After Paris attacks, US and UK discuss privacy vs. security

January 17 2015, byJulie Pace

President Barack Obama listens as British Prime Minister David Cameron speaks during their joint news conference in the East Room of the White House in Washington, Friday, Jan. 16, 2015. In a show of trans-Atlantic unity, President Barack Obama and British Prime Minister David Cameron pledged a joint effort on Friday to fight domestic terrorism following deadly attacks in France. They also strongly urged the U.S. Congress to hold off on implementing new sanctions on Iran in the midst of nuclear talks. (AP Photo/Evan Vucci)

President Barack Obama argued Friday that a resurgent fear of terrorism

across Europe and the United States should not lead countries to overreact and shed privacy protections, even as British Prime Minister David Cameron pressed for more government access to encrypted communications used by U.S. companies.

Obama and Cameron met at the White House just over a week after terror attacks in France left 17 people dead and stirred anxieties on both sides of the Atlantic. In the wake of the attacks, Cameron has redoubled efforts to get more access to online information, while the French government plans to present new anti-terrorism measures next week that would allow for more phone-tapping and other surveillance.

"As technology develops, as the world moves on, we should try to avoid the safe havens that could otherwise be created for terrorists to talk to each other," Cameron said in a joint news conference with Obama.

The response to the Paris attacks could reinvigorate the debate over balancing privacy and security, even as governments and companies still grapple with the backlash against surveillance that followed the 2013 disclosures from former National Security Agency contractor Edward Snowden. With some in France calling the attacks their country's Sept. 11, there are also fears that the government could respond with laws akin to the sweeping USA Patriot Act that the American Congress quickly approved after the 2001 attacks.

Obama avoided taking a public position on Cameron's call for U.S.-based technology companies like Google, Facebook and Apple to give governments more access to encrypted communications. He urged caution, saying he did not believe the threat level was so great that the "pendulum needs to swing" toward more invasive security measures.

Still, Obama agreed with his British counterpart that governments need to keep pace with rapidly evolving technology. He said that if having a

phone number or email address of a potential terrorist isn't enough to disrupt a plot, "that's a problem."

Last fall, FBI Director James Comey complained that new, locked-down operating systems for smartphones made by Apple and Google could hinder law enforcement's ability to investigate and prosecute crime, pointing to cases in which police would have had their hands tied had the phones been encrypted.

Leading American Internet companies expanded their encryption programs in an effort to protect customers' communications in the wake of Snowden's revelations.

The disclosures, contained in top-secret government documents leaked to news organizations, showed the NSA and its British counterpart, GCHQ, were collecting digital communications records from millions of citizens not suspected of a crime.

The prospect of authorized eavesdropping on encrypted communications raised alarms from civil liberties groups, as well as practical concerns that weakening encryption could also put users at risk of hacking.

"There's no way to design a service so that it's secure from North Korea and China while also allowing the British and U.S. governments to gain access," said Christopher Soghoian, principal technologist for the American Civil Liberties Union. "It's either secure or it's insecure."

The head of the Internet Association, a group that counts Facebook, Google, Yahoo, Amazon, eBay and Netflix among its members, said any government access to consumers' data must be "rule-bound, transparent and tailored."

"Just as governments have a duty to protect the public from threats,

Internet services have a duty to our users to ensure the security and privacy of their data," association President Michael Beckerman said in a statement.

U.S. and European intelligence agencies are still piecing together the motivations and associations of those responsible for the attacks in Paris on the satirical newspaper Charlie Hebdo and a kosher grocery. Three gunmen who carried out the attacks and were killed by police claimed links to al-Qaida and the Islamic State group.

A leader of Yemen's al-Qaida branch claimed responsibility for the attacks at Charlie Hebdo, although intelligence officials say they lean toward an assessment that the Paris terror attacks were inspired by al-Qaida but not directly supervised by the group.

Cameron was blistering in his description of those responsible, calling them part of a "poisonous, fanatical death cult." The attacks spurred Cameron's government to become more vocal in pursuing policies to prevent encryption technologies from keeping Britain's security services from being able to monitor terrorist cells.

Leaders in Washington and in European capitals have grown increasingly concerned about homegrown extremism and threats from foreign fighters with Western passports. However, Obama said the U.S. had an advantage over Europe in combatting Islamic extremism because "our Muslim populations, they feel themselves to be Americans."

"There are parts of Europe in which that's not the case," he said. "It's important for Europe not to simply respond with a hammer and law enforcement and military approaches to these problems."