THE Nation.

Surveillance Bill: The Worst of All Worlds

by **AZIZ HUQ**

June 20, 2008

Months of troubled negotiations over new surveillance legislation ended in the House of Representatives today, with the **approval** of the so-called FISA Amendments Act of 2008. Hailed in some quarters as a "**compromise**" after the capitulation of the Protect America Act of 2006, the new surveillance bill is nothing of the kind: on core issues of privacy and accountability, there is no compromise, since little in the measure honors those two values.

Since the *New York Times*'s revelation of massive illegal surveillance by the NSA, electronic privacy has been a battlefield for claims of executive power and civil liberties. In 2006, the Administration used the shadow of midterm Congressional elections to stampede both Houses into temporary authorization of sweeping new powers in the **Protect America Act** (PAA). The measure's grants of new authority had sunset clauses, which expire either immediately before or after the 2008 elections.
The PAA set the scene for another legislative bait-and-switch: On the cusp of national election contests, the Administration rang alarms of crisis, claiming the nation is losing spying capabilities. Legislators inclined to protect civil liberties weighed their exposure to soft-on-security attacks against their allegiance to constitutional values. Either way--in terms of raw power or partisan advantage--the Administration and its supporters win.

House Democratic leadership agreed to support the measure--seemingly out of fear of losing conservative Democrats to an even **weaker proposal**. But it is the worst of both worlds. It contains just enough of a pretense of accountability to allow the legislators to claim a victory for civil liberties, as it sells out core principles of accountability and privacy.

Begin with accountability. Since the enactment of the PAA, the Administration and its allies have pushed for legislative immunity for the telecommunications companies that aided the NSA's illegal spying from 2001 until 2005. (Those companies are the defendants in multiple suits, presently consolidated before the Ninth Circuit Court of Appeals, challenging their complicity in past illegal wiretapping).

They argue that protection is necessary to ensure future cooperation, even though the telecoms were not deterred by the fact their past actions were clearly in violation of **federal law**.

In fact, immunity is on the White House front burner for wholly different reasons: pending lawsuits against the telecoms are the best opportunity for the American public to learn what kind of illegal surveillance occurred under Bush's watch, and how existing law against warrantless wiretapping was circumvented. As bad as the telecoms will look, the Administration will look worse as more of its cynical and results-oriented reasoning and contempt for constitutional rights is fully aired.

At first blush, the new bill seems to be a fair compromise. Under Section 802, pending lawsuits are not automatically dismissed. They are not even moved to the secretive FISA court, as an earlier proposal would have done. Rather, the district court in each case is required to dismiss a case provided that a

defendant telecom can show that it acted with the "authorization" of the President and also with a certain kind of "written request or directive." The bill then provides an elaborate description of that directive: it can be from the Attorney General, or the head of "an element of the intelligence community" (or from their deputy), and must say simply that the surveillance was determined to be lawful. The bill does not say who must have made this determination.

According to the **a report** in the *Washington Post*, this provision would give courts "the chance to evaluate whether telecommunications companies deserve retroactive protection from lawsuits." But the provision does nothing of the kind. Rather, the court can only look to see if the defendant has the piece of paper described in the law, and if it does, the court must dismiss the case. By interposing a certification requirement, and directing judicial attention to a piece of paper, the bill fends off judicial scrutiny of what in fact occurred.

And there is every reason to believe that the telecom defendants will have the necessary piece of paper. Indeed, there is every reason to believe that the bill has been carefully written to track the precise piece of paper the telecoms have--otherwise, why list both the Attorney General and the heads of intelligence community elements? And why include the weird codicil about the deputies of one but not the other?

House minority whip Roy Blunt of Missouri has **all but confirmed** that the law was drafted to give the pretense of judicial review without the substance: "The lawsuits will be dismissed," Blunt explained, "and we feel comfortable that the standard of evidence that the law requires will be easily met."

The bill, in short, is worse than granting absolute immunity: it is an effort to suborn the legitimacy of the federal courts by having a judge rubber-stamp the dismissal of cases against the telecoms without looking at the substance of what, in fact, was done. It reduces the separation of powers to a check-the-box exercise.

The bill does no better on privacy matters--the question of new surveillance power. Title I of the measure grants the executive branch new surveillance powers for collecting the communications of persons overseas. Although it contains several provisions that purport to shelter Americans' privacy both at home and overseas, these parts of the bill are rendered irrelevant by the grant of sweeping collection authorization.

Under the bill, the government can create new surveillance programs, each lasting a year, that focus on "persons reasonably believed to be located outside the United States." Provided that spying agencies do not "intentionally target" someone "known" to be in the United States, or intend to target "a particular, known person reasonably believed to be in the United States" (and with some other minor caveats), large-scale acquisition of data is permitted.

To be sure, the bill then installs judicial review of such collection efforts--but the courts will not examine the actual surveillance programs, let alone individual cases of surveillance. Again, the bill interposes a certification requirement between the court and the facts.

Specifically, the role of judges is limited to ascertaining whether the Attorney General has completed a certification promising that either he has followed the law, or that he will follow the law soon. If the Attorney General cannot meet even this spectacularly low bar, the bill gives the government time to amend and to re-file the certificate. Something even Alberto Gonzales could manage.

This is a radical break from the FISA regime created in 1978, and risks severe harm to Americans'

privacy interests. The most important break with FISA is the absence of any individualized warrant requirement: it is now whole collection programs that are authorized and reviewed. And the abandonment of discrete, individualized legislative authorization and judicial review is only the first of the bill's troubling features.

The new provisions also allow the government to create sweeping new programs that are formally targeted at overseas persons, but that predictably sweep in large. The provision's loose language about targets--who do not in fact have to be overseas, only reasonably believed to be overseas--gives the government substantial latitude in crafting the parameters of its searches. Past experience gives no cause for confidence on this point. If the bill is enacted, Americans could simply no longer have confidence that calls placed or received from abroad would be private.

Democrats have emphasized new Section 102, which affirms that the act is "the exclusive means" for electronic surveillance for national security ends. But this was the provision in the original FISA that the Bush Administration circumvented. Re-enacting a notional rule that has been flagrantly violated for half a decade, and whose violation continues to be defended and even celebrated, is hardly a victory for civil liberties.

All this is too high a cost in the phony war over privacy. Despite the repeated cries of crisis, there is no verifiable evidence--and nothing at all beyond the self-serving complaints of Bush Administration Cassandras--that the pre-PAA regime under the FISA Act was fundamentally flawed. If the PAA wholly lapses, it is certain that the nation's security will not collapse. When the FISA Amendments Act of 2008 passes the Senate--as it almost certainly will next week--we can be certain that it will be the privacy rights of Americans, and their ability to hold government accountable, that will suffer.

About Aziz Huq

Aziz Huq directs the liberty and national security project at New York University's Brennan Center for Justice. He is co-author of ***Unchecked and Unbalanced: Presidential Power in a Time of Terror*** (New Press, 2007)
He is a 2006 recipient of the Carnegie Scholars Fellowship and has published scholarship in the *Columbia Law Review*, the *Yearbook of Islamic and Middle Eastern Law*, and the New School's *Constellations Journal*. He has also written for *Himal Southasian*, *Legal Times* and the *American Prospect*, and appeared as a commentator on *Democracy Now!* and NPR's *Talk of the Nation*. **more...**