The Examiner WASHINGTON

'It can't happen here' just did

By: Gene Healy – June 10, 2013

As a Senate candidate in 2003, Barack Obama called the PATRIOT Act "shoddy and dangerous." Once safely in power, Obama started demonstrating his remarkable capacity for "growing in office" -- expanding federal powers while piously moralizing about their potential abuse.

As a senator, he voted to reauthorize the surveillance law in 2006; and as president, signed another PATRIOT renewal from Europe via presidential autopen in 2011.

Sen. Ron Wyden, D-Ore., has long warned of a "secret PATRIOT Act" -- a classified interpretation of the law that allows the administration to undertake massive data collection on American citizens.

Last week, we got a glimpse of what he meant, when a National Security Agency contractor revealed that the agency has assembled a database of at least seven years' worth of Verizon customers' call records -- a practice that apparently extends to other carriers.

"Nobody is listening to your calls," the peevish president said last week; they're "sifting through this so-called metadata," trying to identify potential leads.

About that "metadata": It allows the government secretly to track who a target communicates with and where he's physically located. That knowledge can be used to unearth who's leaking to reporters, when and where political opponents are meeting -- even who's sleeping with whom.

The NSA's massive call-records database is thus a potential treasure trove for bad-faith political actors -- it can be used to ferret out the sort of information that governments have historically used to blackmail and control dissenters.

We needn't resort to hyperbolic examples like the East German Stasi to understand the dangers here -- there's a relevant comparison much closer to home. A series of congressional investigations in the 1970s taught Americans shocking lessons about Cold War-era surveillance abuses.

In 1974, the House Judiciary Committee tasked Deputy Attorney General Laurence Silberman with reviewing former FBI Director J. Edgar Hoover's secret files.

Silberman was revolted by what he found: Hoover had let the bureau "be used by presidents for nakedly political purposes" and engaged in "subtle blackmail to ensure his and the bureau's power."

In his book "The Secrets of the FBI," Ronald Kessler quotes one of the FBI director's former top lieutenants: "The moment [Hoover] would get something on a senator," he'd send an emissary to the Hill to "advise the senator that 'we're in the course of an investigation, and we by chance happened to come up with this data on your daughter. ... Well, Jesus, what does that tell the senator? From that time on, the senator's right in his pocket."

Another congressional investigation by Sen. Frank Church's Select Committee on Intelligence showed massive privacy violations by the NSA.

Under "Project Minaret," from the early 1960s until 1973, the NSA compiled watch lists of potentially subversive Americans, monitored their overseas calls and telegrams, sharing the results with other federal agencies.

Watch-listed Americans "ranged from members of radical political groups, to celebrities, to ordinary citizens involved in protests." Under Project Shamrock, the NSA collected all telegraphic data entering or leaving the United States, "probably the largest government interception program affecting Americans ever undertaken."

In 1976, Church warned that the NSA's technological prowess "at any time could be turned around on the American people ... such is the capability to monitor everything -- telephone conversations, telegrams, it doesn't matter. There would be no place to hide."

Given the state of technology at the time, Church's anxiety seems almost quaint: telegrams? In the surveillance state's infancy, domestic spying was a comparatively low-tech affair; today, with the federal government er, Hoovering up transactional data on millions of Americans, the possibilities are staggering, as is the potential for abuse.

We shouldn't be too sure it "can't happen here" -- after all, it already did.