Snowden moment may be passing with new fears, pushback

December 23 2015, by Troy Wolverton, San Jose Mercury News

Fears of terrorism are once again trumping talk of civil liberties.

Political debates, particularly among Republicans, are filled with fearful talk about threats to the country. The FBI director is pushing for "backdoors" into encryption software that would allow it to read scrambled communications. And perhaps worst of all, instead of constraining surveillance, Congress last week opened a big new door for domestic spying in the guise of the Cybersecurity Information Sharing Act of 2015.

It's beginning to look like the Snowden moment - the reform movement sparked by revelations by former National Security Agency contractor Edward Snowden of pervasive, illegal and largely uncontrolled government spying - may be passing.

"There's this weird moment we're in now where the momentum has abated a little bit and maybe has shifted," said Andrew Crocker, a staff attorney with the Electronic Frontier Foundation, an online civil liberties organization that has been fighting against the domestic spying programs. "It's disheartening."

When the documents leaked by Snowden started to trickle out in 2013, they ignited a long-needed debate about surveillance and civil liberties.

Congress ended the phone surveillance program, one of the first of the Snowden revelations. A federal court ruled that same program illegal.

Companies like Apple and Google embraced encryption, moving to protect the private communications of their customers and their personal data from the government's prying eyes. And there was a sense that more change was coming.

But now, fewer than three years after Snowden revealed himself, the tide appears to be turning in the wrong direction. It's discouraging, because Snowden, a former contractor with the National Security Agency, revealed that the organization, ostensibly in an effort to combat terrorism, had exceeded all reasonable and legal bounds and was collecting data on nearly all Americans. The documents revealed an agency that was out of control, was violating Americans' civil rights and badly needed to be reined in.

But the cybersecurity bill is perhaps the strongest evidence yet that the pushback against reform has already started. The bill was officially written to address a real problem: the growing number of massive hacking attacks that have compromised personal, corporate and government data. Government officials have argued that in order to combat those threats, they need to encourage more timely sharing of information about them among public agencies and corporations.

Protecting information on the Internet is something privacy and civil liberties advocates can get behind. But the broad collection of data without constraints on what is collected and how it is shared gives rise to fear about the government's law enforcement and intelligence agencies keeping inappropriate and intrusive tabs on citizens.

And it appears they have good reason to fear that happening. In a closed-door, late-night session last week, congressional negotiators quietly inserted the cybersecurity bill into a spending measure to fund the government for the rest of its fiscal year. Not only was there no debate on the cybersecurity measure, but the version that was slipped into the

spending bill was worse than the ones that had previously passed the two houses of Congress, removing even their paltry privacy protections.

The new measure will essentially pressure companies to share personal data on their users with the FBI and the NSA, the same organization that was illegally keeping tabs on citizens' phone calls, privacy advocates warn. And those agencies could hold on to the data and use it to investigate people for things that have nothing to do with hacking attacks, they say. That's why privacy advocates consider the resulting bill to be not a cyber security bill, but a computer surveillance one.

"We have a bill that the (congressional) intelligence committees hijacked during the negotiations process," said Robyn Greene, policy counsel at New America's Open Technology Institute, a tech policy think tank. "What we see is an end product that's a race to the bottom in terms of privacy and security issues."

But it's not just the cybersecurity bill in which you can see an attempt to roll back reform. FBI Director James Comey and other officials have repeatedly attacked encryption by raising the specter of terrorists using the technology to hide discussions of new attacks. Comey and others have been urging companies like Apple to let them have backdoor access into those scrambled communications, despite the fact that adding such vulnerabilities would undermine the cybersecurity of everyday Americans.

Meanwhile, Sen. Dianne Feinstein, D-Calif., has reintroduced a bill that would require social networks and other online service providers to tell the government when they see terrorism-related communications. Critics say the bill would encourage companies to either stop monitoring their networks for abusive communications - or to overshare information on their customers with the government, effectively becoming the government's eyes and ears.

It's not really a big mystery why the reform movement may be losing momentum. The recent attacks in Paris and San Bernardino have reignited fears of terrorism, fears that politicians and policy makers have been only too eager to exploit.

"Unfortunately, it's a common script," said Crocker, of the EFF.

Here's hoping this isn't the end of the story.