

Will NSA Reforms Protect Citizens?

Exclusive: Common citizens around the world may be alarmed at the NSA's electronic dragnet prying into their personal lives, but reforms may focus mostly on the privacy of government leaders and corporate executives, writes Andrés Cala.

By Andrés Cala

The latest diplomatic tussles triggered by revelations of massive National Security Agency spying, including on U.S. allies and multinational organizations, focus less on intrusions into the privacy of average citizens than on the secrets of the powerful.

Indeed, the debate in Europe illustrates how global leaders are more concerned about the NSA and other intelligence services crossing a red line by intercepting the communications of global leaders, as well as large corporations and powerful institutions, than those of regular citizens. And there are reasons for this selective outrage.

For one thing, European intelligence services appear to have been involved in NSA operations at least in Germany, France, Spain, United Kingdom and Italy, and likely elsewhere. Intelligence experts and some government officials in Spain and the UK say the collaboration is part of information-sharing required by bilateral agreements with the U.S. – and all is legal.

Communications are intercepted either from submarine cables crossing the Atlantic Ocean, beyond the reach of domestic laws, or with judges' approval, these people say. Then part of the data haul is passed on to the NSA because the countries lack the resources to process the millions of exchanges, which in France and Spain yielded 130 million metadata interceptions in just a one-month period.

Metadata includes the identities of senders and recipients, locations and keyword searches, but doesn't involve someone listening in on or reading these intercepted communications. The volume is too massive for such attention, but metadata searching does allow authorities to narrow their search for suspicious activity and that does involve inevitable violations of privacy, such as revealing contacts between individuals.

As revealed by Spain's National Intelligence Center (CNI) during a closed-door parliamentary briefing on NSA activities, massive spying is probably not illegal and is partly the result of cooperation between multiple spy agencies.

Thus, the debate is moving from the legality of what has been done, to what legal reforms might be needed to prevent gross intrusions on personal privacy. That said, much of the recent media-driven uproar has not been over the privacy of common citizens, but over spying on politicians and companies, in other words, industrial and political espionage.

In Europe, the strongest reaction against NSA spying came over reports that German Chancellor Angela Merkel's phone had been hacked. President Barack Obama's spokesman quickly issued an assurance that it won't happen again.

Apparently, the NSA believed that this high-level spying would not be discovered or the agency miscalculated the potential diplomatic fallout, which suggests the U.S. will be more careful going forward about targeting allied leaders.

So, the debate has begun within each NSA-targeted government, especially in Europe, as intelligence chiefs across the Continent explain to policy-makers what former NSA contractor Edward Snowden's revelations mean to them.

It does appear that legal safeguards against industrial and political spying will be introduced in European parliaments. Yet, despite calls for internationally agreed limits to be set, history has taught us that there is little that intelligence agencies won't do to accomplish their objectives.

But the risk to common citizens is that while they may want meaningful protections for their privacy they are likely to get a formalized "legal" process for continuing the spying methods, albeit with closer supervision and stricter regulation. In other words, the secret data-mining likely will continue in the hunt for potential "terrorists."

Each country will define the limitations and methods for spying domestically. Then, European rules will be harmonized to facilitate ongoing intelligence operations. Since the spying will remain covert, citizens will be called on to trust the safeguards without actually knowing how effective they are.

And, surely, intelligence services will continue to use legal loopholes, like tapping into underwater data highways. In the end, one way or another, NSA spying will not only continue as the U.S. government has already said but will get more legal cover from European privacy laws.

Meanwhile, nations around the globe are expanding their own cyber-warfare capabilities in a new kind of arms race, meaning that the U.S. and its closest allies won't be the only ones prying into the behavior, beliefs and associations of common citizens. Among others, Russia, China, Iran, Israel and India are bolstering their capacity for electronic spying.

So, once the public shock has worn off from Snowden's disclosures, the NSA spying debate is likely to boil down to a diplomatic spat between leaders who don't like having their privacy violated, while the privacy rights of their citizens can expect less attention.

However, European countries could up the ante if U.S. violations of European privacy laws end up in European courts with the cases scrutinized by independent judges rather than government officials who have their own stake in spying activities.

Spanish privacy laws are among the strongest in Europe and courts have to authorize any tapping into citizens' communications. That said, authorities have broad powers in matters of national security, and Spaniards, who have been under terrorist threat for decades, broadly accept intrusive measures in exchange for safety.

Spain, which has three intelligence services including the CNI, analogous to the CIA, is credited with having effective counter-terrorism operations, especially in North Africa and inside Spain, staying a step ahead of al-Qaida-linked groups, as well as domestic terrorist organizations.

One result of this successful security system is that terrorism has trended down the list of issues considered the most important by Spaniards, cited by less than 1 percent of poll respondents during 2013, after topping 80 percent in 2000, according to the Center for Sociological Research, an autonomous state polling agency.

Many Spaniards thank the government's spy methods for creating a more secure environment. However, the issue of metadata vacuuming up the personal electronic details of millions of citizens might change those attitudes.

In 2005, a former intelligence official was imprisoned for illegally tapping into communications of politicians, journalists and corporations. A judges' association in Spain asked judicial authorities to investigate the CNI and NSA activities.

But the likely outcome of the uproar over Snowden's disclosures is that European leaders and corporate executives will get new U.S. assurances that targeted efforts against them will be curtailed or abandoned, but the electronic dragnet for "terrorists" – across the vast expanse of everyday communications – will continue.

While new rules will be added, the governments around this brave new world will continue playing the same game.

Andrés Cala is an award-winning Colombian journalist, columnist and analyst specializing in geopolitics and energy. He is the lead author of *America's Blind Spot: Chávez, Energy, and US Security*.
