(28411

INTEROFFICE ROUTING AND / OR CARRIER SHEET HQ ASA

MUST REMAIN WITH ATTACHED PAPERS

NUMBER EACH MEMO OR REPLY IN LEFT BORDER PLACE NAME RANK AND TELEPHONE NUMBER BOTTOM OF EACH ACTION DRAW LINE UNDER EACH ACTION

ENTER FILE CLASSIFICATION ADJUTANT _____

TO	FROM	DATE	SUBJECT
AS-20	AS-14	28 Apr 47	Bill S.1019

1. The principal objections that have been raised against S.1019 and its predecessor, S.805, are founded upon fears that the enactment of such legislation would be tantamount to the establishment of a peace-time censorship and might well constitute a serious blow directed against freedom of speech and press. The text of the present bill is intended to be directed specifically against the disclosure of cryptologic information, but it goes far beyond this by making it a crime to publish or divulge "any message, document, writing, note, paper or the contents or meaning thereof" which has at any time been transmitted in code, without getting specific, official permission. Since a great deal of government business is translated by messages in code or cipher, the bill would appear to cover practically all but the most routine State, War or Navy Department business. Hence, it is argued, a bill such as S.1019 - might, if enacted into law, make it possible for officials to use it for self-protection or to further doubtful political ends. The conclusion one reaches is almost inescapable, viz., that the wording of S.1019 is still too broad--in fact, so broad as to preclude any possibility of its being enacted now or in the near future.

2. Another serious objection appears in connection with Section 2 of the bill. This Section is apparently directed against American citizens who have served in foreign armies or navies or have been employed by foreign governments. But it is worded so broadly that it covers non-Americans, too. The question is. how can a U. S. law operate to force a non-U.S. citizen to obtain permission of the Secretary of State, the Secretary of War, and the Secretary of the Navy before divulging certain information? This Section contains an impractical provision and would simply be more or less meaningless.

3. The bill seems to have been drawn up on the theory that only a person who has obtained the information in an official capacity, by virtue of his service in, for, or with the government, can or should be subjected to its provisions. But most of the recent violations of security have been committed by people who have never worked for the government or been in the Army or Navy. They would not be touched by the proposed law.

4. The present bill only takes care of willful leakages, where an intent to disclose information must be present. But in many

TO	FROM	DATE	SUBJECT
AS-20	AS-14	28 Apr 47	Bill S.1019 (continued)

cases, leakage of classified cryptologic information comes from carelessness or indiscretion, because of a failure to realize the real import of the disclosure or to understand the effect it may have on our security. And it seems to me that the latter source of leakage is what we should try to cover as well as the former.

5. The British Official Secrets Act, which apparently works very well (except possibly in the case of "personages" on the highest government level), puts the maintenance of security on a different basis than that of having to obtain authority before making a disclosure. It puts the burden on the individual possessing the information--no matter how he obtained it--and tells him he is responsible for its security. If a person having information in his possession uses it "for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the State," (underlining supplied) or if he "fails to take reasonable care of, or so conducts himself as to endanger the safety of (the material) or information" he is deemed guilty of violating the law. Nowhere does it provide for a proper authority to whom one might apply for permission to disclose. The disclosure having been made, all that is necessary to penalize the one who has made it is to prove that it is or was prejudicial to the safety or interests of the State. The person who makes a disclosure does so at his own risk, and if it turns out to have constituted a violation of security, he can be penalized. That sort of law has plenty of "teeth" in it, yet nobody can say that it sets up a censorship or that there is less freedom of speech or press in Great Britain than in the U.S. because of the Official Secrets Act.

6. Taking a cue from the latter, I have made an attempt to parallel it in the present S.1019, to cover both sources of leakage mentioned in Par. 2 above, and to parallel the severity of the penalty with the classification of the information disclosed--the higher the classification, the more severe the penalty. This has not been an element in any previous bill that I am aware of, but is one that appears reasonable. The attached draft is therefore submitted for such use as may be made of it.

William F. Friedman

WILLIAM F. FRIEDMAN
Chief, Communications Research

2 Incls
1. Copy of S.1019
2. Draft of proposed revision