Intelligence chief defends Internet spying program

JIM KUHNHENN LARA JAKES, Associated Press

WASHINGTON (AP) — Eager to quell a domestic furor over U.S. spying, the nation's top intelligence official stressed Saturday that a previously undisclosed program for tapping into Internet usage is authorized by Congress, falls under strict supervision of a secret court and cannot intentionally target a U.S. citizen. He decried the revelation of that and another intelligence-gathering program as reckless.

For the second time in three days, Director of National Intelligence James Clapper took the rare step of declassifying some details of an intelligence program to respond to media reports about counterterrorism techniques employed by the government.

"Disclosing information about the specific methods the government uses to collect communications can obviously give our enemies a 'playbook' of how to avoid detection," he said in a statement.

Clapper said the data collection under the program, first unveiled by the newspapers The Washington Post and The Guardian, was with the approval of the secret Foreign Intelligence Surveillance Act Court and with the knowledge of

Internet service providers. He emphasized that the government does not act unilaterally to obtain that data from the servers of those providers.

The National Security Agency filed a criminal report with the Justice Department earlier this week in relation to the leaks, Shawn Turner, a spokesman for the Office of the Director of National Intelligence, said in an email Saturday to The Associated Press.

President Barack Obama defended the counterterrorism methods on Friday and said Americans need to "make some choices" in balancing privacy and security. But the president's response and Clapper's unusual public stance underscore the nerve touched by the disclosures and the sensitivity of the Obama administration to any suggestion that it is trampling on the civil liberties of Americans.

Late Thursday, Clapper declassified some details of a phone records collection program employed by the NSA that aims to obtain from phone companies on an "ongoing, daily basis" the records of its customers' calls. Clapper said that under that court-supervised program, only a small fraction of the records collected ever get examined because most are unrelated to any inquiries into terrorism activities.

His statement and declassification Saturday addressed the Internet scouring program, code-named PRISM, that allowed the NSA and FBI to tap directly into the servers of major U.S. Internet companies such as Google, Apple, Microsoft, Facebook and AOL. Like the phone-records program, PRISM was approved by a judge in a secret court order. Unlike that program, however, PRISM allowed the government to seize actual conversations: emails, video chats, instant messages and more.

Clapper said the program, authorized in the USA Patriot Act, has been in place since 2008, the last year of the George W. Bush administration, and "has proven vital to keeping the nation and our allies safe.

"It continues to be one of our most important tools for the protection of the nation's security," he said.

Among the previously classified information about the Internet data collection that Clapper revealed:

—It is an internal government computer system that allows the government to collect foreign intelligence information from electronic communication service providers under court supervision.

—The government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. It requires approval from a FISA Court judge and is conducted with the knowledge of the provider and service providers supply information when they are legally required to do so.

—The program seeks foreign intelligence information concerning foreign targets located outside the United States.

—The government cannot target anyone under the program unless there is an "appropriate, and documented, foreign intelligence purpose" for the acquisition. Those purposes include prevention of terrorism, hostile cyber activities or nuclear proliferation. The foreign target must be reasonably believed to be outside the United States. It cannot intentionally target any U.S. citizen or any person known to be in the U.S.

—The dissemination of information "incidentally intercepted" about a U.S. person is prohibited unless it is "necessary to understand foreign intelligence or assess its importance, is evidence of a crime, or indicates a threat of death or serious bodily harm.

The Post and the Guardian cited confidential slides and other documents about PRISM for their reports. They named Google, Facebook, Microsoft Corp., Apple Inc., Yahoo Inc., AOL Inc. and Paltalk as companies whose data has been obtained.

All the companies have issued statements asserting that they aren't voluntarily handing over user data. They also are emphatically rejecting newspaper reports indicating that PRISM has opened a door for the NSA to tap directly on the companies' data centers whenever the government pleases.

In his statement, Clapper appeared to support that claim by stressing that the government did not act unilaterally, but with court authority.

The Guardian reported Saturday that it had obtained top-secret documents detailing an NSA tool, called Boundless Informant, that maps the information it collects from computer and telephone networks by country. The paper said the documents show NSA collected almost 3 billion pieces of intelligence from U.S. computer networks over a 30-day period ending in March, which the paper says calls into question NSA statements that it cannot determine how many Americans may be accidentally included in its computer surveillance.

NSA spokesperson Judith Emmel said Saturday that "current technology simply does not permit us to positively identify all of the persons or locations associated with a given communication." She said it may be possible to determine that a communication "traversed a particular path within the Internet," but added that "it is harder to know the ultimate source or destination, or more particularly the identity of the person represented by the TO:, FROM: or CC: field of an e-mail address or the abstraction of an IP address."

Emmel said communications are filtered both by automated processes and NSA staff to make sure Americans' privacy is respected.

"This is not just our judgment, but that of the relevant inspectors general, who have also reported this," she said.

Amid unsettling reports of government spying, Obama assured the nation Friday that "nobody is listening to your telephone calls. What the government is doing, he

said, is digesting phone numbers and the durations of calls, seeking links that might "identify potential leads with respect to folks who might engage in terrorism."

While Obama on Friday said the aim of the programs is to make America safe, he offered no specifics about how the surveillance programs have done that. House Intelligence Committee Chairman Rep. Mike Rogers, R-Mich., on Thursday said the phone records sweeps had thwarted a domestic terror attack, but he also didn't offer specifics.

The revelations have divided Congress and led civil liberties advocates and some constitutional scholars to accuse Obama of crossing a line in the name of rooting out terror threats.

Obama, himself a constitutional lawyer, strove to calm Americans' fears but also to remind them that Congress and the courts had signed off on the surveillance.

"I think the American people understand that there are some trade-offs involved," he said when questioned by reporters at a health care event in San Jose, Calif.

Obama echoed intelligence experts — both inside and outside the government — who predicted that potential attackers will find other, secretive ways to communicate now that they know that their phone and Internet records may be targeted.

An al-Qaida affiliated website on Saturday warned against using the Internet to discuss issues related to militant activities in three long articles on what it called "America's greatest and unprecedented scandal of spying on its own citizens and people in other countries."

"Caution: Oh brothers, it is a great danger revealing PRISM, the greatest American spying project," wrote one member, describing the NSA program that gathers information from major U.S. Internet companies.

"A highly important caution for the Internet jihadis ... American intelligence gets information from Facebook and Google," wrote another.

Former Rep. Pete Hoekstra, R-Mich., who served on the House Intelligence Committee for a decade, said "the bad folks' antennas go back up and they become more cautious for a period of time."

"But we'll just keep coming up with more sophisticated ways to dig into these data. It becomes a techies game, and we will try to come up with new tools to cut through the clutter," he said.

Hoekstra said he approved the phone surveillance program but did not know about the online spying.

Source URL (retrieved on *03/09/2014 - 8:01pm*):
http://www.ecnmag.com/news/2013/06/intelligence-chief-defends-internet-spying-program