Tech giants urge governor to veto Georgia cybercrime bill

May 1 2018, by Ben Nadler

Tech giants Google and Microsoft have joined a chorus or cybersecurity experts urging Georgia Gov. Nathan Deal to veto a bill that makes unauthorized computer access a crime punishable by up to a year in prison.

The 1½-page proposal, passed in March in the final chaotic hours of Georgia's legislative session, would make it illegal to intentionally access a computer or network without authorization.

It's designed to give law enforcement the ability to prosecute "online snoopers"—hackers who probe computer systems for vulnerabilities but don't disrupt or steal data. The legislation follows the recent discovery by unauthorized independent cybersecurity experts of a gaping vulnerability in the computer network where Georgia's elections are managed.

The Republican governor has until May 8 to veto or sign the bill into law. Deal's office said only that he was reviewing the legislation as he does with all other bills. He has not publicly indicated a stance on the issue.

A group of more than 50 academics, researchers, cybersecurity experts and technologists wrote Deal recently urging him to veto the bill.

The group said the "legislation will chill security research and harm the state's cybersecurity industry." They said that the bill was problematic because it created new liabilities for security researchers who identify

and disclose weaknesses to improve cybersecurity.

The bill would seriously impede the kind of independent research that helps keep critical computer networks safe from intrusion, said Kennesaw State University information security researcher Andy Green, one of the signers of the letter to Deal.

Last June, an independent researcher alerted Green to the massive unplugged security hole that exposed the personal data of Georgia's 6.7 million registered voters to the open internet. He confirmed it and sounded the alarm. The subsequent erasure of data from the elections server by its custodians—just days after a lawsuit was filed calling into question the integrity of Georgia's statewide voting system—made national headlines.

Such probing would be criminalized—making it punishable by up to a year in prison—under the bill.

"I don't know about you but I'm too busy to go to jail for a year," said Green.

So-called "White Hat" hackers who merely identify security holes—even obvious ones into which a novice could stumble—would no longer contact the owners of leaky networks and say: "'Hey, you've got a problem with these systems. Let me show you how I did it, explain how you can make yourself less susceptible to attack here."

"That is going to stop, basically," Green said.

The law also would legalize in Georgia "active defense measures that are designed to prevent or detect unauthorized computer access."

It does not, however, define "defensive measures" and that gives pause

to experts who consider the bill giving license to "hack back."

Representatives from Google and Microsoft, in a joint letter to Deal, took issue with the "active defense" provision, noting that such a broad, undefined authorization of "hacking of other networks and systems under the undefined guise of cybersecurity ... is highly controversial within cybersecurity circles."

Georgia has become an important cybersecurity industry hub, ranking third in the nation in information security business and generating more than $4.7 billion in annual revenue, according to the Georgia Department of Economic Development.

The state has more than 150 cybersecurity firms as well as information security institutes at the Georgia Institute of Technology, Georgia State University, Augusta University and Kennesaw State.