Offshore

Intelligence Overkill

By Marvin Ott

These days it is easy to forget that prior to World War II, the United States had no government intelligence collection and analysis capability worthy of the name. The American "intelligence community" began with the OSS during the War and then took permanent institutional form with the creation of the Central Intelligence Agency (CIA) in 1947. In 1952, the National Security Agency *was established to exploit intelligence con*tained in electronic communications ("signals intelligence" or SIGINT). NSA soon became the largest of the many agencies engaged in intelligence and also the most secretive. As the contemporary era took shape, electronic data and communications became the lifeblood of national and global commerce, diplomacy and defense. If you did not want others to know what you were planning and doing, you had to protect your data and communications through encryption. This was NSA's world; providing the encryption that could protect official U.S. communications while developing the capability to decode and read the encrypted messages of other governments. This required vast computing power and thousands of mathematicians. SIGINT became a mainstay of the U.S. intelligence community product — provided to U.S. officials to strengthen their capacity to defend U.S. national interests.

The principal targets of America's Cold War intelligence were pretty straightforward; gather and analyze information on the intentions, capabilities and actions of hostile governments. The USSR and the Soviet satellite regimes in Eastern Europe were the main targets for obvious reasons. Other significant targets included China, North Korea and unfriendly regimes in the Middle East. At a time when most communications and data moved by land lines in an analog format, SIGINT was hard to do and effort had to be carefully prioritized. SIGINT was an important but not dominant part of what the intelligence community provided to policymakers. In the 1980s, with improved encryption widely available and with other adverse technological changes, there were many who thought of NSA and SIGINT as wasting assets.

But NSA's golden era was just dawning. A wireless world of digital communications and universal dependence on computers has created what in military parlance would be termed a "target-rich environment." Most of us, including well-informed government officials, did not realize how rich until an NSA contractor decided to release a vast trove of NSA's secret files into the public domain. Over the last month, we have seen a deluge of disclosure concerning what NSA collects and how it does it. The revelations have been stunning. *The New York Times*, in a recent summation, put it well. "From thousands of classified documents, the National Security Agency emerges as an electronic omnivore of staggering capabilities, eavesdropping and hacking its way around the world to strip governments and other targets of their secrets, all the while enforcing the utmost secrecy about its own operations.... The NSA seems to be listening everywhere in the world, gathering every stray electron that might add, however minutely, to the United States government's knowledge of the world.... Its scale and aggressiveness are breathtaking."

Among the revelations, we have learned that the NSA listened in on the personal phones of Germany's chancellor and Brazil's president. Neither Angela Merkel nor Dilma Roussef is pleased. Shortly after President Obama was first elected, he was warned to ditch his ubiquitous Blackberry because NSA (and presumably others) could hack into it. At the other end of the scale, Taliban militants in the remotest corners of Afghanistan also were hacked.

All this has produced, besides an impressive amount of sophisticated reporting in *The Washington Post* and *New York Times*, grist for congressional hearings and op-ed commentaries. The question on the table is what (if anything) should be done about all this. The implications for domestic privacy and law are profound, but outside the purview of this column. At a minimum, Congress will need to draw some very bright lines regarding what the NSA can and cannot do when eavesdropping on Americans. Internationally, the agency has a much freer hand. The issue here is one of prudence and proportion — the application of a common sense test to the use of this capability. If you are with a colleague and friend and you need five dollars, you ask them to loan it to you; you don't pick their pockets to get it.

The problems with NSA's global vacuum cleaner approach are multiple. First, much of this activity risks alienating friends or potential friends for no real reason. If the President wants to know what Merkel is thinking, he can ask her. Second, it was surely inevitable that intelligence collection on this almost incomprehensible scale could not be kept secret indefinitely — particularly when the intelligence community (like the rest of the federal government) relies increasingly on contractors who are more about making money than about public service. Third, the assumption that more data always equals better analysis equals better policy is simply untrue. Vast quantities of data can overwhelm both collectors and analysts. Huge amounts remain undigested and unused. Analysts deluged with minutely detailed information can lose the ability to see the big picture or think beyond conventional wisdom. Too much data can kill analytical and policy creativity. Fourth, NSA's exploitation of the ubiquitous U.S. Internet providers like Google and Yahoo will generate a reaction against them overseas and jeopardize their business as well as the American de facto monopoly of the architecture of the Internet.

Americans can legitimately take pride in NSA's capabilities, but intelligence overkill has a price, and the bill is coming due.

Marvin Ott is a professor at Johns Hopkins University and a Public Policy Scholar at the Woodrow Wilson Center of the Smithsonian Institution. He is a summer resident of Cranberry Isles.