord Camden held in Entick v. Carrington, 19 Howell, State Trials, 1029. Mr. Justice Bradley made effective use of this case in Boyd v. United States. But in the Weeks Case, and those which followed, this court decided with great emphasis and established as the law for the federal courts that the protection of the Fourth Amendment would be much impaired, unless it was held that not only was the official violator of the rights under the amendment subject to action at the suit of the injured defendant, but also that the evidence thereby obtained could not be received.

The well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will. This phase of the misuse of governmental power of compulsion is the emphasis of the opinion of the court in the Boyd Case. This appears, too, in the Weeks Case, in the Silverthorne Case, and in the Amos Case.

Gouled v. United States carried the inhibition against unreasonable searches and seizures to the extreme limit. Its authority is not to be enlarged by implication, and must be confined to the precise state of facts disclosed by the record. A representative of the Intelligence Department of the Army, having by stealth obtained admission to the defendant's office, seized and carried away certain private papers valuable for evidential purposes. This was held an unreasonable search and seizure within the Fourth Amendment. A stealthy entrance in such cir- [277 U.S. 438, 464] cumstances became the equivalent to an entry by force. There was actual entrance into the private quarters of defendant and the taking away of something tangible. Here we have testimony only of voluntary conversations secretly overheard.

The amendment itself shows that the search is to be of material things-the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized.

It is urged that the language of Mr. Justice Field in Ex parte Jackson, already quoted, offers an analogy to the interpretation of the Fourth Amendment in respect of wire tapping. But the analogy fails. The Fourth Amendment may have proper application to a sealed letter in the mail, because of the constitutional provision for the Postoffice Department and the relations between the government and those who pay to secure protection of their sealed letters. See Revised Statutes, 3978 to 3988, whereby Congress monopolizes the carriage of letters and excludes from that business everyone else, and section

3929 (39 USCA 259), which forbids any postmaster or other person to open any letter not addressed to himself. It is plainly within the words of the amendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers of effects. The letter is a paper, an effect, and in the custody of a government that forbids carriage, except under its protection.

The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. [277 U.S. 438, 465] By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place.

The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.

This court, in Carroll v. United States, 267 U.S. 132, 149 , 45 S. Ct. 280, 284 (69 L. Ed. 543, 39 A. L. R. 790), declared:

> 'The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests, as well as the interest and rights of individual citizens.'

Justice Bradley, in the Boyd Case, and Justice Clarke, in the Gouled Case, said that the Fifth Amendment and the Fourth Amendment were to be liberally construed to effect the purpose of the framers of the Constitution in the interest of liberty. But that cannot justify enlargement of the language employed beyond the possible practical meaning of houses, persons, papers, and effects, or so to apply the words search and seizure as to forbid hearing or sight.

Hester v. United States, 265 U.S. 57 , 44 S. Ct. 445, held that the testimony of two officers of the law who trespassed on the defendant's land, concealed themselves 100 yards away from his house, and saw him come out and hand a bottle of whisky to another, was not inadmissible. While there was a trespass, there was no search of person, house, papers, or effects. United States v. Lee, 274 U.S. 559, 563 , 47 S. Ct. 746; Eversole v. State, 106 Tex. Cr. R. 567, 294 S. W. 210.

Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, [277 U.S. 438, 466] and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment. The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.

Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure.

We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

What has been said disposes of the only question that comes within the terms of our order granting certiorari in these cases. But some of our number, departing from that order, have concluded that there is merit in the twofold objection, overruled in both courts below, that evidence obtained through intercepting of telephone messages by a government agents was inadmissible, because the mode of obtaining it was unethical and a misdemeanor under the law of Washington. To avoid any misapprehension of our views of that objection we shall deal with it in both of its phases.

While a territory, the English common law prevailed in Washington, and thus continued after her admission in 1889. The rules of evidence in criminal cases in courts of the United States sitting there consequently are those of the common law. United States v. Reid, 12 How. 361, [277 U.S. 438, 467] 363, 366; Logan v. United States, 144 U.S. 263, 301 , 12 S. Ct. 617; Rosen v. United States, 245 U.S. 467 , 38 S. Ct. 148; Withaup v. United States (C. C. A.) 127 F. 530, 534; Robinson v. United States (C. C. A.) 292 F. 683, 685.

The common-law rule is that the admissibility of evidence is not affected by the illegality of the means by which it was obtained. Professor Greenleaf, in his work on Evidence (volume 1 (12th Ed., by Redfield) 254(a)), says:

> 'It may be mentioned in this place, that though papers and other subjects of evidence may have been illegally taken from the possession of the party against whom they are offered, or otherwise unlawfully obtained, this is no valid objection to their admissibility, if they are pertinent to the issue. The court will not take notice how they were obtained, whether lawfully or unlawfully, nor will it form an issue, to determine that question.'

Mr. Jones, in his work on the same subject, refers to Mr. Greenleaf's statement, and says:

> 'Where there is no violation of a constitutional guaranty, the verity of the above statement is absolute.' Section 2075, note 3, vol. 5.

The rule is supported by many English and American cases cited by Jones in section 2075, note 3, and section 2076, note 6, vol. 5; and by Wigmore, vol. 4, 2183. It is recognized by this court in Adams v. New York, 192 U.S. 585 , 24 S. Ct. 372. The Weeks Case announced an exception to the commonlaw rule by excluding all evidence in the procuring of which government officials took part by methods forbidden by the Fourth and Fifth Amendments. Many state courts do not follow the Weeks Case. People v. Defore, 242 N. Y. 13, 150 N. E. 585. But those who do treat it as an exception to the general common-law rule and required by constitutional limitations. Hughes v. State, 145 Tenn. 544, 551, 566, 238 S. W. 588, 20 A. L. R. 639; State v. Wills, 91 W. Va. 659, 677, 114 S. E. 261, 24 A. L. R. 1398; State v. Slamon, 73 Vt. 212, 214, 215, 50 A. 1097, 87 Am. St. Rep. 711; Gindrat v. People, 138 Ill. 103, 111, 27 N. E. 1085; People v. Castree, 311 Ill. 392, 396, 397, 143 N. E. 112, 32 A. L. R. 357; State v. [277 U.S. 438, 468] Gardner, 77 Mont. 8, 21, 249 P. 574, 52 A. L. R. 454; State v. Fahn, 53 N. D. 203, 210, 205 N. W. 67. The common-law rule must apply in the case at bar.

Nor can we, without the sanction of congressional enactment, subscribe to the suggestion that the courts have a discretion to exclude evidence, the admission of which is not unconstitutional, because unethically secured. This would be at variance with the common-law doctrine generally supported by authority. There is no case that sustains, nor any recognized text-book that gives color to, such a view. Our general experience shows that much evidence has always been receivable, although not obtained by conformity to the highest ethics. The history of criminal trials shows numerous cases of prosecutions of oathbound conspiracies for murder, robbery, and other crimes, where officers of the law have disguished themselves and joined the organizations, taken the oaths, and given themselves every appearance of active members engaged in the promotion of crime for the purpose of securing evidence. Evidence secured by such means has always been received.

A standard which would forbid the reception of evidence, if obtained by other than nice ethical conduct by government officials, would make society suffer and give criminals greater immunity than has been known heretofore. In the absence of controlling legislation by Congress, those who realize the difficulties in bringing offenders to justice may well deem it wise that the exclusion of evidence should be confined to cases where rights under the Constitution would be violated by admitting it.

The statute of Washington, adopted in 1909, provides (Remington Compiled Statutes 1922, 2656(18) that:

> 'Every person ... who shall intercept, read or in any manner interrupt or delay the sending of a

> message over any telegraph or telephone line ... shall be guilty of a misdemeanor.' [277 U.S. 438, 469] This statute does not declare that evidence obtained by such interception shall be inadmissible, and by the common law, already referred to, it would not be. People v. McDonald, 177 App. Div. 806, 165 N. Y. S. 41. Whether the state of Washington may prosecute and punish federal officers violating this law, and those whose messages were intercepted may sue them civilly, is not before us. But clearly a statute, passed 20 years after the admission of the state into the Union, cannot affect the rules of evidence applicable in courts of the United States. Chief Justice Taney, in United States v. Reid, 12 How. 361, 363 (13 L. Ed. 1023), construing the thirty-fourth section of the Judiciary Act (now 28 USCA 77), said:
>
> 'But it could not be supposed, without very plain words to show it, that Congress intended to give to the states the power of prescribing the rules of evidence in trials for offenses against the United States. For this construction would in effect place the criminal jurisprudence of one sovereignty under the control of another.'

See, also, Withaup v. United States (C. C. A.) 127 F. 530, 534.

The judgments of the Circuit Court of Appeals are affirmed. The mandates will go down forthwith under rule 31.

AFFIRMED.

Mr. Justice HOLMES.

My brother BRANDEIS has given this case so exhaustive an examination that I desire to add but a few words. While I do not deny it I am not prepared to say that the penumbra of the Fourth and Fifth Amendments covers the defendant, although I fully agree that courts are apt to err by sticking too closely to the words of a law where those words import a policy that goes beyond them. Gooch v. Oregon Short Line R. R. Co., 258 U.S. 22, 24 , 42 S. Ct. 192. But I think, as Mr. Justice BRANDEIS says, that apart from the Constitution the government ought not to use [277 U.S. 438, 470] evidence obtained and only obtainable by a criminal act. There is no body of precedents by which we are bound, and which confines us to logical deduction from established rules. Therefore we must consider the two objects of desire both of which we cannot have and make up our minds which to choose. It is desirable that criminals should be detected, and to that end that all available evidence should be used. It also is desirable that the government should not itself foster and pay for other crimes, when they are the means by which the evidence is to be obtained. If it pays its officers for having got evidence by crime I do not see why it may not as well pay them for getting it in the same way, and I can attach no importance to protestations of disapproval if it knowingly accepts and pays and announces that in future it will pay for the fruits. We have to choose, and for my part I think it a less evil that some criminals should escape than that the government should play an ignoble part.

For those who agree with me no distinction can be taken between the government as prosecutor and the government as judge. If the existing code does not permit district attorenys to have a hand in such dirty business it does not permit the judge to allow such iniquities to succeed. See Silverthorne Lumber Co. v. United States, 251 U.S. 385 , 40 S. Ct. 182, 24 A. L. R. 1426. And if all that I have said so far be accepted it makes no difference that in this case wire tapping is made a crime by the law of the state, not by the law of the United States. It is true that a state cannot make rules of evidence for courts of the United States, but the state has authority over the conduct in question, and I hardly think that the United States would appear to greater advantage when paying for an odious crime against state law than when inciting to the disregard of its own. I am aware of the often-repeated statement that in a criminal proceeding the court will not take notice of the manner in which papers offered in evidence have been [277 U.S. 438, 471] obtained. But that somewhat rudimentary mode of disposing of the question has been overthrown by Weeks v. United States, 232 U.S. 383 , 34 S. Ct. 341, L. R. A. 1915B, 834, Ann. Cas. 1915C, 1177, and the cases that have followed it. I have said that we are free to choose between two principles of policy. But if we are to confine ourselves to precedent and logic the reason for excluding evidence obtained by violating the Constitution seems to me logically to lead to excluding evidence obtained by a crime of the officers of the law.

Mr. Justice BRANDEIS (dissenting).

The defendants were convicted of conspiring to violate the National Prohibition Act (27 USCA). Before any of the persons now charged had been arrested or indicted, the telephones by means of which they habitually communicated with one another and with others had been tapped by federal officers. To this end, a lineman of long experience in wire tapping was employed, on behalf of the government and at its expense. He tapped eight telephones, some in the homes of the persons charged, some in their offices. Acting on behalf of the government and in their official capacity, at least six other prohibition agents listened over the tapped wires and reported the messages taken. Their operations extended over a period of nearly five months. The typewritten record of the notes of conversations overheard occupies 775 typewritten pages. By objections seasonably made and persistently renewed, the defendants objected to the admission of the evidence obtained by wire tapping, on the ground that the government's wire tapping constituted an unreasonable search and seizure, in violation of the Fourth Amendment, and that the use as evidence of the conversations overheard compelled the defendants to be witnesses against themselves, in violation of the Fifth Amendment.

The government makes no attempt to defend the methods employed by its officers. Indeed, it concedes [277 U.S. 438, 472] that, if wire tapping can be deemed a search and seizure within the Fourth Amendment, such wire tapping as was practiced in the case at bar was an unreasonable search and seizure, and that the evidence thus obtained was inadmissible. But it relies on the language of the amendment, and it claims that the protection given thereby cannot properly be held to include a telephone conversation.

> 'We must never forget,' said Mr. Chief Justice Marshall in McCulloch v. Maryland, 4 Wheat. 316, 407 4 L. Ed. 579, 'that it is a Constitution we are expounding.' Since then this court has repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the fathers could not have dreamed. See Pensacola Telegraph Co. v. Western Union Telegraph Co., 96 U.S. 1, 9; Northern Pacific Ry. Co. v. North Dakota, 250 U.S. 135, 39 S. Ct. 502; Dakota Central Telephone Co. v. South Dakota, 250 U.S. 163, 39 S. Ct. 507, 4 A. L. R. 1623; Brooks v. United States, 267 U.S. 432, 45 S. Ct. 345, 37 A. L. R. 1407. We have likewise held that general limitations on the powers of government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the states from meeting modern conditions by regulations which 'a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive.' Village of Euclid v. Ambler Realty Co., 272 U.S. 365, 387, 47 S. Ct. 114, 118 (71 L. Ed. 303); Buck v. Bell, 274 U.S. 200, 47 S. Ct. 584, 71 L. 1000. Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world. It was with reference to such a clause that this court said in Weems v. United States, 217 U.S. 349, 373, 30 S. Ct. 544, 551 (54 L. Ed. 793, 19 Ann. Cas. 705):
>
> 'Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions [277 U.S. 438, 473] and purposes. Therefore a principal to be vital must be capable of wider application than the mischief which gave it birth. This is peculiarly true of Constitutions. They are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall, 'designed to approach immortality as nearly as human institutions can approach it.' The future is their care and provision for events of good and bad tendencies of which no prophecy can be made. In the application of a Constitution, therefore, our contemplation cannot be only of what has been but of what may be. Under any other rule a Constitution would indeed be as easy of application as it would be deficient in efficacy and power. Its general principles would have little value and be converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality.'

When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken' had been necessarily simple. Force and violence were then the only means known to man by which a

government could directly effect self-incrimination. It could compel the individual to testify-a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life-a seizure effected, if need be, by breaking and entry. Protection against such invasion of 'the sanctities of a man's home and the privacies of life' was provided in the Fourth and Fifth Amendments by specific language. Boyd v. United States, 116 U.S. 616, 630 , 6 S. Ct. 524. But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. [277 U.S. 438, 474] Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. 'That places the liberty of every man in the hands of every petty officer' was said by James Otis of much lesser intrusions than these. 1 To Lord Camden a far slighter intrusion seemed 'subversive of all the comforts of society.' 2 Can it be that the Constitution affords no protection against such invasions of individual security?

A sufficient answer is found in Boyd v. United States, 116 U.S. 616 , 627-630, 6 S. Ct. 524, a case that will be remembered as long as civil liberty lives in the United States. This court there reviewed the history that lay behind the Fourth and Fifth Amendments. We said with reference to Lord Camden's judgment in Entick v. Carrington, 19 Howell's State Trials, 1030:

> 'The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case there before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employe of the sanctities of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal se- [277 U.S. 438, 475] curity, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense-it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence of a crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth Amendments run almost into each other.'3

In Ex parte Jackson, 96 U.S. 727 , it was held that a sealed letter intrusted to the mail is protected by the amendments. The mail is a public service furnished by the government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message. As Judge Rudkin said below:

> 'True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference.'

The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all con- [277 U.S. 438, 476] versations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.

Time and again this court, in giving effect to the principle underlying the Fourth Amendment, has refused to place an unduly literal construction upon it. This was notably illustrated in the Boyd Case itself. Taking language in its ordinary meaning, there is no 'search' or 'seizure' when a defendant is required to produce a document in the orderly process of a court's procedure. 'The right of the people of

be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,' would not be violated, under any ordinary construction of language, by compelling obedience to a subpoena. But this court holds the evidence inadmissible simply because the information leading to the issue of the subpoena has been unlawfully secured. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 40 S. Ct. 182. Literally, there is no 'search' or 'seizure' when a friendly visitor abstracts papers from an office; yet we held in Gouled v. United States, 255 U.S. 298, 41 S. Ct. 261, that evidence so obtained could not be used. No court which looked at the words of the amendment rather than at its underlying purpose would hold, as this court did in Ex parte Jackson, 96 U.S. 727, 733, that its protection extended to letters in the mails. The provision against self-incrimination in the Fifth Amendment has been given an equally broad construction. The language is:

> 'No person ... shall be compelled in any criminal case to be a witness against himself.'

Yet we have held not only that the [277 U.S. 438, 477] protection of the amendment extends to a witness before a grand jury, although he has not been charged with crime (Counselman v. Hitchcock, 142 U.S. 547, 562, 586 S., 12 S. Ct. 195), but that:

> 'It applies alike to civil and criminal proceedings, wherever the answer might tend to subject to criminal responsibility him who gives it. The privilege protects a mere witness as fully as it does one who is also a party defendant.' McCarthy v. Arndstein, 266 U.S. 34, 40, 45 S. Ct. 16, 17 (69 L. Ed. 158).

The narrow language of the Amendment has been consistently construed in the light of its object, 'to insure that a person should not be compelled, when acting as a witness in any investigation, to give testimony which might tend to show that he himself had committed a crime. The privilege is limited to criminal matters, but it is as broad as the mischief against which it seeks to guard.' Counselman v. Hitchcock, supra, page 562 (12 S. Ct. 198).

Decisions of this court applying the principle of the Boyd Case have settled these things. Unjustified search and seizure violates the Fourth Amendment, whatever the character of the paper;4 whether the paper when taken by the federal officers was in the home,5 in an office,6 or elsewhere;7 whether the taking was effected by force,8 by [277 U.S. 438, 478] fraud,9 or in the orderly process of a court's procedure. 10 From these decisions, it follows necessarily that the amendment is violated by the officer's reading the paper without a physical seizure, without his even touching it, and that use, in any criminal proceeding, of the contents of the paper so examined-as where they are testified to by a federal officer who thus saw the document or where, through knowledge so obtained, a copy has been procured elsewhere11-any such use constitutes a violation of the Fifth Amendment.

The protection guaranteed by the amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence [277 U.S. 438, 479] in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

Applying to the Fourth and Fifth Amendments the established rule of construction, the defendants' objections to the evidence obtained by wire tapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding. 12

Independently of the constitutional question, I am of opinion that the judgment should be reversed. By the laws of Washington, wire tapping is a crime. 13 Pierce's [277 U.S. 438, 480] Code 1921, 8976(18). To prove its case, the government was obliged to lay bare the crimes committed by its officers on its behalf. A federal court should not permit such a prosecution to continue. Compare Harkin v. Brundage (No. 117) 276 U.S. 36, 48 S. Ct. 268, decided February 20, 1928

[277 U.S. 438, 481] The situation in the case at bar differs widely from that presented in Burdeau v. McDowell, 256 U.S. 465, 41 S. Ct. 574, 13 A. L. R. 1159. There only a single lot of papers was involved. They had been obtained by a private detective while acting on behalf of a private party, without the knowledge of any federal official, long before any one had thought of instituting a [277 U.S. 438, 482] federal prosecution. Here the evidence obtained by crime was obtained at the government's expense, by its officers, while acting on its behalf; the officers who committed these crimes are the same officers who were charged with the enforcement of the Prohibition Act; the crimes of these officers were committed for the purpose of securing evidence with which to obtain an indictment and to secure a conviction. The evidence so obtained constitutes the warp and woof of the government's case. The aggregate of the government evidence occupies 306 pages of the printed record. More than 210 of them are filled by recitals of the details of the wire tapping and of facts ascertained thereby. 14 There is literally no other evidence of guilt on the part of some of the defendants except that illegally obtained by these officers. As to nearly all the defendants (except those who admitted guilt), the evidence relied upon to secure a conviction consisted mainly of that which these officers had so obtained by violating the state law.

As Judge Rudkin said below (19 F.(2d) 842):

> 'Here we are concerned with neither eavesdroppers nor thieves. Nor are we concerned with the acts of private individuals. ... We are concerned only with the acts of federal agents, whose powers are limited and controlled by the Constitution of the United States.'

The Eighteenth Amendment has not in terms empowered Congress to authorize any one to violate the criminal laws of a state. And Congress has never purported to do so. Compare Maryland v. Soper, 270 U.S. 9, 46 S. Ct. 185. The terms of appointment of federal prohibition agents do not purport to confer upon them authority to violate any criminal law. Their superior officer, the Secretary of the Treasury, has not instructed them to commit [277 U.S. 438, 483] crime on behalf of the United States. It may be assumed that the Attorney General of the United States did not give any such instruction. 15

When these unlawful acts were committed they were crimes only of the officers individually. The government was innocent, in legal contemplation; for no federal official is authorized to commit a crime on its behalf. When the government, having full knowledge, sought, through the Department of Justice, to avail itself of the fruits of these acts in order to accomplish its own ends, it assumed moral responsibility for the officers' crimes. Compare the Paquete Habana, 189 U.S. 453, 465, 23 S. Ct. 593; O'Reilly de Camara v. Brooke, 209 U.S. 45, 52, 28 S. Ct. 439; Dodge v. United States, 272 U.S. 530, 532, 47 S. Ct. 191; Gambino v. United States, 275 U.S. 310, 48 S. Ct. 137, and if this court should permit the government, by means of its officers' crimes, to effect its purpose of punishing the defendants, there would seem to be present all the elements of a ratification. If so, the government itself would become a lawbreaker.

Will this court, by sustaining the judgment below, sanction such conduct on the part of the executive? The governing principle has long been settled. It is that a court will not redress a wrong when he who invokes its aid has unclean hands. 16 The maxim of unclean hands comes [277 U.S. 438, 484] from courts of equity. 17 But the principle prevails also in courts of law. Its common application is in civil actions between private parties. Where the government is the actor, the reasons for applying it are even more persuasive. Where the remedies invoked are those of the criminal law, the reasons are compelling. 18

The door of a court is not barred because the plaintiff has committed a crime. The confirmed criminal is as much entitled to redress as his most virtuous fellow citizen; no record of crime, however long, makes one an outlaw. The court's aid is denied only when he who seeks it has violated the law in connection

with the very transaction as to which he seeks legal redress. 19 Then aid is denied despite the defendant's wrong. It is denied in order to maintain respect for law; in order to promote confidence in the administration of justice; in order to preserve the judicial process from contamination. The rule is one, not of action, but of inaction. It is sometimes [277 U.S. 438, 485] spoken of as a rule of substantive law. But it extends to matters of procedure as well. 20 A defense may be waived. It is waived when not pleaded. But the objection that the plaintiff comes with unclean hands will be taken by the court itself. 21 It will be taken despite the wish to the contrary of all the parties to the litigation. The court protects itself.

Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means-to declare that the government may commit crimes in order to secure the conviction of a private criminal-would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.

Mr. Justice BUTLER (dissenting).

I sincerely regret that I cannot support the opinion and judgments of the court in these cases. [277 U.S. 438, 486] The order allowing the writs of certiorari operated to limit arguments of counsel to the constitutional question. I do not participate in the controversy that has arisen here as to whether the evidence was inadmissible because the mode of obtaining it was unethical and a misdemeanor under state law. I prefer to say nothing concerning those questions because they are not within the jurisdiction taken by the order.

The court is required to construe the provision of the Fourth Amendment that declares:

> 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.'

The Fifth Amendment prevents the use of evidence obtained through searches and seizures in violation of the rights of the accused protected by the Fourth Amendment.

The single question for consideration is this: May the government, consistently with that clause, have its officers whenever they see fit, tap wires, listen to, take down, and report the private messages and conversations transmitted by telephones?

The United States maintains that:

> 'The 'wire tapping' operations of the federal prohibition agents were not a 'search and seizure' in violation of the security of the 'persons, houses, papers and effects' of the petitioners in the constitutional sense or within the intendment of the Fourth Amendment.'

The court, adhering to and reiterating the principles laid down and applied in prior decisions22 construing the search and seizure clause, in substance adopts the contention of the government.

The question at issue depends upon a just appreciation of the facts. [277 U.S. 438, 487] Telephones are used generally for transmission of messages concerning official, social, business and personal affairs including communications that are private and privileged-those between physician and patient, lwayer and client, parent and child, husband and wife. The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission the exclusive use of the wire belongs to the persons served by it. Wire tapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence. As the communications

passed, they were heard and taken down.

In Boyd v. United States, 116 U.S. 616 , 6 S. Ct. 524, there was no 'search or seizure' within the literal or ordinary meaning of the words, nor was Boyd-if these constitutional provisions were read strictly according to the letter-compelled in a 'criminal case' to be a 'witness' against himself. The statute, there held unconstitutional because repugnant to the search and seizure clause, merely authorized judgment for sums claimed by the government on account of revenue if the defendant failed to produce his books, invoices and papers. The principle of that case has been followed, developed and applied in this and many other courts. And it is in harmony with the rule of liberal construction that always has been applied to provisions of the Constitution safeguarding personal rights (Byars v. United States, 273 U.S. 28, 32 , 47 S. Ct. 248), as well as to those granting governmental powers. McCulloch v. Maryland, 4 Wheat. 316, 404, 406, 407, 421; Marbury v. Madison, 1 Cranch, 137, 153, 176; Cohens v. Virginia, 6 Wheat. 264; Myers v. United States, 272 U.S. 52 , 47 S. Ct. 21.

This court has always construed the Constitution in the light of the principles upon which it was founded. [277 U.S. 438, 488] The direct operation or literal meaning of the words used do not measure the purpose or scope of its provisions. Under the principles established and applied by this court, the Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words. That construction is consonant with sound reason and in full accord with the course of decisions since McCulloch v. Maryland. That is the principle directly applied in the Boyd Case.

When the facts in these cases are truly estimated, a fair application of that principle decides the constitutional question in favor of the petitioners. With great deference, I think they should be given a new trial.

Mr. Justice STONE (dissenting).

I concur in the opinions of Mr. Justice HOLMES and Mr. Justice BRANDEIS. I agree also with that of Mr. Justice BUTLER so far as it deals with the merits. The effect of the order granting certiorari was to limit the argument to a single question, but I do not understand that it restrains the court from a consideration of any question which we find to be presented by the record, for, under Judicial Code, 240(a), 28 USCA 347(a), this court determines a case here on certiorari 'with the same power and authority, and with like effect, as if the cause had been brought (here) by unrestricted writ of error or appeal.'

Footnotes

[Footnote 1] Otis' argument against Writs of Assistance. See Tudor, James Otis, p. 66; John Adams' Works, vol. II, p. 524; Minot, Continuation of the History of Massachusetts Bay, vol. II, p. 95.

[Footnote 2] Entick v. Carrington, 19 Howell's State Trials, 1030, 1066.

[Footnote 3] In Interstate Commerce Commission v. Brimson, 154 U.S. 447 , 479, 155 U.S. 3 , 14 S. Ct. 1125, 15 S. Ct. 19, the statement made in the Boyd Case was repeated, and the court quoted the statement of Mr. Justice Field in Re Pacific Railway Commission (C. C.) 32 F. 241, 250: 'Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value.' The Boyd Case has been recently reaffirmed in Silverthorne Lumber Co. v. United States, 251 U.S. 385 , 40 S. Ct. 182, in Gouled v. United States, 255 U.S. 298 , 41 S. Ct. 261, and in Byars v. United States, 273 U.S. 28 , 47 S. Ct. 248.

[Footnote 4] Gouled v. United States, 255 U.S. 298 , 41 S. Ct. 261.

[Footnote 5] Weeks v. United States, 232 U.S. 383 , 34 S. Ct. 341, L. R. A. 1915B, 834, Ann. Cas. 1915C, 1177; Amos v. United States, 255 U.S. 313 , 41 S. Ct. 266; Agnello v. United States, 269 U.S.

20, 46 S. Ct. 4; Byars v. United States, 273 U.S. 28, 47 S. Ct. 248.

[Footnote 6] Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524; Hale v. Henkel, 201 U.S. 43, 70, 26 S. Ct. 370; Silverthorne Lumber Co. v. United States, 251 U.S. 385, 40 S. Ct. 182; Gouled v. United States, 255 U.S. 298, 41 S. Ct. 261; Marron v. United States, 275 U.S. 192, 48 S. Ct. 74.

[Footnote 7] Ex parte Jackson, 96 U.S. 727, 733; Carroll v. United States, 267 U.S. 132, 156, 45 S. Ct. 280, 39 A. L. R. 790; Gambino v. United States, 275 U.S. 310, 48 S. Ct. 137, 52 A. L. R. 1381.

[Footnote 8] Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, L. R. A. 1915B, 834, Ann. Cas. 1915C, 1177; Silverthorne Lumber Co. v. United States, 251 U.S. 385, 40 S. Ct. 182; Amos v. United States, 255 U.S. 313, 41 S. Ct. 266; Carroll v. United States, 267 U.S. 132, 156, 45 S. Ct. 280, 39 A. L. R. 790; Agnello v. United States, 269 U.S. 20, 46 S. Ct. 4; Gambino v. United States, 275 U.S. 310, 48 S. Ct. 137, 52 A. L. R. 1381.

[Footnote 9] Gouled v. United States, 255 U.S. 298, 41 S. Ct. 261.

[Footnote 10] Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524; Hale v. Henkel, 201 U.S. 43, 70, 26 S. Ct. 370. See Gouled v. United States, 255 U.S. 298, 41 S. Ct. 261; Byars v. United States, 273 U.S. 28, 47 S. Ct. 248; Marron v. United States, 275 U.S. 192, 48 S. Ct. 74.

[Footnote 11] Silverthorne Lumber Co. v. United States, 251 U.S. 385, 40 S. Ct. 182. Compare Gouled v. United States, 255 U.S. 298, 307, 41 S. Ct. 261. In Stroud v. United States, 251 U.S. 15, 40 S. Ct. 50, and Hester v. United States, 265 U.S. 57, 44 S. Ct. 445, the letter and articles admitted were not obtained by unlawful search and seizure. They were voluntary disclosures by the defendant. Compare Smith v. United States (C. C. A.) 2 F.(2d) 715; United States v. Lee, 274 U.S. 559, 47 S. Ct. 746.

[Footnote 12] The point is thus stated by counsel for the telephone companies, who have filed a brief as amici curiae: 'Criminals will not escape detection and conviction merely because evidence obtained by tapping wires of a public telephone system is inadmissible. if it should be so held; but, in any event, it is better that a few criminals escape than that the privacies of life of all the people be exposed to the agents of the government, who will act at their own discretion, the honest and the dishonest, unauthorized and unrestrained by the courts. Legislation making wire tapping a crime will not suffice if the courts nevertheless hold the evidence to be lawful.'

[Footnote 13] In the following states it is a criminal offense to intercept a message sent by telegraph and/or telephone: Alabama, Code 1923, 5256; Arizona, Revised Statutes 1913, Penal Code, 692; Arkansas, Crawford & Moses' Digest, 1921, 10246; California, Deering's Penal Code 1927, 640; Colorado, Compiled Laws 1921, 6969; Connecticut, General Statutes 1918, 6292; Idaho, Compiled Statutes 1919, 8574, 8586; Illinois, Revsied Statutes 1927, c. 134, 16; Iowa, Code 1927, 13121; Kansas, Revised Statutes 1923, c. 17, 1908; Michigan Compiled Laws 1915, 15403; Montana, Penal

Code 1921, 11518; Nebraska, Compiled Statutes 1922, 7115; Nevada, Revised Laws 1912, 4608, 6752(18); New York, Consolidated Laws, c. 40, 1423(6); North Dakota, Compiled Laws 1913, 10231; Ohio, Page's General Code 1926, 13402; Oklahoma, Session Laws 1923, c. 46; Oregon, Olson's Laws 1920, 2265; South Dakota, Revised Code 1919, 4312; Tennessee, Shannon's Code 1917, 1839, 1840; Utah, Compiled Laws 1917, 8433; Virginia, Code 1924, 4477(2), (3); Washington, Pierce's Code 1921, 8976(18); Wisconsin, Statutes 1927, 348.37; Wyoming, Compiled Statutes 1920, 7148. Compare State v. Behringer, 19 Ariz. 502, 172 P. 660; State v. Nordskog, 76 Wash. 472, 136 P. 694, 50 L. R. A. (N. S.) 1216.

In the following states it is a criminal offense for a company engaged in the transmission of messages by telegraph and/or telephone, or its employees, or, in many instances, persons conniving with them, to disclose or to assist in the disclosure of any message: Alabama, Code 1923, 5543, 5545; Arizona, Revised Statutes 1913, Penal Code, 621, 623, 691; Arkansas, Crawford & Moses' Digest 1921, 10250; California, Deering's Penal Code 1927, 619, 621, 639, 641; Colorado, Compiled Laws 1921, 6966, 6968, 6970; Connecticut, General Statutes 1918, 6292; Florida, Revised General Statutes 1920, 5754,

5755; Idaho, Compiled Statutes 1919, 8568, 8570; Illinois, Revised Statutes 1927, c. 134, 7, 7a; Indiana, Burns' Revised Statutes 1926, 2862; Iowa, Code 1924, 8305; Louisiana, Acts 1918, c. 134, p. 228; Maine, Revised Statutes 1916, c. 60, 24; Maryland, Bagby's Code 1926, art. 27, 489; Michigan, Compiled Statutes 1915, 15104; Minnesota, General Statutes 1923, 10423, 10424; Mississippi, Hemingway's Code 1927, 1174; Missouri, Revised Statutes 1919, 3605; Montana, Penal Code 1921, 11494; Nebraska, Compiled Statutes 1922, 7088; Nevada, Revised Laws 1912, 4603, 4605, 4609, 4631; New Jersey, Compiled Statutes 1910, p. 5319; New York, Consolidated Laws, c. 40, 552, 553; North Carolina, Consolidated Statutes 1919, 4497, 4498, 4499; North Dakota, Compiled Laws 1913, 10078; Ohio, Page's General Code 1926, 13388, 13419; Oklahoma, Session Laws 1923, c. 46; Oregon, Olson's Laws 1920, 2260, 2262, 2266; Pennsylvania. Statutes 1920, 6306,

6308, 6309; Rhode Island, General Laws, 1923, 6104; South Dakota, Revised Code 1919, 4346, 9801; Tennessee, Shannon's Code 1917, 1837, 1838; Utah, Compiled Laws 1917, 8403, 8405, 8434; Washington, Pierce's Code 1921, 8982, 8983; Wisconsin, Statutes 1927, 348.36.

The Alaska Penal Code, Act of March 3, 1899, c. 429, 30 Stat. 1253, 1278, provides that, 'if any officer, agent, operator, clerk, or employee of any telegraph company, or any other person, shall wilfully divulge to any other person than the party from whom the same was received, or to whom the same was addressed, or his agent or attorney, any message received or sent, or intended to be sent, over any telegraph line, or the contents, substance, purport, effect, or meaning of such message, or any part thereof, ... the person so offending shall be deemed guilty of a misdemeanor, and shall be punished by a fine not to exceed one thousand dollars or imprisonment not to exceed one year, or by both such fine and imprisonment, in the discretion of the court.'

The Act of October 29, 1918, c. 197, 40 Stat. 1017 (Comp. St. 3115 3/4 xx), provided: 'That whoever during the period of governmental operation of the telephone and telegraph systems of the United States ... shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary for operation of the service, tap any telegraph or telephone line, or wilfully interfere with the operation of such telephone and telegraph systems or with the transmission of any telephone or telegraph message, or with the delivery of any such message, or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled to receive the same, shall be fined not exceeding $1,000 or imprisoned for not more than one year, or both.'

The Radio Act of February 23, 1927, c. 169, 27. 44 Stat. 1162, 1172 (47 USCA 107), provides that 'no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted message to any person.'

[Footnote 14] The above figures relate to case No. 493. In Nos. 532, 533, the government evidence fills 278 pages, of which 140 are recitals of the evidence obtained by wire tapping.

[Footnote 15] According to the government's brief, p. 41, 'The Prohibition Unit of the Treasury disclaims it (wire tapping) and the Department of Justice has frowned on it.' See, also, 'Prohibition Enforcement,' 69th Congress, 2d Session, Senate Doc. No. 198, pp. iv, v, 13, 15, referred to committee, January 25, 1927; also same, part 2.

[Footnote 16] See Hannay v. Eve, 3 Cranch, 242, 247; Bank of the United States v. Owens, 2 Pet. 527, 538; Bartle v. Nutt, 4 Pet. 184, 188; Kennett v. Chambers, 14 How. 38, 52; Marshall v. Baltimore & Ohio R. R. Co., 16 How. 314, 334; Tool Co. v. Norris, 2 Wall. 45, 54; The Ouachita Cotton, 6 Wall. 521, 532; Coppell v. Hall, 7 Wall. 542; Forsyth v. Woods, 11 Wall. 484, 486; Hanauer v. Doane, 12 Wall. 342, 349; Trist v. Child, 21 Wall. 441, 448; Meguire v. Corwine, 101 U.S. 108 , 111; Oscanyan v. Arms Co., 103 U.S. 261 ; Irwin v. Williar, 110 U.S. 499, 510 , 4 S. Ct. 160; Woodstock Iron Co. v. Richmond & Danville Extension Co., 129 U.S. 643 , 9 S. Ct. 402; Gibbs v. Consolidated Gas Co., 130 U.S. 396, 411 , 9 S. Ct. 553; Embrey v. Jemison, 131 U.S. 336, 348 , 9 S. Ct. 776; West v. Camden, 135 U.S. 507, 521 , 10 S. Ct. 838; McMullen v. Hoffman, 174 U.S. 639, 654 , 19 S. Ct. 839; Hazelton v. Sheckells, 202 U.S. 71 , 26 S. Ct. 567, 6 Ann. Cas. 217; Crocker v. United States, 240 U.S. 74, 78 , 36 S. Ct. 245. Compare Holman v. Johnson, 1 Cowp. 341.

[Footnote 17] See Creath's Administrator v. Sims, 5 How. 192, 204; Kennett v. Chambers, 14 How. 38, 49; Randall v. Howard, 2 Black, 585, 586; Wheeler v. Sage, 1 Wall. 518, 530; Dent v. Ferguson, 132 U.S. 50, 64 , 10 S. Ct. 13; Pope Manufacturing Co. v. Gormully, 144 U.S. 224, 236 , 12 S. Ct. 632; Miller v. Ammon, 145 U.S. 421, 425 , 12 S. Ct. 884; Hazelton v. Sheckells, 202 U.S. 71, 79 , 26 S. Ct. 567, 6 Ann. Cas. 217. Compare International News Service v. Associated Press, 248 U.S. 215, 245 , 39 S. Ct. 68, 2 A. L. R. 293.

[Footnote 18] Compare State v. Simmons, 39 Kan. 262, 264, 265, 18 P. 177; State v. Miller, 44 Mo. App. 159, 163, 164; In re Robinson, 29 Neb. 135, 45 N. W. 267, 8 L. R. A. 398, 26 Am. St. Rep. 378; Harris v. State, 15 Tex. App. 629, 634, 635, 639.

[Footnote 19] See Armstrong v. Toler, 11 Wheat. 258; Brooks v. Martin, 2 Wall. 70; Planters' Bank v. Union Bank, 16 Wall. 483, 499, 500; Houston & Texas Central R. Co. v. Texas, 177 U.S. 66, 99 , 20 S. Ct. 545; Bothwell v. Buckbee, Mears Co., 275 U.S. 274 , 48 S. Ct. 124.

[Footnote 20] See Lutton v. Benin, 11 Mod. 50; Barlow v. Hall, 2 Anstr. 461; Wells v. Gurney, 8 Barn. & C. 769; Ilsley v. Nichols, 12 Pick. (Mass.) 270, 22 Am. Dec. 425; Carpenter v. Spooner, 4 N. Y. Super. Ct. (N. Y.) 717; Metcalf v. Clark, 41 Barb. (N. Y.) 45; Reed v. Williams, 29 N. J. Law, 385; Hill v. Goodrich, 32 Conn. 588; Townsend v. Smith, 47 Wis. 623, 3 N. W. 439, 32 Am. Rep. 793; Blandin v. Ostrander (C. C. A.) 239 F. 700; Harkin v. Brundage, 276 U.S. 36 , 48 S. Ct. 268.

[Footnote 21] Coppell v. Hall, 7 Wall. 542, 558; Oscanyan v. Arms Co., 103 U.S. 261 , 267; Higgins v. McCrea, 116 U.S. 671, 685 , 6 S. Ct. 557. Compare Evans v. Richardson, 3 Mer. 469; Norman v. Cole, 3 Esp. 253; Northwestern Salt Co. v. Electrolytic Alkali Co., (1913) 3 K. B. 422.

[Footnote 22] Ex parte Jackson, 96 U.S. 727 ; Boyd v. United States, 116 U.S. 616 , 6 S. Ct. 524; Weeks v. United States, 232 U.S. 383 , 34 S. Ct. 341, L. R. A. 1915B, 834, Ann. Cas. 1915C, 1177; Silverthorne Lumber Co. v. United States, 251 U.S. 385 , 40 S. Ct. 182, 24 A. L. R. 1426; Gouled v. United States, 255 U.S. 298 , 41 S. Ct. 261; Amos v. United States, 255 U.S. 313 , 41 S. Ct. 266.