Keeping the NSA in Perspective

By George Friedman

In June 1942, the bulk of the Japanese fleet sailed to seize the Island of Midway. Had Midway fallen, Pearl Harbor would have been at risk and U.S. submarines, unable to refuel at Midway, would have been much less effective. Most of all, the Japanese wanted to surprise the Americans and draw them into a naval battle they couldn't win.

The Japanese fleet was vast. The Americans had two carriers intact in addition to one that was badly damaged. The United States had only one advantage: It had broken Japan's naval code and thus knew a great deal of the country's battle plan. In large part because of this cryptologic advantage, a handful of American ships devastated the Japanese fleet and changed the balance of power in the Pacific permanently.

This – and the advantage given to the allies by penetrating German codes – taught the Americans about the centrality of communications code breaking. It is reasonable to argue that World War II would have ended much less satisfactorily for the United States had its military not broken German and Japanese codes. Where the Americans had previously been guided to a great extent by Henry Stimson's famous principle that "gentlemen do not read each other's mail," by the end of World War II they were obsessed with stealing and reading all relevant communications.

The National Security Agency evolved out of various post-war organizations charged with this task. In 1951, all of these disparate efforts were organized under the NSA to capture and decrypt communications of other governments around the world – particularly those of the Soviet Union, which was ruled by

Josef Stalin, and of China, which the United States was fighting in 1951. How far the NSA could go in pursuing this was governed only by the extent to which such communications were electronic and the extent to which the NSA could intercept and decrypt them.

The amount of communications other countries sent electronically surged after World War II yet represented only a fraction of their communications. Resources were limited, and given that the primary threat to the United States was posed by nation-states, the NSA focused on state communications. But the principle on which the NSA was founded has remained, and as the world has come to rely more heavily on electronic and digital communication, the scope of the NSA's commission has expanded.

What drove all of this was Pearl Harbor. The United States knew that the Japanese were going to attack. They did not know where or when. The result was disaster. All American strategic thinking during the Cold War was built around Pearl Harbor – the deep fear that the Soviets would launch a first strike that the United States did not know about. The fear of an unforeseen nuclear attack gave the NSA leave to be as aggressive as possible in penetrating not only Soviet codes but also the codes of other nations. You don't know what you don't know, and given the stakes, the United States became obsessed with knowing everything it possibly could.

In order to collect data about nuclear attacks, you must also collect vast amounts of data that have nothing to do with nuclear attacks. The Cold War with the Soviet Union had to do with more than just nuclear exchanges, and the information on what the Soviets were doing – what governments they had penetrated, who was working for them – was a global issue. But you couldn't judge what was important and what was unimportant until after you read it. Thus the mechanics of assuaging fears about a "nuclear Pearl Harbor" rapidly devolved into a global collection system, whereby vast amounts of information were

collected regardless of their pertinence to the Cold War.

There was nothing that was not potentially important, and a highly focused collection strategy could miss vital things. So the focus grew, the technology advanced and the penetration of private communications logically followed. This was not confined to the United States. The Soviet Union, China, the United Kingdom, France, Israel, India and any country with foreign policy interests spent a great deal on collecting electronic information. Much of what was collected on all sides was not read because far more was collected than could possibly be absorbed by the staff. Still, it was collected. It became a vast intrusion mitigated only by inherent inefficiency or the strength of the target's encryption.

Justified Fear

The Pearl Harbor dread declined with the end of the Cold War — until Sept. 11, 2001. In order to understand 9/11's impact, a clear memory of our own fears must be recalled. As individuals, Americans were stunned by 9/11 not only because of its size and daring but also because it was unexpected. Terrorist attacks were not uncommon, but this one raised another question: What comes next? Unlike Timothy McVeigh, it appeared that al Qaeda was capable of other, perhaps greater acts of terrorism. Fear gripped the land. It was a justified fear, and while it resonated across the world, it struck the United States particularly hard.

Part of the fear was that U.S. intelligence had failed again to predict the attack. The public did not know what would come next, nor did it believe that U.S. intelligence had any idea. A federal commission on 9/11 was created to study the defense failure. It charged that the president had ignored warnings. The focus in those days was on intelligence failure. The CIA admitted it lacked the human sources inside al Qaeda. By default the only way to track al Qaeda was via their communications. It was to be the NSA's job.

As we have written, al Qaeda was a global, sparse and dispersed network. It appeared to be tied together by burying itself in a vast new communications network: the Internet. At one point, al Qaeda had communicated by embedding messages in pictures transmitted via the Internet. They appeared to be using free and anonymous Hotmail accounts. To find Japanese communications, you looked in the electronic ether. To find al Qaeda's message, you looked on the Internet.

But with a global, sparse and dispersed network you are looking for at most a few hundred men in the midst of billions of people, and a few dozen messages among hundreds of billions. And given the architecture of the Internet, the messages did not have to originate where the sender was located or be read where the reader was located. It was like looking for a needle in a haystack. The needle can be found only if you are willing to sift the entire haystack. That led to PRISM and other NSA programs.

The mission was to stop any further al Qaeda attacks. The means was to break into their communications and read their plans and orders. To find their plans and orders, it was necessary to examine all communications. The anonymity of the Internet and the uncertainties built into its system meant that any message could be one of a tiny handful of messages. Nothing could be ruled out. Everything was suspect. This was reality, not paranoia.

It also meant that the NSA could not exclude the communications of American citizens because some al Qaeda members were citizens. This was an attack on the civil rights of Americans, but it was not an unprecedented attack. During World War II, the United States imposed postal censorship on military personnel, and the FBI intercepted selected letters sent in the United States and from overseas. The government created a system of voluntary media censorship that was less than voluntary in many ways. Most famously, the United States abrogated the civil rights of citizens of Japanese origin by

seizing property and transporting them to other locations. Members of pro-German organizations were harassed and arrested even prior to Pearl Harbor. Decades earlier, Abraham Lincoln suspended the writ of habeas corpus during the Civil War, effectively allowing the arrest and isolation of citizens without due process.

There are two major differences between the war on terror and the aforementioned wars. First, there was a declaration of war in World War II. Second, there is a provision in the Constitution that allows the president to suspend habeas corpus in the event of a rebellion. The declaration of war imbues the president with certain powers as commander in chief – as does rebellion. Neither of these conditions was put in place to justify NSA programs such as PRISM.

Moreover, partly because of the constitutional basis of the actions and partly because of the nature of the conflicts, World War II and the Civil War had a clear end, a point at which civil rights had to be restored or a process had to be created for their restoration. No such terminal point exists for the war on terror. As was witnessed at the Boston Marathon – and in many instances over the past several centuries – the ease with which improvised explosive devices can be assembled makes it possible for simple terrorist acts to be carried out cheaply and effectively. Some plots might be detectable by intercepting all communications, but obviously the Boston Marathon attack could not be predicted.

The problem with the war on terror is that it has no criteria of success that is potentially obtainable. It defines no level of terrorism that is tolerable but has as its goal the elimination of all terrorism, not just from Islamic sources but from all sources. That is simply never going to happen and therefore, PRISM and its attendant programs will never end. These intrusions, unlike all prior ones, have set a condition for success that is unattainable, and therefore the suspension of civil rights is permanent. Without a constitutional

amendment, formal declaration of war or declaration of a state of emergency, the executive branch has overridden fundamental limits on its powers and protections for citizens.

Since World War II, the constitutional requirements for waging war have fallen by the wayside. President Harry S. Truman used a U.N resolution to justify the Korean War. President Lyndon Johnson justified an extended large-scale war with the Gulf of Tonkin Resolution, equating it to a declaration of war. The conceptual chaos of the war on terror left out any declaration, and it also included North Korea in the axis of evil the United States was fighting against. Former NSA contractor Edward Snowden is charged with aiding an enemy that has never been legally designated. Anyone who might contemplate terrorism is therefore an enemy. The enemy in this case was clear. It was the organization of al Qaeda but since that was not a rigid nation but an evolving group, the definition spread well beyond them to include any person contemplating an infinite number of actions. After all, how do you define terrorism, and how do you distinguish it from crime?

Three thousand people died in the 9/11 attacks, and we know that al Qaeda wished to kill more because it has said that it intended to do so. Al Qaeda and other jihadist movements – and indeed those unaffiliated with Islamic movements – pose threats. Some of their members are American citizens, others are citizens of foreign nations. Preventing these attacks, rather than prosecuting in the aftermath, is important. I do not know enough about PRISM to even try to guess how useful it is.

At the same time, the threat that PRISM is fighting must be kept in perspective. Some terrorist threats are dangerous, but you simply cannot stop every nut who wants to pop off a pipe bomb for a political cause. So the critical question is whether the danger posed by terrorism is sufficient to justify indifference to the spirit of the Constitution, despite the

current state of the law. If it is, then formally declare war or declare a state of emergency. The danger of PRISM and other programs is that the decision to build it was not made after the Congress and the president were required to make a clear finding on war and peace. That was the point where they undermined the Constitution, and the American public is responsible for allowing them to do so.

Defensible Origins, Dangerous Futures

The emergence of programs such as PRISM was not the result of despots seeking to control the world. It had a much more clear, logical and defensible origin in our experiences of war and in legitimate fears of real dangers. The NSA was charged with stopping terrorism, and it devised a plan that was not nearly as secret as some claim. Obviously it was not as effective as hoped, or the Boston Marathon attack wouldn't have happened. If the program was meant to suppress dissent it has certainly failed, as the polls and the media of the past weeks show.

The revelations about PRISM are far from new or interesting in themselves. The NSA was created with a charter to do these things, and given the state of technology it was inevitable that the NSA would be capturing communications around the world. Many leaks prior to Snowden's showed that the NSA was doing this. It would have been more newsworthy if the leak revealed the NSA had not been capturing all communications. But this does give us an opportunity to consider what has happened and to consider whether it is tolerable.

The threat posed by PRISM and other programs is not what has been done with them but rather what could happen if they are permitted to survive. But this is not simply about the United States ending this program. The United States certainly is not the only country with such a program. But a reasonable start is for the country that claims to be most dedicated to its Constitution to adhere to it meticulously above and beyond the

narrowest interpretation. This is not a path without danger. As Benjamin Franklin said, “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.”

“Keeping the NSA in Perspective is republished with permission of Stratfor.”