

April 16, 2018

Office of the Governor  
206 Washington Street  
111 State Capitol  
Atlanta, Georgia 30334

Dear Gov. Nathan 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, unwitting users whose devices have been compromised by malicious hackers, or innocent people 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.*

Bruce Schneier  
Fellow and Lecturer  
Harvard Kennedy School\*

Andy Green  
Lecturer of Information Security and Assurance  
Kennesaw State University\*

Keith R. Watson GCIH  
Information Security Engineer Lead  
College of Computing, Georgia Institute of Technology\*

Frank S. Rietta  
Founder and Web Application Security Architect  
Rietta, Inc.

Peter G. Neumann  
Chief Scientist, Computer Science Lab  
SRI International\*

Marten Mickos, CEO and Alex Rice, CTO, and team  
HackerOne

Laramie Miller  
Information Assurance Manager  
U.S. Army\*

John Vittal  
Retired Director of Technology  
Verizon\*

David Jefferson  
Computer Scientist  
Lawrence Livermore National Laboratory (ret'd)\*

K.S. Bhaskar  
President  
YottaDB

Josh More  
President  
Eyra Security

Gray R. Capo, M.C.S.E.  
President  
R3ality Inc.

Kraig Beahn  
CTO/CEO  
Enguity Technology Corp.

John Covici  
President  
Covici Computer Systems

Alisa Peters, Senior Software Engineer  
Sidney San Martin, Software Engineer  
Devon H. O'Dell, Senior Systems Engineer  
Google\*

Kelly Kane  
Senior Infrastructure Engineer

Patrick Dyl  
Network Assurance  
Cox Communications\*

Randy Bush  
Member of Technical Staff  
Arrcus, Inc.

Adrienne Platner  
Software Engineer

Matt Drollette  
Principal Software Engineer  
OrderMyGear\*

Dan Gillmor  
Director, News Co/Lab  
Walter Cronkite School of Journalism and Mass Communication, Arizona State University\*

Brian G. Coffey  
IT Consultant, Security Researcher, Pen Tester  
Freelance, Self-Employed

C. Lee Davis  
DevOps/InfoSec Manager  
Fabric.com, an Amazon company\*

Jonathan Major  
Sr. Network Engineer  
Internetwork Engineering\*

M. F. "Pat" Sprague  
Electronic Engineer  
Evolving Resources, Inc.\*

William Sempf  
Co-founder/Application Security Architect  
Products Of Innovative New Technology

Bennett Cyphers  
Staff Technologist  
Electronic Frontier Foundation

Jonathan David Arndt  
Programmer

Karl O. Pinc  
President and Chief Technologist  
The Meme Factory, Inc.

Vladimir Mikhelson  
VP-Technology  
Holleb Consulting, Inc.\*

Tony Gies  
Site Reliability Engineer  
Tigerpaw Software\*

Paul Slagle  
Senior Director  
Healthcare Products LexisNexis\*

Erik Postma  
Mathematical Software Group Manager  
Maplesoft\*

Griffin Boyce  
Systems Administrator  
Berkman Klein Center for Internet and Society at Harvard University\*

Jeremy Beker  
Senior Software Engineer  
Food52\*

Corinne Braun  
Technical Consultant  
Mac Consulting Unlimited

James P. Renken  
Managing Member  
Sandwich.Net, LLC

Joshua James  
Digital Forensic Consultant

Matt Cowger  
Director, Cloud Native Technologies  
Dell Technologies\*

Bob Grimes  
Principal Firmware Engineer  
iRobot\*

Jeff Vineburg  
Security Analyst

Jason Ross  
Information Security Consultant

Christopher Grayson  
Founder, Principal Engineer  
Web Sight

John Bartas  
Senior Full-Stack Software Engineer  
Fortinet, Inc.\*

Hasan Diwan  
Director of Analytics  
Jackson St Capital LLC, Barcelona, Spain\*

Tim Ramsey  
Manager, Instructor-Led Training  
CISSP\*

Sunoo Park  
Ph.D. candidate  
MIT\*

Joshua Blum  
Software Engineer  
Keybase, Inc.\*

Benjamin Schliesser  
Vice President of Solutions Engineering  
Volta Networks\*

Rich Kulawiec  
Senior Internet Security Architect  
Fire on the Mountain

Mikki Barry  
Data Security and Privacy Attorney

Cliff Sojourner  
Computer Scientist, Engineer and Mathematician