The Espionage Act Reform Act

Starting in the early 1900s, Congress passed the Espionage Act and several related laws in order to prevent government employees and other individuals entrusted with the government's secrets from selling or revealing that information to our enemies. Today, over 4 million people have an active security clearances because of their work for or with the government. These people have agreed to protect the government's secrets. It is important that they keep their word, and criminal penalties serve as an important deterrent for those who might violate that trust. However, the secrecy laws go far beyond their stated purpose and have been repeatedly abused by the executive branch to chill investigative journalism and to prevent oversight of illegal government surveillance programs by Congress and the Federal Communications Commission.

This bill narrows the Espionage Act and related secrecy statutes to ensure that criminal penalties for revealing government secrets only apply to those entrusted with government secrets. This includes government employees, defense contractors and individuals working in critical infrastructure sectors. The bill also keeps in place criminal penalties for foreign spies, individuals who are working for foreign governments, or those violating another federal law, who conspire, aid, or abet a violation of these secrecy laws. Finally, the bill narrows the theft of government property statute, so that it only applies to tangible things, and not just information. This is already the standard adopted by the 9th circuit.

Every single person convicted, to date, under the Espionage Act could still have been convicted had this bill been the law at the time they were prosecuted.

This bill:

- Protects journalists who solicit, obtain, or publish government secrets from prosecution.
- Ensures that each member of Congress is equally able to receive classified information, including from whistleblowers. Currently, the law criminalizes the disclosure of classified information related to signals intelligence to any member of Congress, unless it is in response to a "lawful demand" from a committee. This puts members in the minority party and those not chairing any committee at a significant disadvantage.
- Ensures that federal courts, inspector generals, the FCC, Federal Trade Commission, and Privacy & Civil Liberties Oversight Board can conduct oversight into privacy abuses.
- Ensures that cybersecurity experts who discover classified government backdoors in encryption algorithms and communications apps used by the public can publish their research without the risk of criminal penalties. It is up to governments to hide their surveillance backdoors; academic researchers and other experts should not face legal risks for discovering them.

Frequently Asked Questions

Q: **How would this bill impact the government's prosecution of Edward Snowden?**

A: This bill would have no impact. The bill leaves in place criminal penalties for current and former government employees and contractors who reveal classified information they obtained through a trusted relationship with the government.

Q: How would this bill impact the government's prosecution of Julian Assange?

A: The government would still be able to prosecute Julian Assange.

Q: What about hackers who break into government systems and steal our secrets?

A: The Espionage Act is not necessary to punish hackers who break into U.S. government systems. Congress included a special espionage offense (U.S.C § 1030(a)(1)) in the Computer Fraud and Abuse Act, which specifically criminalizes this.

Q: How have secrecy laws been abused to stop Congressional oversight of surveillance?

In 1976, the Church Committee revealed the existence of Project SHAMROCK, a 30-year, illegal NSA surveillance program in which the agency obtained copies of Americans' domestic and international telegraph messages.

This public NSA document describes the impact 18 USC 798 had on Congressional oversight:

> Probably the most interesting aspect of this confrontation, from an Agency standpoint, was the lengthy disagreement over whether section 798 precluded any open session and disclosure of information pertaining to NSA. Both Chairman Church and Vice-Chairman Tower (through Senator Goldwater) requested the Congressional Research Service (CRS) to provide a legal opinion on the matter. The American Law Division of the CRS did provide a lengthy opinion which was inconclusive. The **CRS essentially said that section 798 may mean** what NSA maintained it meant, i.e., **that no public disclosure was authorized, and thus the speech and debate clause of the Constitution may not protect individual congressmen from the criminal penalties of section 798**. The committee was extremely divided on the question and voted several times not to conduct an open session. However, the chairman finally did obtain a vote to have a public session, based on an opinion of the Senate Parliamentarian that the Senate rules permitted the committee to decide the question. This action was strongly questioned by the minority members of the committee, with several asserting that the disclosure constituted a violation of law. NSA officials were not required to be present during the disclosure to which NSA objected because the

disclosure was not authorized and they too could have been considered to be subject to the criminal penalties of section 798 had they participated.

Q: How have these secrecy laws prevented independent regulatory agencies from investigating corporate violations of privacy laws?

After the NSA's SHAMROCK program was revealed by the press in 1976, the FCC opened an investigation, as the disclosure to the NSA by the phone companies of customer communications violated federal communications law. As then-FCC Chairman Richard Wiley described below in in an exchange with Congresswoman Bella Abzug at a hearing in 1976, the carriers refused to answer the FCC's questions, citing the secrecy rules in 18 USC 798. Unable to get answers, the FCC then shut down its investigation:

> **Ms. Abzug:** Are you saying that you think the statute bars you from looking into unlawful interceptions, or from even inquiring as to whether there were unlawful interceptions ?
> **Mr. Wiley:** As I tried to say before, when this first came to our attention, which was after the Daily News story, we had never heard of Operation Shamrock in the FCC. We had been told that there was going to be a complaint issued by the paper as a user of communication services. That did not occur. We then went back and filed our own letter with the carriers. They, acting on the advice of the Senate committee — that is the Church committee and the staff of the Senate committee — as they told us, and 798 refused to give us the information. This would have provided us with the basis on which to give these answers.
> **Ms. Abzug:** And you dropped it merely because the corporations refused to give you any information, even though they may have been acting unlawfully within the confines of your general jurisdiction as a regulatory agency? What steps did you take beyond that ?
> **Mr. Wiley:** As I pointed out in my statement, **we didn't go further because of the provisions of 798. If you do not like 798, I would suggest that you change the law, but that is the way the provision reads.**
>
> ...
>
> **Mr. Wiley:** In all candor, I would like to carry out my responsibilities, but I do not know in light of 798 what to do.

Q: How else have these laws been abused?

A: In 1981, NSA learned that journalist James Bamford was writing a book on the history of the agency and had obtained from DOJ through FOIA documents about the NSA, which the NSA did not think DOJ should have released. NSA attempted, unsuccessfully, to pressure the journalist into returning the documents and not publishing the book, including threatening him with prosecution under 18 USC 798.