May 25, 2016

Via email

Representative Robert E. Craven, Sr.
Rhode Island House of Representatives
rep-craven@rilegislature.gov

Senator Frank S. Lombardi
Rhode Island Senate
sen-lombardi@rilegislature.gov

Re: House Bill 7406 Substitute A and Senate Bill 2584 (computer crime) – oppose

Dear Representative Craven and Senator Lombardi:

The undersigned civil liberties organizations regret to inform you that we must respectfully oppose House Bill 7406 Substitute A, and its companion Senate Bill 2584. These bills would amend the existing Rhode Island statute on computer crime (R.I. Gen. Laws 11-52) to create a new offense of "unauthorized access to confidential information."

A. The organizations joining this letter

The Electronic Frontier Foundation (EFF) is a non-profit member-supported civil liberties organization based in San Francisco, California. EFF works to protect rights in the digital world. EFF has more than 26,000 members and supporters across the country.

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

The Bill of Rights Defense Committee/Defending Dissent Foundation is a national civil liberties organization that protects the right to political expression and works to ensure government accountability and transparency to strengthen participatory democracy and to fulfill the promise of the Bill of Rights.

The Center for Democracy and Technology (CDT) is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

New America's Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multi-disciplinary approach that brings together advocates, researchers, organizers, and innovators.

B. Summary of the bill

H.B. 7406 Substitute A would impose criminal penalties on a person who "[1] intentionally, [2] without authority, [3] directly or indirectly accesses a computer, computer program, computer system, or computer network [4] with the intent to either view, obtain, copy, or download any confidential information contained in or stored on such computer, computer program, computer system, or computer network . . . ." *See* R.I. Gen. Laws 11-52-3.1(a) (proposed).

The bill would define "confidential information" as "[1] computer data [2] of a business, non-profit, or government entity [3] that is protected from disclosure on a computer, computer program, computer system or computer network and [4] that the computer, computer program, computer system or computer network does not transmit or disclose unless initiated by, or with the permission of, the owner of such computer, computer program, computer system or computer network." *See* R.I. Gen. Laws 11-52-1(10) (proposed).

The bill would define the offense as a felony punishable by up to five years imprisonment and a fine of up to $5,000. *See* R.I. Gen. Laws 11-52-3.1(a) (proposed); and R.I. Gen. Laws 11-52-5(a).

C. Concerns about the bill

1. Redundancy

H.B. 7406 Substitute A is not needed to protect confidential information stored in computer systems. Rhode Island already criminalizes "intentional access" to a computer system or its data, without authorization and with fraudulent or other illegal purposes. *See* R.I. Gen. Laws 11-52-3. Rhode Island also already criminalizes "computer theft," defined to include intentionally and without claim of right taking a computer system or its data. *See* R.I. Gen. Laws 11-52-4. "Confidential information," the subject of the bill, is a form of "data contained in a computer," a subject of these two statutes. So under current Rhode Island law, it already is a crime in myriad circumstances to view or take somebody else's confidential computer information.

Computer technologies, and how people use them, are constantly and rapidly changing in complex and unpredictable ways. There is an inherent danger that criminal prohibitions in this area will punish or chill activities that are innocent, commonplace, salutary, and protected by the First Amendment. So any new criminal prohibitions against how people use computers can only be justified if there is a clear problem that is not already solved by existing laws. These bills do not pass this test of necessity.

2. The term "without authority"

A key element of the new crime created by H.B. 7406 Substitute A would be vague and overbroad: access "without authority." *See* R.I. Gen. Laws 11-52-3.1 (proposed).

This phrase is insufficiently defined as follows in another part of the current Rhode Island computer crime statute: "A person is 'without authority' when: (A) he or she has no right or permission of the owner to use a computer, or, he or she uses a computer in a manner exceeding his or her right or permission or (B) he or she uses an Internet service e-mail system offered by a Rhode Island based Internet service provider in contravention of the authority granted by or in violation of the policies set by the Internet service provider." *See* R.I. Gen. Laws 11-52-1(15)(v). *See also, e.g.,* R.I. Gen. Laws 11-52-3 (defining the existing computer crime of "intentional access" as, among other things, access "without authorization").

The analogous federal statute, the Computer Fraud and Abuse Act ("CFAA"), contains a similar term: "without authorization or exceeding authorized access." *See, e.g.,* 18 U.S.C. 1030(a)(1). All too often, prosecutors have asserted, and some courts have agreed, that this CFAA language criminalizes the commonplace and innocuous act of violating a website's terms of service ("TOS") or an employer's computer use policy. The better reasoned court decisions have rejected this approach. *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015); *WEC Carolina Energy LLC v. Miller*, 867 F.3d 199 (4th Cir.2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). In the words of a leading scholar in this area:

> Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers, broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web. . . . [C]ourts should reject contract-based notions of authorization, and instead limit the scope of unauthorized access statutes to cases involving the circumvention of code-based restrictions.

See Orin Kerr, "Cybercrime's scope: Interpreting 'access' and 'authorization' in computer misuse statutes," 78 N.Y.U. L. Rev. 1596 (2003).

Thus, computer crime laws must narrowly define unauthorized access, in order to avoid criminalizing innocent violations of TOS fine print. Specifically, we oppose computer crime laws that lack the following narrow definition:

> The term "access without authorization" means to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to access the computer, file or data, but does not include circumventing a technological measure that does not effectively control access to a computer, file or data. The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or employer.

In short, the current definition of "without authority" sweeps too broadly and would criminalize legitimate Internet activity.

3. The accused's state-of-mind

The bill defines the criminal state-of-mind as mere "intent to view, obtain, copy, or download" confidential computer information. *See* R.I. Gen. Laws 11-52-3.1(a) (proposed). Anyone who intentionally and without authority accessed a computer with this state-of-mind could be incarcerated for up to five years.

We understand that a purpose of the bill is to address the commercially motivated theft of trade secrets. *See* Letter of 2/23/16 from Rhode Island Attorney General Peter Kilmartin to Chairman Cale Keable. Yet the bill does not limit the new offense to persons seeking financial gain. Rather, the bill's broadly defined state-of-mind element would also include people with no financial motive, such as a whistle blower seeking to expose their employer's wrongdoing. The original version of the bill would also reach a person who guesses their spouse's computer password and reads their private emails.

4. The term "protected from disclosure"

The bill defines "confidential information," in relevant part here, as data that is "protected from disclosure." *See* R.I. Gen. Laws 11-52-1(10) (proposed). But computer crime laws should only apply to accessing information that is "effectively" protected from disclosure. The word "effectively" is needed to address the problem of "security through obscurity," that is, the disfavored practice of relying on secrecy (such as an unpublished URL) to secure sensitive information. Absent the word "effectively," a person might be prosecuted if they access such unsecured information. Computer users should not be penalized for accessing information for which no one has actually implemented security protocols to impede access.

5. Independent security research

Any legislation that creates a new computer crime must have an appropriately written exception for independent computer security research. Frequently, security researchers (in the words of the bills) "intentionally and without authorization" attempt to "access" the parts of computer systems that are "protected from disclosure." Security researchers do so in order to identify, and then report to manufacturers, software defects and other security vulnerabilities that manufacturers may have missed. Frequently, manufacturers respond by fixing the security flaw. Thus, independent computer security research is a critical means to protect everybody's safety and privacy, by improving the quality of computer security. Any legislation that prohibits or chills computer security research would decrease all of our computer security.

H.B. 7406 Substitute A contains an exception for independent security research, but it is not adequate. It narrowly defines such research to include only access to "a data program, service, or system." *See* R.I. Gen. Laws 11-52-1(19) (proposed). This pointedly does not contain numerous terms that are currently defined in the Rhode Island computer crime statute, including

"computer," "computer data," "computer network," "computer operation," "computer program," "computer services," "computer software," and "computer system." *See* R.I. Gen. Laws 11-52-1(2) – (9). Independent security researchers who seek to test computers and not mere data would be punished or chilled.

Moreover, the originally filed version of the bill contains no exception at all for independent security research. If the final version of this bill lacks an appropriate security research exception, we will oppose the bill on that basis, too.

6. The penalty

The proposed offense would always be a felony punishable by up to five years imprisonment and a fine of up to $5,000. *See* R.I. Gen. Laws 11-52-3.1(a) (proposed Substitute A); and R.I. Gen. Laws 11-52-5(a). A felony-only penalty is especially inappropriate where, as here, the offense does not include as an element the intent to defraud. The bill should be amended to allow a misdemeanor penalty, including but not limited to first time offenses with no intent to defraud.

7. Potential stacking of charges

It is already a crime in Rhode Island to "access" a computer, intentionally and without authorization. *See* R.I. Gen. Laws 11-52-3. The bill would further make it a crime to "access" a computer, intentionally and without authorization, with intent to "view" or "copy" broadly defined "confidential information." *See* R.I. Gen. Laws 11-52-3.1(a) (proposed) & 11-52-1(10) (proposed).

As a result, if a person committed a single act of unauthorized access with the aforementioned intent, they might be charged under two different Rhode Island computer crimes. They would thus face up to ten years of incarceration (five years for each offense). This is excessive in relation to the conduct.

8. Vague and overbroad terms in existing law

The existing Rhode Island computer crime statute contains several terms that are vague and overbroad. For example:

- The statute defines "access" to a computer to include "approach." *See* R.I. Gen. Laws 11-52-1(1). Yet one might approach a computer without accessing it, and one might approach a computer physically as opposed to digitally. This definition sweeps within its scope the act of walking towards an ATM machine.

- The statute defines "access" to a computer to include "communicate with." *See* R.I. Gen. Laws 11-52-1(1). This would sweep up the act of internet-wide scanning.

- The statute defines "computer" to include an "organic device." *See* R.I. Gen. Laws 11-52-1(3). This would sweep up items like animals that are not traditionally considered

computers. The definition of "computer" in the federal CFAA does not contain this term. *See* 18 U.S.C. 1030(e)(1).

These vague and overbroad terms should be removed from the Rhode Island computer crime statute. Certainly the statute should not be expanded before such removal.

* * *

Thank you for considering our objections to H.B. 7406 Substitute A, and to the companion S.B. 2584. If you have any questions, please do not hesitate to email Adam Schwartz of the EFF at adam@eff.org, or to call him at (415) 436-9333, extension 176.

Respectfully submitted,

Adam Schwartz
Senior Staff Attorney
Electronic Frontier Foundation

Amie Stepanovich
U.S. Policy Manager and Global Policy Counsel
Access Now

Sue Udry
Executive Director
Bill of Rights Defense Committee / Defending Dissent Foundation

Gabe Rottman
Deputy Director of Freedom, Security & Technology Project
Center for Democracy and Technology

Ross Schulman
Senior Policy Counsel
New America's Open Technology Institute

cc: Speaker of the House Nicholas A. Mattiello (rep-mattiello@rilegislature.gov)
Majority Leader John J. DeSimone (rep-desimone@rilegislature.gov)
Minority Leader Brian C. Newberry (rep-newberry@rilegislature.gov)
Judiciary Chair Cale P. Keable (rep-keable@rilegislature.gov)
President M. Teresa Paiva Weed (sen-paivaweed@rilegislature.gov)
Majority Leader Dominick J. Ruggerio (sen-ruggerio@rilegislature.gov)
Minority Leader Dennis L. Algiere (sen-algiere@rilegislature.gov)
Judiciary Chair Michael J. McCaffrey (sen-mccaffrey@rilegislature.gov)
Special Assistant Attorney General Joee Lindbeck (jlindbeck@riag.ri.gov)