NSA claims ability to ensure no illegal spying (Update)

June 9 2013, by Associated Press

In this Sept. 23, 2010, file photo Army Gen. Keith B. Alexander, then-commander of the U.S. Cyber Command, testifies about cyberspace operations during a hearing on Capitol Hill in Washington. "More times than we can count, we've made history, without history even knowing we were there," reads a quote on the National Security Agency's web page by current NSA director Alexander. The NSA's experts include mathematicians, and cryptologists, who do everything from breaking codes to learning and translating multiple foreign languages, as well as computer hackers who engage in offensive attacks. (AP Photo/Manuel Balce Ceneta, File)

The supersecret agency with the power and legal authority to gather electronic communications worldwide to hunt U.S. adversaries says it has the technical know-how to ensure it's not illegally spying on Americans.

But mistakes do happen in data-sifting conducted mostly by machines, not humans. Sometimes, former intelligence officials say, that means intelligence agencies destroy material they should not have seen, passed to them by the National Security Agency.

The eavesdropping, code-breaking agency is fighting back after last week's revelations in the media of two surveillance programs that have raised privacy concerns.

One program collects hundreds of millions of U.S. phone records. The second gathers audio, video, email, photographic and Internet search usage of foreign nationals overseas, and probably some Americans in the process, who use major providers such as Microsoft, Google, Apple, and Yahoo.

The programs were first reported in a series of articles published by The Guardian newspaper. On Sunday it identified Edward Snowden, a 29-year-old American who works as contract employee at the NSA, as the source of the disclosures. The newspaper said it was publishing the identity of Snowden, a former technical assistant for the CIA and current employee of defense contractor Booz Allen Hamilton, at his request.

"I have no intention of hiding who I am because I know I have done nothing wrong," he was quoted as saying.

The NSA filed a criminal report with the Justice Department earlier this

week in relation to the leaks. The director of national intelligence, James Clapper, has stated repeatedly that the NSA's programs do not target U.S. citizens and that the agency uses a process known as "minimization" to sift out data from "any U.S. persons whose communications might be incidentally intercepted."

His statement Saturday said that "the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence ... is evidence of a crime or indicates a threat of death or serious bodily harm."

While the NSA has deferred any public comment to Clapper, it did offer an internal article written by director of compliance John DeLong, who is in charge of making sure the NSA protects Americans' privacy.

DeLong writes that privacy protections are being written into the technology that sifts the information, "which allows us to augment—not wholly replace—human safeguards."

The NSA also uses "technology to record and review our activities. ... Sometimes, where appropriate, we even embed legal and policy guidance directly into our IT architecture."

What that means is that the data sifting is mostly done not by humans, but by computers, following complicated algorithms telling them what to look for and who has a right to see it, according to Ronald Marks, a former CIA official.

"Through software, you can search for key words and key phrases linking a communication to a particular group or individual that would fire it off to individual agencies that have interest in it," just like Amazon or Google scans millions of emails and purchases to track consumer preferences, explained Marks, author of "Spying in America

in the Post 9/11 World."

Detailed algorithms try to determine whether something is U.S. citizen-related or not. "It shows analysts, 'we've got a U.S. citizen here, so we've got to be careful with it,'" he said.

But the process isn't perfect, and sometimes what should be private information reaches agencies not authorized to see it.

In that case, there are policies in place to "destroy that kind of information not file it or keep it if an American's name coincidentally or serendipitously comes up," John Negroponte, the first director of national intelligence, said in an Associated Press interview Friday.

Marks said that "when information gets sent to the CIA that shouldn't, it gets destroyed, and a note sent back to NSA saying, 'You shouldn't have sent that.'" He added, "Mistakes get made, but my own experience on the inside of it is, they tend to be really careful about it."

Michael Hayden, who led both the NSA and CIA, said the government doesn't touch the phone records unless an individual is connected to terrorism.

He described on "Fox News Sunday" how it works if a U.S. intelligence agent seized a cellphone at a terrorist hideout in Pakistan.

"It's the first time you've ever had that cellphone number. You know it's related to terrorism because of the pocket litter you've gotten in that operation," Hayden said. "You simply ask that database, 'Hey, any of you phone numbers in there ever talked to this phone number in Waziristan?'"

Hayden said the Obama administration had expanded the scope of the

surveillance, but that oversight by lawmakers and the Foreign Intelligence Surveillance Court also had grown because of changes in the law.

U.S. lawmakers who appeared on the Sunday television talk shows argued the pros and cons of the surveillance programs.

The head of the Senate Intelligence Committee, Democrat Dianne Feinstein, told ABC that the phone program had helped disrupt a 2009 plot to bomb New York City's subways and played a role in the case against an American who scouted targets in Mumbai, India, before a deadly terrorist attack there in 2008.

Democratic Sen. Mark Udall said on CNN that he was not "convinced that the collection of this vast trove of data has led to disruption of plots" against the U.S. He also said he expects "the government to protect my privacy, and it feels like that isn't what's been happening."

The NSA was founded in 1952, but only years later was it publicly acknowledged, which explains the nickname, "No Such Agency."

The agency also includes the Central Security Service, the military arm of code-breakers who work jointly with the agency. Their tightly guarded compound requires the highest of clearances to enter and is equipped with electronic means to ward off an attack by hackers.

Other NSA facilities in Georgia, Texas, Colorado and Hawaii duplicate much of the headquarters' brain and computer power in case a terrorist attack takes out the main location, though each focuses on a different part of the globe.

A new million-square-foot (90,000-square-meter) storage facility in Utah will give the agency untold additional capacity to store the massive

amounts of data it collects, as well as adding to its analytical capability.

"NSA is the elephant of the U.S. intelligence community, the biggest organization by far with the most capability and (literally) the most memory," said former senior CIA official Bruce Riedel, who now runs the Brookings Intelligence Project.

NSA's experts include mathematicians and cryptologists, a term that means everything from breaking codes to learning and translating multiple foreign languages. There also are computer hackers who engage in offensive attacks like the one the U.S. and Israel are widely believed to have been part of, planting the Stuxnet virus into Iranian nuclear hardware, damaging Iran's nuclear development program in 2010.

NSA workers are notoriously secretive. They're known for keeping their families in the dark about what they do, including their hunt for terrorist mastermind Osama bin Laden. NSA code-breakers were an essential part of the team that tracked down bin Laden at a compound in Pakistan in 2011.

Their mission tracking al-Qaida and related terrorist groups continues, with NSA analysts and operators sent out to every conflict zone and overseas U.S. post, in addition to surveillance and analysis conducted at headquarters outside Washington.