U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515–6216
One Hundred Tenth Congress

Statement of Undersigned Members of the House Judiciary Concerning the Administration's Terrorist Surveillance Program and the Issue of Retroactive Immunity

As a result of our review of classified as well as unclassified materials concerning the Administration's Terrorist Surveillance Program, we have concluded that blanket retroactive immunity for phone companies is not justified.[1] However, we do recommend a course of action that would both permit the carriers the opportunity to defend themselves in court and also protect classified information – by eliminating current legal barriers and authorizing relevant carriers to present fully in court their claims that they are immune from civil liability under current law, with appropriate protections to carefully safeguard classified information. In addition, we recommend legislation to fill a current gap in liability protection for carriers, and to create a bipartisan commission to thoroughly investigate the legality of the warrantless surveillance program.

I. Review of Materials by the House Judiciary Committee

In recent weeks, Judiciary Committee members have received classified briefings from intelligence and Justice Department officials on the Administration's warrantless surveillance program; we have been provided access to the same classified documents on the program that were provided months ago to the Senate Intelligence and Judiciary Committees (and, more recently, to the House Permanent Select Committee on Intelligence); and the Committee has conducted lengthy and extensive classified hearings on February 28 and March 5 to hear testimony from telecom and Administration officials.[2] A key focus of that effort was the issue of

---

[1]Under the proposal supported by the Administration and contained in the Senate FISA bill, participating carriers would receive blanket retroactive immunity from any lawsuit challenging their conduct concerning warrantless surveillance if the Attorney General simply certifies that the company was told in writing that the surveillance was authorized by the President to detect or prevent a terrorist attack and determined by the Administration to be lawful. The immunity would be granted regardless of whether the surveillance was in fact lawful, whether the company exercised due diligence, or whether the company met the criteria for immunity already existing in the law. The court's role would be limited to determining whether the Attorney General had committed an "abuse of discretion."

[2]Shortly after the Administration made some classified information on the warrantless surveillance program available to some Judiciary Committee members, after years of requests,

retroactive immunity for phone companies that participated in the warrantless surveillance program.

II. Findings and Determinations

We have concluded that the Administration has not established a valid and credible case justifying the extraordinary action of Congress enacting blanket retroactive immunity as set forth in the Senate bill. We have reached this conclusion as a result of a number of findings and determinations we made pursuant to our classified briefings, our review of relevant documents, and our classified hearings, as well as our review of publicly available information.

1. Variable Actions by Carriers

The case for blanket retroactive immunity would be stronger if the various carriers had taken consistent actions in response to requests from the Administration. That is not what we found. Without revealing any specific details, we found a variety of actions at various times with differing justifications in response to Administration requests. It is not our place to judge carriers' actions, as we certainly understand the very sensitive and compelling factual context in which these actions took place. Instead, we believe that such determinations are far more properly within the purview of the courts under our system of government.

2. Variable Legal Rules

If there were one simple, straightforward legal rule that applied to the conduct in question, it could perhaps be argued that it is a straightforward matter for the legislature to assess the lawfulness of the conduct in question. Without revealing any specific details, that is not what we found. It appears that a variety of legal rules and regimes may apply to the conduct of the carriers. We would note that one carrier has publicly stated that there are "numerous defenses and immunities reflected in existing statutory and case law" for companies that cooperate with legally authorized government surveillance requests.[3] We would again note that it is not our

---

Chairman Conyers wrote to the White House reiterating previous requests for additional relevant information and requesting that such information be made available to the entire Committee and, to the extent possible, "to the American public via immediate and appropriate declassification." Letter from Chairman Conyers to White House Counsel Fred Fielding (Feb. 12, 2008) at 2. Although the Administration recently agreed to extend access to the full Committee, it has still not provided the additional information requested or agreed to declassify any information. It should be noted that some Members join this statement based on their review of unclassified information.

[3] See Letter from Wayne Watts, Senior Executive Vice President of AT&T to Congressmen John Dingell, Edward Markey, and Bart Stupak (Oct. 12, 2007) ("AT&T letter") at 6. It should be emphasized that by citing this or any other public statements by carriers, we are

place to specify, on an after-the-fact basis, which legal rules apply to which facts. Instead, such analysis is typically the role of the courts, particularly in instances as complex as this.

3. Important Legal Determinations Remain Pending

One of the cornerstone principles of our system of government is that it is the proper role of the courts to resolve factual and legal disputes between parties. The granting of blanket retroactive legal immunity is inconsistent with that principle.

Further, as Members of the Judiciary Committee, we are frequently confronted with requests for private relief. One of the more important principles we apply in reviewing such matters is whether the party seeking relief from Congress has exhausted available legal remedies first. Numerous legal actions have been brought against carriers alleging significant invasions of privacy by their customers. In the lawsuit that has progressed the furthest, the carrier and the government have sought to dismiss the action based primarily on the state secrets privilege. Although the trial court has refused to grant this relief, it is public knowledge that the government and the carrier are appealing the decision.[4] In our view, the fact that such remedies have not been fully exhausted militates against a Congressional grant of retroactive blanket immunity at this time.

4. No Credible Evidence of Irreparable Damage to Carriers

In our view, the arguments for blanket retroactive immunity – that a decision not to enact it will irreparably harm the relevant carriers and that it will endanger our national security – have not been substantiated, either in a public or a classified setting. Without revealing any specific details, the relevant carriers are significant companies that appear capable of dealing with the lawsuits and accusations brought against them. We have seen no indication that in the event these actions were allowed to proceed, either their reputations or their financial viability would be meaningfully impaired. As a matter of fact, it could just as easily be asserted that the carriers could be best served by clearing their names, or that their reputations would suffer greater harm as a result of a legislative enactment of blanket retroactive immunity.

5. No Credible Evidence of Significant Damage to Intelligence Gathering

Without revealing any specific details, we have not seen credible evidence that carriers would refuse to take needed action with respect to intelligence gathering in the future as a result of Congress' decision not to enact blanket retroactive immunity. As good corporate citizens, we

---

neither confirming nor denying whether such company in fact participated in the warrantless surveillance program.

[4] See, e.g., Howard Mintz, "DOJ Faces Showdown over Domestic Spying," Oakland Tribune (Aug. 13, 2007).

would expect no less. This is consistent with a recent report in *The New York Times* that a telecommunications lawyer stated that he had seen "little practical effect on the industry's surveillance operations" since the Protect America Act expired earlier in February and that "most operations appear to have continued unabated."[5] Indeed as noted above, the carriers have many, many paths to avoid such liability, and in many respects, it is premature to consider whether to relieve them of liability, indemnify them, or take other action. We would also note that we have taken care in legislation that has passed already[6] and in proposed future legislation to ensure that relevant carriers receive prospective legal immunity for taking specified actions in response to appropriate government requests.

III. Recommendations

While the information we have seen does not justify retroactive legal immunity, we do believe another option is available that would protect the legitimate interests of carriers in light of the legal framework that already exists. Under current law, carriers that cooperate with government surveillance activities are already entitled to immunity from lawsuit under many circumstances. For example, one statute provides that "no cause of action shall lie in any court" against a carrier that provides the content of telecommunications to the federal government when the company has received a court order or "a certification in writing" by the Attorney General or a designee stating "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required."[7]

However, based on both unclassified and classified information, we have concluded that carriers may be unable to demonstrate their claims to immunity in court under current law because of the state secrets doctrine and related constraints concerning classified information. This is despite our conclusion that the carriers believe these claims to be valid and that at least some may well be upheld by the courts. It is a matter of public record that the U.S. has intervened in pending civil lawsuits against carriers, claiming that they should be dismissed altogether under the state secrets doctrine so that no information relating to the warrantless surveillance program and carriers' participation in it is presented to or revealed in court. That issue is currently pending on appeal.[8] The government has publicly stated that the companies "can't really defend

---

[5] See Eric Lichtblau, "In Wiretap Law's Stead, Uncertainty," New York Times (Feb. 27, 2008).

[6] E.g. 50 U.S.C. 1805(i)(FISA)

[7] 18 U.S.C. 2511 2(a)(ii)(A) and (B).

[8] See Dan Eggen & Ellen Nakashima, "Bush Moves to Shield Telecommunications Firms," Washington Post (March 2, 2008).

themselves, because this is all classified, confidential information."[9] One carrier has publicly stated that when litigation "involves allegations of highly classified intelligence activities, private parties are disabled from making the factual showing necessary to demonstrate that the cases lack legal merit."[10]

Accordingly, we support a resolution that would, notwithstanding the state secrets doctrine, authorize relevant carriers to present fully in court their claims that they are immune from civil liability under current law, with appropriate security protections to carefully safeguard classified information. This solution would ensure that carriers can fully present their arguments that they are immune under current law, while also ensuring that Americans who believe their privacy rights were violated will have the issue considered by the courts based on the applicable facts and law, consistent with our traditional system of government and checks and balances.

Our review has also led us to support two other recommendations. First, there is arguably a gap in liability protections for carriers that complied with lawful surveillance requests covering the time period between the expiration of the Protect America Act and the future enactment of more lasting FISA reform legislation. As Speaker Pelosi and Senate Majority Leader Reid have proposed, legislation to fill that gap is justified and important.[11] This provision is not included in the Senate FISA bill, and should be included in any final legislative product.

In addition, our review of classified information has reinforced serious concerns about the potential illegality of the Administration's actions in authorizing and carrying out its warrantless surveillance program. We, therefore, recommend the creation of a bipartisan commission to conduct hearings and take other evidence to fully examine that program. Like the 9/11 Commission, it would make findings and recommendations in both classified and unclassified reports and thus inform and educate the American people on this troubling subject.

John D. Rockefeller IV

Howard L. Berman

---

[9] See White House Office of the Press Secretary, Background Briefing by Senior Administration Officials on FISA (Feb. 26, 2008) at 11. See also id. at 13 (senior Administration official noting that companies are "precluded from actually litigating them and defending against" civil lawsuits).

[10] AT&T letter at 8.

[11] See Joint Statement by Speaker Nancy Pelosi and Senate Majority Leader Harry Reid on FISA (Feb. 16, 2008).