salon.com

http://www.salon.com/opinion/greenwald/2010/09/27/privacy

MONDAY, SEP 27, 2010 06:28 ET

The Obama administration's war on privacy

BY GLENN GREENWALD

GLENN GREENWALD

AP

(updated below - Update II)

In early August, two dictatorial (and U.S.-allied) Gulf states -- Saudi Arabia and the United Arab Emirates -- announced a ban on the use of Blackberries because, as **the *BBC* put it**, "[b]oth nations are unhappy that they are unable to monitor such communications via the handsets." Those two governments demand the power to intercept and monitor every single form of communication. No human interaction may take place beyond their prying ears. Since Blackberry communication data are sent directly to servers in Canada and the company which operates Blackberry -- Research in Motion -- **refused to turn the data over to those governments**, "authorities [] decided to ban Blackberry services rather than continue to allow an uncontrolled and unmonitored flow of electronic information within their borders." That's the core mindset of the Omnipotent Surveillance State: above all else, what is strictly prohibited is the ability of citizens to communicate in private; we can't have any "uncontrolled and unmonitored flow of electronic information."

That controversy generated **substantial coverage in the U.S. media**, which depicted it as reflective of the censorship and all-consuming surveillance powers of those undemocratic states. But the following week, *The New York Times* published **an Op-Ed by Richard Falkenrath** -- a top-level Homeland Security official in the Bush administration and current principal in the private firm of former Bush DHS Secretary Michael Chertoff -- expressing support for the UAE's Blackberry ban. Falkenrath asserted that "[a]mong law enforcement investigators and intelligence officers [in the U.S.], **the Emirates' decision met with approval, admiration and perhaps even a touch of envy**." New Internet technologies -- including voice-over-Internet calls (such as Skype) and text messaging -- are increasingly difficult for governments to monitor, and Falkenrath noted, correctly, that the UAE "is in no way unique in wanting a back door into the telecommunications services used inside its borders to allow officials to eavesdrop on users." The U.S. Government is every bit as eager as the UAE and Saudi Arabia to ensure full and unfettered access to everyone's communications:

> New Internet technologies -- including voice-over-Internet calls (such as Skype) and text messaging -- are increasingly difficult for governments to monitor . . . . Hence the envy some American intelligence officials felt about the Emirates' decision. . . .
>
> Companies can sometimes evade government intrusion for a while. In many cases, governments fail to keep pace with telecommunications innovation; in others, governmental intrusion into ostensibly private communications offends liberal sensibilities.
>
> But in the end, **it is governments, not private industry, that rule the airwaves and the Internet.** The Emirates acted understandably and appropriately: governments should not be

> timid about using their full powers to ensure that their law enforcement and intelligence agencies are able to keep their citizens safe.

The tyrannical mentality of the UAE, Saudi and Bush DHS authorities are far from aberrational. They are perfectly representative of how the current U.S. administration thinks as well: every communication and all other human transactions must be subject to government surveillance. Nothing may be beyond the reach of official spying agencies. There must be no such thing as true privacy from government authorities.

Anyone who thinks that is hyperbole should simply read two articles today describing efforts of the Obama administration to obliterate remaining vestiges of privacy. The first is **this *New York Times* article by Charlie Savage**, which describes how the Obama administration will propose new legislation to mandate that the U.S. Government have access to all forms of communications, "including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype." In other words, the U.S. Government is taking **exactly** the position of the UAE and the Saudis: no communications are permitted to be beyond the surveillance reach of U.S. authorities.

The new law would not expand the Government's legal authority to eavesdrop -- that's unnecessary, since post-9/11 legislation has dramatically expanded those authorities -- but would require all communications, including ones over the Internet, to be built so as to enable the U.S. Government to intercept and monitor them at any time when the law permits. In other words, Internet services could legally exist only insofar as there would be no such thing as truly private communications; all must contain a "back door" to enable government officials to eavesdrop:

> Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone. . . . .
>
> The bill, which the Obama administration plans to submit to lawmakers next year, raises fresh questions about how to balance security needs with protecting privacy and fostering innovation. And because security services around the world face the same problem, it could set an example that is copied globally.
>
> James X. Dempsey, vice president of the Center for Democracy and Technology, an Internet policy group, said the proposal had "huge implications" and **challenged "fundamental elements of the Internet revolution" -- including its decentralized design.**
>
> "They are really asking for the authority to redesign services that take advantage of the unique, and now pervasive, architecture of the Internet," he said. "They basically want to turn back the clock and make Internet services function the way that the telephone system used to function."

In other words, the Obama administration is demanding exactly that which the UAE demanded: full, unfettered access to all communications. Amazingly, the administration had the **temerity to condemn the UAE's ban on Blackberries** on the ground that it impedes "the free flow of information," but in response, the UAE correctly pointed out how hypocritical that condemnation was:

> Yousef Al Otaiba, the UAE Ambassador to the United States, said [State Department spokesman P.J.] Crowley's comments were disappointing and **contradict the U.S. government's own approach to telecommunication regulation.**

> "In fact, the UAE is exercising its sovereign right and is asking for exactly the same regulatory compliance -- and with the same principles of judicial and regulatory oversight -- that Blackberry grants the U.S. and other governments and nothing more," Otaiba said.
>
> "Importantly, the UAE requires the same compliance as the U.S. for the very same reasons: to protect national security and to assist in law enforcement."

And that was before the Obama administration's plan to significantly expand its surveillance capabilities by essentially banning any Internet communications which it cannot monitor.

Then there is **this article in *The Washington Post* this morning**, which reports that "[t]he Obama administration wants to require U.S. banks to report **all electronic money transfers into and out of the country, a dramatic expansion in efforts to counter terrorist financing and money laundering."** Whereas banks are now required to report all such transactions over $10,000 or which are otherwise suspicious, "the new rule would require banks to disclose even the smallest transfers." "The proposal also calls for banks to provide annually the Social Security numbers for all wire-transfer senders and recipients." It would create a centralized database enabling the U.S. Government to monitor **a vastly expanded range of financial transactions engaged in by people who are under no suspicion whatsoever of criminal activity**:

> "This regulation is outrageous," said Peter Djinis, a lawyer who advises financial institutions on complying with financial rules and a former FinCEN executive assistant director for regulatory policy. **"Consider me old-fashioned, but I believe you need to show some evidence of criminality before you are granted unfettered access to the private financial affairs of every individual and company that dares to conduct financial transactions overseas."**

That concept -- that the U.S. Government should not be monitoring, surveilling and collecting data on individuals who are not under criminal investigation -- was once the hallmark of basic American liberty, so uncontroversial as to require no defense. But decades of effective fear-mongering over everything from Communists to drug kingpins -- and particularly the last decade of invoking the all-justifying, Scary mantra of Terrorism -- has reduced much of the American citizenry into a frightened and meek puddle of acquiescence which not only tolerates, but craves, a complete deprivation of privacy. Needless to say, both articles this morning are suffused with quotes from government officials tossing around the standard clichés about Scary Terrorists, Drug Lords, and other cartoon menaces hauled out to justify every expansion of government power and every reduction of individual privacy (that, of course, was the **same rationale invoked by UAE and Saudi officials**: "The UAE issued a statement explaining the decision, saying it had come because 'certain Blackberry services' allow users to avoid 'any legal accountability', raising 'judicial, social and national security concerns'.").

Leave aside the fact that endlessly increasing government surviellance is not only ineffective in detecting Terrorist plots and other crimes, but is **actually counterproductive**, as it swamps the Government with more data than it can possibly process and manage. What these Obama proposals illustrates is just how far we've descended in the security/liberty debate, where only the former consideration has value, while the latter has none. Whereas it was once axiomatic that the Government should not spy on citizens who have done nothing wrong, that belief is now relegated to the civil libertarian fringes. Concerns about privacy were once the predominant consensus of mainstream American political thought. Justice Louis Brandeis famously wrote in dissent in the 1928 **case *Olmstead v. United States*** (emphasis added):

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government,

> **the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men.**

For much of the 20th Century, fears of government surveillance into the private domestic sphere dominated mainstream political debates. To underscore how true that is, consider what **Senator Frank Church (D-Idaho) said** after leading a mid-1970s Senate investigation into the spying abuses of the prior decades and the growing surveillance technologies of the NSA:

> **"That capability at any time could be turned around on the American people," he said in 1975, "and no American would have any privacy left, such is the capability to monitor everything:** telephone conversations, telegrams, it doesn't matter. There would be no place to hide."
>
> He added that if a dictator ever took over, the N.S.A. "could enable it to impose total tyranny, and there would be no way to fight back."

Church's investigation led to many of the intelligence reforms which have been progressively eroded over the last decade (such as FISA). He was a hero to liberals and Democrats generally. But today, people who speak the way he did -- who warn of the dangers of unfettered government surveillance -- are deemed shrill, unSerious paranoids and civil liberties extremists, including by much of the Democratic establishment. That's why we see not the Bush administration -- but a Democratic President -- simultaneously proposing laws that would literally abolish many remaining vestiges of privacy in the communications and finance sectors. The fact that this comes in the wake of **numerous reports** that **law enforcement agencies** repeatedly **abuse their spying powers** makes little difference. Church's warning of "the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide" is exactly what these new laws, copying our Saudi and UAE friends, would enable.

* * * * *

Then again, the GOP Senate nominee in Delaware -- who is almost certain to lose -- is really weird, so we probably shouldn't be talking about any of these surveillance issues lest they distract from what actually matters, and worse, further undermine the paramount Democratic crusade, inspired by *The Wizard of Oz*, to vanquish the scary Wicked Witch.

UPDATE: What makes this trend all the more pernicious is that at exactly the same time that the Government is demanding greater and greater access to what you do and say, it is hiding its own conduct behind an always-higher and more impenetrable wall of secrecy. Everything you do and say must be accessible to them; you can have no secrets from them. But everything they do -- including even criminal acts such as **torture**, **assassinations** and **warrantless surveillance** -- is completely off-limits to you, deemed "state secrets" that not even courts can review in order to determine their legality. This is all driven by Francis Bacon's observation that "knowledge is power": the idea is to make sure that they have full knowledge of what you do (i.e., full power over it), while you have no knowledge about what they do (i.e., no power).

UPDATE II: For those insisting that the Government must have the technological ability to eavesdrop on any and all communications in order to stop Terrorists and criminals, what are you going to do about in-person communications? By this logic, the Government should install eavesdropping devices in all private homes and public spaces, provided they promise only to listen in when the law allows them to do so (I believe there was **a book** written about that once). For those insisting that the Government must have the physical ability to spy on all communications, what objections could one have to such a proposal? We've developed this child-like belief that all Bad Things can be prevented -- we can be

Kept Safe from all dangers -- provided we just vest enough power in the Government to protect us all. What we lose from that mentality, however, is quite vast yet rarely counted. A central value of the Internet was that it was supposed to enable the flow of information free from the surveillance and control of governmental and other authorities.

-- Glenn Greenwald