

FISA Redux – Pass the Bill

James A. Lewis

July 2008

The public debate over FISA in the U.S. has followed the same route as so many other public debates on hard topics: it's been ill informed, driven by extreme views, shaped by partisanship rather than pragmatism and resulted in a second-best outcome that nobody likes. The whispering you hear is people beginning to ask if our government is too broken to work anymore.

Perhaps it's just a passing phase in the history of the Republic, although the phase is entering its second decade. But put that aside for a moment and look at the current FISA bill. It is greeted with hysteria in some quarters, and with calls for Senators and Congresspersons to lie across the tracks to block the FISA train. It is hard to see why. The bill changes very little and the changes it does make are for the better. It takes a collection program started in 2001 – necessary, but probably illegal – and makes it legal. More importantly, it restores a good measure of oversight to communications interception that could apply to U.S. persons.

Surveillance of communications is one of the best tools – perhaps the best tool – in guarding against another surprise attack by terrorists. It is irreplaceable, unless you want to hire thousands of agents and build a domestic intelligence system like that found in Easter Germany before the fall or in China today. Or you could adopt a simple faith-based approach – it could be called the “Bismarck Strategy” - that assumes we need do little or nothing to protect ourselves.¹ Of the three, continued surveillance with oversight is the only serious option.

The sore point in the FISA bill for many critics is retroactive ‘immunity’ for telecom companies (“statutory defenses”). The Administration at first wanted blanket immunity. The compromise was to refer the decision on to grant immunity to a court. Originally, the decision on whether or not the companies had acted illegally (and should be punished) would have been made by the FISC – the Foreign Intelligence Surveillance Court. The final bill, however, now refers the decision to U.S. District Courts.

This was probably a necessary compromise to get a bill, but it means there is some chance that critics of the government can engage in forum shopping. They will avoid the Fourth District (Richmond), famously conservative, and gravitate to the Ninth (San Francisco), famously liberal. The outcome, in any case, will be that whatever court has the final ruling, will be immunity for the Telecom companies.

This is as it should be. If you are driving down the street and a policeman flags you down and asks you to help in an emergency, you are generally immune from liability if you are acting in good faith. You can choose not to help, but that would make you a weasel; it is unfortunate that our society is being driven to outcomes that produce more weasels than Samaritans. The

¹ Otto Von Bismarck, Chancellor of imperial Germany, is alleged to have said in the early 1900s that “There is a special Providence that protects idiots, drunkards, children and the United States of America.”

Telecom companies that cooperated were all contacted by senior officials (such as the Attorney General) shortly after the 911 attacks and asked to help. It is likely that they have classified documents signed by senior officials requesting assistance (these will eventually be produced in court, triggering immunity). And, all other issues fall aside when you consider that they were doing the right thing.

Immunity is not a minor issue. A failure to grant it would increase the risk of terrorist success, by eroding trust between companies and the governments and making future cooperation in detecting terrorist planning more difficult. Libertarians may prefer this outcome, but the real question is whether we can devise a system that allows for necessary surveillance while protecting civil liberties. The FISA bill, for all its faults, does this and immunity is a part of the solution.

There are also worries over 'bulk' monitoring of traffic, as if it was possible to go back to the olden days of copper wire. Bulk monitoring is essential for effective communications surveillance in the new technological environment.

The principle fault with the bill is that it does not do what is needed to adjust oversight and collection to technological change. Telecommunications were much simpler in the 1970s – there were no packets, email, or internet - and it was easy to distinguish between foreign and domestic traffic. This is no longer the case. Domestic traffic can travel over foreign networks and foreign traffic can travel over domestic networks. The old foreign/domestic divide, which we relied on to protect civil liberties, no longer works. The collection problem is how do you wiretap a cloud (CSIS had a closed roundtable on this topic last November) and the answer is that it can be done, but not in a way that is consistent with rules from the 1970s.

This does not mean that the need for rules, oversight and accountability has been diminished or should be thrown overboard in the interests of enabling collection. If anything, the need for oversight has increased. It means that the rules must be different, but coming up with these new rules would have required a difficult discussion of technology and intelligence needs. That discussion was too hard to have in the current political environment, so the bill we have is a stop-gap. It doesn't fix FISA, but it allows it to limp forward, providing both needed surveillance and necessary oversight. This might be the best that can be hoped for.