

F. JAMES SENSENBRENNER, JR.
FIFTH DISTRICT, WISCONSIN
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON
CRIME, TERRORISM, AND
HOMELAND SECURITY
CHAIRMAN
COMMITTEE ON SCIENCE, SPACE,
AND TECHNOLOGY
VICE-CHAIRMAN



Congress of the United States
House of Representatives
Washington, DC 20515-4905
April 23, 2013

WASHINGTON OFFICE:
ROOM 2449
RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4905
202-225-5101
DISTRICT OFFICE:
120 BISHOPS WAY, ROOM 154
BROOKFIELD, WI 53005-6294
262-784-1111
OUTSIDE MILWAUKEE METRO
CALLING AREA:
1-800-242-1119
WEBSITE:
[HTTP://SENSENBRENNER.HOUSE.GOV](http://SENSENBRENNER.HOUSE.GOV)

The Honorable Eric Holder
Attorney General
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530

Dear Attorney General Holder:

As you know, the House Judiciary Committee has been considering updates to the Electronic Communications Privacy Act (ECPA), particularly the included Stored Communications Act (SCA).¹ The SCA permits a “governmental entity” to compel a service provider to disclose the contents of electronic communications in certain circumstances.

The SCA’s compelled-disclosure provisions give different levels of protections based on where an email is held and how long it has been stored. The government can obtain communications without a warrant under the SCA if they are stored with a remote computing service or if they are stored with an electronic service provider for more than 180 days.²

The distinctions the SCA draws are, at best, anachronistic, and I believe, inconsistent with the Fourth Amendment. Fourth Amendment protection attaches when a government search infringes upon “an expectation of privacy that society is prepared to consider reasonable.”³ This expectation reasonably exists for emails regardless of where and how long they are stored. Modern lives are conducted through email accounts. By peering into an individual’s email, the government gains intimate access into every aspect of that person’s life. These are precisely the privacies that the Fourth Amendment was intended to protect.

In *U.S. v. Warshak*, the Sixth Circuit recognized that email has become analogous to a letter or phone call, and therefore, “the government cannot compel a commercial [Internet Service Provider] to turn over the contents of an email without triggering the Fourth Amendment.”⁴

The Department of Justice (DOJ or Department) has indicated some support for this view. At a hearing before the House Judiciary Committee’s Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Elana Tyrangiel, Acting Assistant Attorney General for the Office of Legal Policy, testified:

¹ Store Communications Act, 18 U.S.C. §§ 2701 *et seq.*

² *Id.* at § 2703(a). Under the SCA, “remote computing service[s]” provide “computer storage or processing services” to customers. 18 U.S.C. § 2511(2). “Electronic communication services” permit “users . . . to send or receive electronic communications.” 18 U.S.C. § 2510(15).

³ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

⁴ *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.⁵

While I agree with the Sixth Circuit's decision in *Warshak*, the circuit split it created has engendered uncertainty for Internet service providers who may be faced with subpoenas to produce the contents of email accounts that are valid under the SCA, but inconsistent with the Fourth Amendment under *Warshak*.

I am optimistic that Congress will update ECPA and the SCA to address these inconsistencies. In the meantime, formal guidance from the Department would provide certainty for businesses and individuals. Please respond to the following questions by May 9, 2013:

1. Has DOJ adopted a formal policy to require a warrant to access email communications regardless of whether they have been opened or where they have been sent?
2. If so, when was the policy adopted?
3. Does the Department believe that the Fourth Amendment applies to email communications?

In addition to responding to the above questions, please provide copies of any DOJ guidance or policy statements on obtaining access to email communications.

Sincerely,



F. James Sensenbrenner
Chairman
Subcommittee on Crime, Terrorism, Homeland Security, and Oversight
House Judiciary Committee

⁵ *Testimony before the House Judiciary Committee Subcommittee on Crime, Terrorism, Homeland Security, and Oversight*, Elana Tyrangiel, Acting Assistant Attorney General for the Office of Legal Policy, U.S. Department of Justice (March 19, 2013).