GEORGIA SB 315 VETO LETTER

SIGN-ON DRAFT

NOT FOR PUBLIC DISTRIBUTION

This letter will be distributed to the Georgia governor's office and news media, and will be published by the Electronic Frontier Foundaiton. This draft may undergo further proofreading before publication.

If you would like to sign this letter, please email Dave Maass at dm@eff.org with the following information by 11 am Thursday, April 12:

Name
Job Title
Company (encouraged, but optional)

Please include a * next to the company if this is for identification purposes only, not endorsement.

April XX, 2018

Dear Gov. Deal,

We are information security specialists, computer scientists, technologists, business owners, academics, and students, and we urge you to veto S.B. 315.

This legislation, however well-intentioned, risks long term negative consequences for digital security in Georgia and beyond. We are concerned that this legislation will chill security research and harm the state's cybersecurity industry. As a result, security vulnerabilities in important computer systems will not be uncovered and disclosed responsibly, which will only make it easier for bad actors to exploit them. The bill also gives companies license to engage in countermeasures that could harm users who are unaware that their computers are being used for malicious activity.

Georgia has done much to position itself as a leader in the cybersecurity sector. The state's industry—estimated at $4.7 billion—is the third largest in the country. Georgia is

internationally recognized as a training ground for the professionals who will keep computer users safe. In order to maintain this status, the state should not pass legislation that will undermine both security practitioners and cybersecurity itself.

Specifically, the bill undermines cybersecurity in two ways:

1) **New liability for security research:** The bill potentially creates new liability for independent researchers that identify and disclose vulnerabilities to improve cybersecurity. Though the bill includes an exemption for “legitimate business activities," this term is undefined and creates ambiguity for researchers unconnected with a business (such as academics or independent researchers acting without remuneration) and how activities will be qualified as "legitimate."
2) **Allowing "hack back":** The bill allows intrusion on other computers as preemptive “active defense" – a loaded term the bill also leaves dangerously undefined and without oversight. This provision could give authority under state law to companies to “hack back” or spy on independent researchers, unknowing people whose devices have been compromised by malicious hackers, or innocent users that a company merely suspects of bad intentions.

S.B. 315, as written, creates barriers to cybersecurity research that can damage the state’s information security industry and ultimately make its citizens less safe. It gives state approval for dangerous “hacking back” methods that will cause more problems than they solve. The bill is more likely to hurt researchers, professionals, and law-abiding citizens than improve cybersecurity. We urge you to veto this legislation.

Sincerely,

* Indicates this information is for identification purposes only and does not represent a formal position by the individual’s employer.