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

January 23, 2017

VIA EMAIL

Representative Mike Burns
326B Blatt Bldg.
Columbia, SC 29201

Representative Bill Chumley
326A Blatt Bldg.
Columbia, SC 29201

Dear Representatives Burns and Chumley,

We are writing today on behalf of the Electronic Frontier Foundation (EFF), a non-profit, member-supported, international civil liberties organization that works to protect rights in the digital world. EFF respectfully and strongly urges you to withdraw H. 3003, also known as the "Human Trafficking Prevention Act," because it creates an egregious regulatory regime that mandates both censorship and invasions of privacy.[1]

In order to conduct business in the state of South Carolina, H. 3003 requires any "business, manufacturer, wholesaler or individual that manufactures, distributes or sells a product that makes content accessible on the Internet" to include in the product a "digital blocking capability" that blocks online access to "obscenity," "child pornography," "revenge pornography," "any hub that facilitates prostitution," and "websites that are known to facilitate any trafficking of persons."

H. 3003 is a gross violation of the free speech rights of Internet users, particularly given that content filtering technology is inaccurate. The bill also violates the privacy of consumers by requiring them to engage in invasive interactions with companies in order to deactivate the blocking feature. The bill creates an exorbitant new tax for both Internet users and companies wishing to opt out of the regulatory regime. The bill violates the rights of online service providers by penalizing them for content created by their users. The bill further hurts companies by requiring costly technical features that may ultimately discourage business in the state of South Carolina.

Censorship in the Digital Age

H. 3003 violates both the First Amendment right to freedom of speech and the South Carolina constitution's identical guarantee that the General Assembly shall make no law "abridging the freedom of speech or of the press."[2] The bill creates a vague and overinclusive censorship regime that would block Internet users from accessing wholly legal content and using online communications platforms. Due to technical limitations

[1] http://www.scstatehouse.gov/sess122_2017-2018/bills/3003.htm
[2] http://www.scstatehouse.gov/scconstitution/A01.pdf

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

and definitional imprecision, it is difficult—if not impossible—to create censorship technology that only blocks illegal content or activity.

For example, while "obscenity" is not protected by the First Amendment[3] and South Carolina has attempted to define it while outlawing its dissemination,[4] it can be difficult to determine whether any particular piece of content violates "contemporary community standards," a key component of the test for obscenity, particularly when standards vary across jurisdictions and the decision maker is a non-human algorithm.

Similarly, not only is "revenge pornography" undefined in the bill, it is unclear how an algorithm could ascertain the circumstances and context of an image that are not present within the image itself—for example, that the subject of an image did not consent to its posting online or that the poster intended to harm the subject by sharing the image.

Illegal prostitution is often coded in such a way that makes it difficult to properly identify those listings among online ads. Moreover, the terms "hub that facilitates prostitution" and "websites that are known to facilitate any trafficking of persons" could literally be all online communications products and services, including email and text messaging applications, in addition to any notorious "adult" websites. It would be a gross violation of freedom of speech to censor such a broad range of online communications platforms in an attempt to mitigate illegal prostitution and human trafficking.

Additionally, the criminal penalties triggered by this legislation would incentivize companies to purposely create automatic filters that are overinclusive in order to avoid liability, which would surely sweep in wholly legal online content and communications platforms.

Finally, the bill's breadth of application is staggering. The legislation can reasonably be read to apply to *any company in the Internet ecosystem*—including device manufacturers (e.g., smartphones, tablets, computers, smart TVs, video game consoles, and Wi-Fi routers), ISPs that provide Internet access, web hosting companies, and online service providers such as search engines, email and text messaging providers, social media platforms, and blogging platforms. All of these companies arguably provide products that "make content accessible on the Internet," and thus would have to install censorship technology to do business in South Carolina.

A Poor Remedy

The legislature has anticipated such an overbroad censorship regime by requiring the unblocking of non-obscene content within five days after the inappropriate censorship is reported.[5] However, any length of time that legal content is censored by the government is a First Amendment harm, and no mitigation is contemplated for content that is wrongly blocked as "child pornography" or "revenge pornography."

Social media websites would be exempt from the censorship regime, but *only if* they are "primarily used for social interaction" (the meaning of which is unclear) and

---

[3] *Miller v. California*, 413 U.S. 15 (1973).
[4] Sec. 16-15-305, http://www.scstatehouse.gov/code/t16c015.php#16-15-305.
[5] Sec. 16-15-530(A) (proposed).

they have "a reporting center and remain reasonably proactive in removing obscene content."[6]

Although H. 3003 permits consumers to deactivate the "digital blocking ability" on their devices and online products, the mechanism for doing so—particularly the $20 fee and the option of going to court—significantly burdens individuals who want to ensure that they can access wholly legal online content and communications platforms.[7]

This deactivation process also violates consumers' privacy. For consumers who want greater control over their devices and online experiences, the bill would fundamentally change the relationship between consumers and the companies from which they obtain goods and services. Consumers would be forced to identify themselves when making a written request for filter deactivation, creating an awkward situation that might suggest that they want access to controversial or illegal sexual material. Moreover, the bill provides no protection for this sensitive information, which could be subject to all-too-common data breaches if stored by the companies, and subject to bureaucratic abuse if stored by the government.[8]

Finally, consumers would be forced to review a patronizing "written warning regarding the potential danger" of accessing the Internet without a filter, subjecting them to information that may be inaccurate or offend their personal beliefs. And if companies, as opposed to the South Carolina government, must provide this written warning, this may be compelled speech subject to First Amendment challenge.[9]

H. 3003 creates a significant barrier to accessing Internet content and services that consumers have a right to view and use. In the interest of limited and responsible government, the state must not insert itself into the private lives of its citizens.

A Burdensome Consumer Tax

H. 3003 would require consumers to pay $20 to deactivate filters on *every* product or service that "makes content accessible on the Internet," effectively creating a new and highly burdensome tax scheme—because many Americans own multiple Internet-connected devices and use many online services. According to a 2014 report by Ericsson, the average household in North America owned 5.2 Internet-connect devices.[10]

---

[6] Sec. 16-15-530(B) (proposed).
[7] Sec. 16-15-520(4) (proposed); Sec. 16-15-530(C) (proposed).
[8] Symantec, *Over Half a Billion Personal Information Records Stolen or Lost in 2015*, https://www.symantec.com/content/dam/symantec/docs/infographics/istr-reporting-breaches-or-not-en.pdf.
[9] *See, e.g., Agency for Int'l Development v. Alliance for Open Society Int'l*, 133 S. Ct. 2321(2013) ("It is … a basic First Amendment principle that freedom of speech prohibits the government from telling people what they must say.") (internal quotations omitted).
[10] Ericsson, *North America Mobility Report June 2015*, http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015-rnam-appendices.pdf.

Consider the effective tax rates based on these device prices:[11]

Device	Retail Cost	H. 3003 Equivalent Tax
iPhone 7	$699.99	2.9%
Samsung Galaxy Tablet	$229.99	8.7%
NetGear Router	$118.99	16.8%
Playstation 4 console	$249.99	8%
Sony Smart TV	$449.99	4.4%
Kindle Paperwhite	$119.99	16.6%
Lenovo Laptop	$249.99	8%

H. 3003 would result in a consumer who purchases these seven items paying an additional $140, the equivalent of a 6.6% tax on consumer electronics. Many consumers who may not otherwise be interested in pornography will opt to pay these fees in order to avoid the inconvenience of repeatedly running into mistakenly blocked sites. Other consumers may decide to simply purchase their technology out of state. As written, the bill arguably also covers online services, requiring users to pay $20 for the many email, text messaging, blogging, and social media platforms they use.

The bill also allows companies to pay a $20 "opt-out fee" for each product that enters South Carolina, yet this cost would surely be passed on to the consumer. If this cost is not passed on to the consumer, then the opt-out fee may also be considered a burdensome tax upon companies. For manufacturers and online service providers, the number of devices and the number of users could be in the millions, making this opt-out fee collectively exorbitant and unrealistic.

Additional Burdens on Companies

H. 3003 is particularly problematic because it puts criminal liability on companies for the actions of third parties. Specifically, if a company provides to South Carolinians a product that "makes content accessible on the Internet," but the specific categories of content and communications platforms targeted by the bill are not "rendered inaccessible," companies and their executives would be subject to felonies, fines, and up to 10 years in prison.[12]

Given that it is technology users who create the illegal content or engage in illegal activity, it is fundamentally unfair and disproportionate to place this kind of liability on companies who are merely conduits for their users. Moreover, federal law generally immunizes Internet intermediaries from liability arising from publishing content created by others, and preempts state law inconsistent with that immunity.[13]

Additionally, the framing of the criminal liability does not seem to consider any intent or *mens rea* requirement, effectively creating a strict liability enforcement regime—something also fundamentally unfair given the limitations of filtering technology. That is, even companies who fully intend to comply with South Carolina law might break the law if their "digital blocking capability" is faulty.

---

[11] Prices were obtained from the Best Buy website, http://www.bestbuy.com/.
[12] Sec. 16-15-550 (proposed).
[13] 47 U.S.C. § 230.

Finally, H. 3003 would put significant financial and logistical strain on companies who want to do business in South Carolina, resulting in serious repercussions for the South Carolina economy and consumer choice. The bill would force companies to invest heavily in a censorship infrastructure, by not only developing the technology but establishing an entire model for handling blocking and de-blocking requests. They would also need to create new infrastructure for the bureaucratic process of obtaining written requests and providing the written warning. This bill would discourage many companies that "make content accessible on the Internet" from providing their devices and online services to South Carolinians. Consumer electronic stores, for example, may see their sales drop as consumers instead cross state lines in order to obtain cheaper devices untethered from censorship filters.

Conflicts of Interest

We must also note that the Human Trafficking Prevention Act is a model piece of legislation promoted by a technology company through its non-profit foundation.[14] This should raise alarms for legislators, as the ultimate goal may be in fact to benefit a specific company.

Conclusion

H. 3003 will not have the impact that the authors intend, and instead create enormous burdens for free speech, user control of devices and online experiences, privacy, and the consumer electronics economy. We will continue to oppose this bill as it progresses, while alerting our supporters and our allies in the technology community to the dangers the bill presents. We urge you to withdraw H. 3003.

Sincerely,

Sophia Cope
Staff Attorney
sophia@eff.org
(415) 436-9333 x155

Dave Maass
Investigative Researcher
dm@eff.org
(415) 436-9333 x151

[14] The Clean Services Foundation, http://www.tel-electronics.com/clean/.