ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

February 2, 2018

VIA EMAIL

Senator Bruce Thompson
Bruce.Thompson@senate.ga.gov

Senator Butch Miller
321 State Capitol
butch.miller@senate.ga.gov

Senator John Albers
info@senatoralbers.com

Senator Renee S. Unterman
Renee.Unterman@senate.ga.gov

Senator Jeff Mullis
jeff.mullis@senate.ga.gov

Senator Bill Cowsert
Senate Majority Leader
bill.cowsert@senate.ga.gov

Senator Steve Henson
Senate Minority Leader
stevehenson@mindspring.com

Re: Senate Bill 315 – Oppose Unless Amend

Dear Senators Thompson, Miller, Albers, Unterman, Mullis, and Cowsert:

CC: Senate Majority Leader Cowsert, and Senate Minority Leader Henson

I am writing on behalf of the Electronic Frontier Foundation (EFF) to respectfully oppose S.B. 315 as currently drafted.

Section 1 creates a new crime of unauthorized computer access. This section may be intended to target malicious behavior like computer break-ins or identity theft. In fact, however, it would criminalize violation of a website's terms of service, due to the broad, preexisting definition of "without authority" in Georgia's computer crime statute.[1] As a result, this bill would turn innocent individuals into criminals on the basis of innocuous and commonplace online behavior, chill important independent computer security research in the state, and render O.C.G.A. 16-9-93 unconstitutionally vague.

S.B. 315 is not merely problematic; it is needlessly problematic. Georgia's existing computer crime law (O.C.G.A. 16-9-93) is broad enough to capture malicious data theft and computer break-ins, including those who access personal information for the purpose of identity theft.

To avoid turning innocent Georgians into criminals, Section 1 must be removed.

[1] *See* O.C.G.A. 16-9-92.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

EFF's Interest in S.B. 315

EFF is a non-profit, member-supported civil liberties organization dedicated to protecting the rights of Internet users. With the support of more than 44,000 dues-paying members and supporters across the country, EFF represents the interests of technology users in policy debates surrounding the principled and fair application of laws—including computer crime laws—in the digital age.

EFF understands that online crimes like identity theft are a serious concern for Georgia's lawmakers, citizens, and law enforcement. It is equally important to ensure that computer crime laws are not so broadly and vaguely written that they burden constitutional rights, make criminals out of ordinary individuals, or chill the independent computer security research necessary to keep all Americans safe online.

Georgia Doesn't Need S.B. 315 – Georgia's Far-Reaching Computer Crime Law Already Criminalizes Malicious Activities Involving Computers

S.B. 315 would dramatically expand O.C.G.A. 16-9-93 by criminalizing anyone who "accesses" a computer "without authority" – even if that access is not tied to any intent to cause harm or any actual resulting harm.[2]

But Georgia's existing computer crime law already criminalizes a wide range of malicious activities involving computers: "computer theft" (obtaining property without authority), "computer trespass" (using a computer without authority with the intention of causing damage, deleting data, or interfering with a computer, program, or network), "computer invasion of privacy" (examining employment, medical, salary, credit, financial, or any other "personal data" without authority), "computer forgery" (alteration or deletion of data with the intent to defraud), and "computer password disclosure" (disclosing access mechanisms without authority). O.C.G.A. 16-9-93.

S.B. 315 is needless. The bill doesn't solve any problems; it will only create them.

S.B. 315 Could Turn Innocent Internet Users Into Criminals Based on Innocuous and Commonplace Online Behavior—Violating a Website's Terms of Service

Because of the broad existing definition of "without authority," S.B. 315's new criminal ban on access without authority would include violating an employer's policy against checking baseball scores on a work computer, lying about your age or height in your user profile contrary to a website's policy, or sharing passwords with family members in violation of the service provider's rules. The law's current definition of "without

[2] Under S.B. 315, Section 1, "any person who accesses a computer or computer network with knowledge that such access is without authority shall be guilty of the crime of unauthorized computer access."

authority" broadly extends to use that "exceeds any right or permission granted by the owner."[3] On its face, this includes user violation of provider term of service agreements. Also, courts have held that this term is broad enough to cover computer use that violates corporate policy, that is contrary to corporate interests, or that was motivated by an improper purpose.[4]

Courts across the United States have recognized the practical and constitutional problems with criminalizing terms of service violations. Specifically, in interpreting the scope of the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, many courts have held that the CFAA does not apply to Terms of Service violations. *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015); *WEC Carolina Energy LLC v. Miller*, 867 F.3d 199 (4th Cir. 2012). As the Ninth Circuit explained, "Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into . . . crimes simply because a computer is involved." *See Nosal I*, 676 F.3d at 860. In jurisdictions where terms of service violations are crimes, "describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." *Id*. at 862.

By transforming "millions of ordinary citizens" into criminals on the basis of innocuous activity, criminalizing terms of service violations also violates the constitutional rule of lenity—which "not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize." *Id.* 862, 863.

S.B. 315 Would Chill Important Security Research

Moreover, by criminalizing terms of service violations, S.B. 315 would also potentially criminalize—and undoubtedly chill— independent computer security research. The Georgia Institute of Technology is nationally regarded for its computer science and cybersecurity programs. A large element of cybersecurity research involves intentionally accessing computers in order to find security flaws, so that those flaws can be repaired

---

[3] O.C.G.A. 16-9-92

[4] *See, e.g., DuCom v. State*, 288 Ga. App. 555, 563 (2007) (use of computer system after defendant had "formed an intent" to start her own company was "without authority"); *Vurv Tech. LLC v. Kenexa Corp.*, No. 1:08-CV-3442-WSD, 2009 WL 2171042, at *5 (N.D. Ga. July 20, 2009) (access in violation of their confidentiality agreement after defendants had formed their intent to leave was "without authority"); *IPC Sys., Inc. v. Garrigan*, No. 1:11-CV-3910-AT, 2012 WL 12872028, at *10 (N.D. Ga. May 21, 2012) (allegation that defendant accessed a company computer for "nonbusiness related reasons" sufficient to state a claim); *Fugarino v. State*, 531 S.E. 2d 187 (Ga. App. 2000) (the jury may infer from the circumstances, including an employee's vindictive or retaliatory conduct, that the use was knowingly without authority).

before a wrongdoer finds and exploits them. S.B. 315 does include language that would exempt access for "legitimate business activity," but this language is vague and could still chill security research and innovation at Georgia Tech and throughout the state.

Overbroad readings of the CFAA have already chilled security researchers,[5] which in turn harms consumers when vulnerable products are inevitably exploited. Take Equifax as an example. In 2016, an independent researcher warned Equifax about vulnerabilities in its system, but Equifax instead ignored them.[6] This research could have prevented the leak of sensitive data of 145 million Americans if the researcher had disclosed their findings. They may have been deterred from doing so by the threat of CFAA prosecution. This illustrates why it is vital for independent researchers to hold companies accountable to their customers. By alienating the security research community, S.B. 315 may even encourage the talent that Georgia Tech attracts to attend schools in another state.

***

Georgians should not face the potential of criminal charges for violating a website's terms of service. And the bounds of criminal law should not be defined by lengthy corporate computer use agreements – which almost no one reads.

Thus, EFF strongly opposes S.B. 315 as currently drafted. To avoid turning innocent Georgians into criminals, Section 1 must be removed.

I can be reached at 415-436-9333 x164 or jamie@eff.org if you have any questions.

Sincerely,

Jamie Williams
Staff Attorney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

[5] https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague
[6] https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning