# US looks at ways to prevent spying on its spying (Update)

January 27 2014, by Stephen Braun

In this Jan. 23, 2014 file photo, President Barack Obama speaks in the East Room of the White House in Washington. The U.S. government is looking at ways to prevent anyone from spying on its own surveillance of Americans' phone records. As the Obama administration considers shifting the collection of Americans' phone records from the National Security Agency to requiring that they be stored at phone companies or elsewhere, it's quietly funding research that would allow it to search the information using encryption so that phone company employees or eavesdroppers couldn't see who the U.S. is spying on, The Associated Press has learned. (AP Photo/Carolyn Kaster, File)

The U.S. government is looking at ways to prevent anyone from spying on its own surveillance of Americans' phone records.

As the Obama administration considers shifting the collection of those records from the National Security Agency to requiring that they be stored at phone companies or elsewhere, it is quietly funding research to prevent phone company employees or eavesdroppers from seeing whom the U.S. is spying on, The Associated Press has learned.

The Office of the Director of National Intelligence has paid at least five research teams across America to develop a system for high-volume, encrypted searches of electronic records kept outside the government's possession. The project is among several ideas that would allow the government to discontinue storing Americans' phone records, but still search them as needed.

Under the research, U.S. data mining would be shielded by secret coding that could conceal identifying details from outsiders and even the owners of the targeted databases, according to public documents obtained by The Associated Press and AP interviews with researchers, corporate executives and government officials.

In other developments Monday:

—The Justice Department and leading Internet companies agreed to a compromise with the government that would allow the firms to reveal how often they are ordered to turn over information about their customers in national security investigations. The deal with Google Inc., Microsoft Corp., Yahoo Inc., Facebook Inc. and LinkedIn Corp. would provide public information in general terms. Other technology companies were also expected to participate.

—Published reports said new documents leaked by former NSA

contactor Edward Snowden suggest that popular mapping, gaming and social networking apps on smartphones can feed the NSA and Britain's GCHQ eavesdropping agency with personal data, including location information and details such as political affiliation or sexual orientation. The reports, published by The New York Times, the Guardian and ProPublica, said the intelligence agencies get routine access to data generated by apps such as the Angry Birds game franchise or the Google Maps navigation service.

—When the New York Times published a censored U.S. document on the smartphone surveillance program, computer experts said they were able to extract what appeared to be the name of an NSA employee, a Middle Eastern terror group the program was targeting and details about the types of computer files the NSA found useful. Since Snowden began leaking documents in June, his supporters have maintained they have been careful not to disclose any agent's identity or operational details that would compromise ongoing surveillance. The employee did not return phone or email messages from the AP. A DNI spokesman said they asked the Times to redact, or black out, the material. A Times spokeswoman blamed a "production error" and said the section was redacted.

—NBC News reported that British cyber spies demonstrated a pilot program to their U.S. partners in 2012 in which they were able to monitor YouTube in real time and collect addresses from the billions of videos watched daily, as well as some user information, for analysis. At the time the documents were printed, they were also able to spy on Facebook and Twitter. The network said the monitoring program was called "Squeaky Dolphin."

Under pressure, the administration has provided only vague descriptions about changes it is considering to the NSA's daily collection and storage of Americans' phone records, which are presently kept in NSA

databanks. To resolve legal, privacy and civil liberties concerns, President Barack Obama this month ordered the attorney general and senior intelligence officials to recommend changes by March 28 that would allow the U.S. to identify suspected terrorists' phone calls without the government holding the phone records itself.

One federal review panel urged Obama to order phone companies or an unspecified third party to store the records; another panel said collecting the phone records was illegal and ineffective and urged Obama to abandon the program entirely.

Internal documents describing the Security and Privacy Assurance Research project do not cite the NSA or its phone surveillance program. But if the project were to prove successful, its encrypted search technology could pave the way for the government to shift storage of the records from NSA computers to either phone companies or a third-party organization.

A DNI spokesman, Michael Birmingham, confirmed that the research was relevant to the NSA's phone records program. He cited "interest throughout the intelligence community" but cautioned that it may be some time before the technology is used.

The intelligence director's office is by law exempt from disclosing detailed budget figures, so it's unclear how much money the government has spent on the SPAR project, which is overseen by the DNI's Intelligence Advanced Research Projects Activity office. Birmingham said the research is aimed for use in a "situation where a large sensitive data set is held by one party which another seeks to query, preserving privacy and enforcing access policies."

A Columbia University computer sciences expert who heads one of the DNI-funded teams, Steven M. Bellovin, estimates the government could

start conducting encrypted searches within the next year or two.

"If the NSA wanted to deploy something like this it would take one to two years to get the hardware and software in place to start collecting data this way either from phone companies or whatever other entity they decide on," said Bellovin, who is also a former chief technologist for the Federal Trade Commission.

The NSA's surveillance program collects millions of Americans' daily calling records into a central agency database. When the agency wants to review telephone traffic associated with a suspected terrorist—the agency made 300 such queries in 2012—it then searches that data bank and retrieves matching calling records and stores them separately for further analysis.

Using a "three-hop" method that allows the NSA to pull in records from three widening tiers of phone contacts, the agency could collect the phone records of up to 2.5 million Americans during each single query. Obama this month imposed a limit of "two hops," or scrutinizing phone calls that are two steps removed from a number associated with a terrorist organization, instead of the current three.

An encrypted search system would permit the NSA to shift storage of phone records to either phone providers or a third party, and conduct secure searches remotely through their databases. The coding could shield both the extracted metadata and identities of those conducting the searches, Bellovin said. The government could use encrypted searches to ensure its analysts were not leaking information or abusing anyone's privacy during their data searches. And the technique could also be used by the NSA to securely search out and retrieve Internet metadata, such as emails and other electronic records.

Some computer science experts are less sanguine about the prospects for

encrypted search techniques. Searches could bog down because of the encryption computations needed, said Daniel Weitzner, principal research scientist at MIT's Computer Science and Artificial Intelligence Laboratory and former deputy U.S. chief technology officer for the Obama administration.

"There's no silver bullet that guarantees the intelligence community will only have access to the records they're supposed to have access to," Weitzner said. "We also need oversight of the actual use of the data."

Intelligence officials worry that phone records stored outside the government could take longer to search and could be vulnerable to hackers or other security threats. The former NSA deputy director, John Inglis, told Congress last year that privacy—both for the agency and for Americans' whose records were collected—is a prime consideration in the agency's preference to store the phone data itself.

The encrypted search techniques could make it more difficult for hackers to access the phone records and could prevent phone companies from knowing which records the government was searching.

"It would remove one of the big objections to having the phone companies hold the data," Bellovin said.

Similar research is underway by researchers at University of California at Irvine; a group from the University of Wisconsin-Madison and the University of Texas at Austin; another group from MIT, Yale and Rensselaer Polytechnic Institute; and a fourth from Stealth Software Technologies, a Los Angeles-based technology company.