

LIBRARIES Long Beach, California

Gabriel J. Gardner is a librarian at California State University at Long Beach. He studies, among other things, the reasons that some scholars—even those with access to scientific journals for which their colleges and universities have paid for subscriptions—prefer shared papers, even when those papers have been pirated in violation of copyright laws.

Gardner has published papers on the topic and given presentations at meetings of academic librarians.

Thomas H. Allen, president of the Association of American Publishers. last month sent a letter to Gardner's boss at Cal State to complain about a presentation Gardner made on the research—and that letter is now being shared online and being criticized by many librarians. Gardner and Cal State say that the letter distorts his research and implies that talking about such repositories of pirated papers as Sci-Hub is the same thing as endorsing them. And they say Allen is trying to intimidate librarians who are pushing for change in scholarly publishing.

In his letter, Allen said that Gardner, in a recent session at the American Library Association, "essentially" said of Sci-Hub, "Try it, you'll like it." Sci-Hub, Gardner noted, is under court orders not to continue its operations.

"Sci-Hub's methods are not benign," Allen wrote. "They include illegally accessing the secure computer networks of a large number of major universities by, among other methods, hijacking 'proxy' credentials used to facilitate off-campus remote access to university computer systems and databases. The techniques employed by it to defeat security standards are similar to those employed by other cyberintrusions," including those that protect the privacy of students' and researchers' records.

Allen went on to say that he found it "surprising" that a Cal State librarian would "promote the activities of an adjudicated thief who has compromised university computer systems and databases worldwide." While some supporters of Sci-Hub "invoke academic freedom," Allen said, such arguments are nothing more than "rationalizations" to "justify the theft of intellectual property."

Via email, Gardner said that he never endorsed Sci-Hub or its methods, but that in discussing the site, he said it was easy to use. He said it's important for librarians to be aware of that fact.

"I believe the letter was an attempt at intimidation; my deans certainly interpreted it as such," Gardner said. "The pretext that the purpose of the letter was to educate us about the severity of intellectual property violations is laughable. Every librarian in the country knows that they shouldn't advocate piracy, to do so is a clear violation of the American Library Association's Code of Ethics."

Roman Kochan, dean of library services at Cal State Long Beach, has issued his own letter, strongly defending Gardner and asking why the publishers' group is not doing more to help university libraries deal with journal costs.

Kochan—citing a recording of the session—noted that Gardner said Sci-Hub was engaged in "massive piracy" with "illegal" actions, and in no way endorsed Sci-Hub. He said that Allen's criticisms were "fundamental factual inaccuracies." Further, he said that Gardner's work was very much covered by academic freedom, and as such had the strong endorsement of Cal State Long Beach.

More broadly, in comments receiving praise on social media from librarians, Kochan took the publishing industry to task for not working with academic librarians to create more affordable models for the dissemination of scholarship.

"The larger issue here is that the academic publishing model has become unsustainable," Kochan wrote. "Like many university libraries, the library budgets at California State University at Long Beach and the California State University generally cannot sustain annual price increases of 3 percent to 10 percent by many of your organization's members. Journal subscription prices are a key part of the reason that extralegal services, such as Sci-Hub, flourish." Reported in: <u>insidehighered.com</u>, August 8.

Grand Forks, North Dakota

Can a public library kick out people who are asking other library goers to sign a petition? That question is being asked after a group of people in Grand Forks, led by C. T. Marhula, said they were kicked out of the Grand Forks Public Library in August.

Since it was announced that two locations (Midtown and Downtown) were selected for a new library in Grand Forks, many people have expressed their disapproval. "Many, many people want to keep the new library at its current location," Marhula said. "We've collected a lot of signatures."

Marhula said he went through the proper channels to get his group into the library to circulate the petition. "This is not North Dakota nice. This is not constitutational," Marhula said. "The constitution guarantees the right to petition."

However, David Thompson, an attorney in Grand Forks, said it's not as simple as that. "The First Amendment of The Constitution protects free speech, but it's not an absolute right," Thompson said. "In other words,

5

people have no right to yell fire in a crowded theater."

Thompson said several court cases allow the government to regulate speech in a reasonable time, place or manner. "If they were approaching people as they were reading at tables, going to card catalogs or using computers . . . for people to do that in a library, which is a quiet place, probably one of the most quiet public places that there are, would be basis for a government or representative of a government to ask people to leave," Thompson said.

Library Director Wendy Wendt said it's their longstanding policy to prohibit soliciting in any way at the library. The library board said they are going to take a look at the policy, "clear up some of the language" and ensure "it's being enforced fairly." Reported in: <u>valleynewslive.com</u>, August 17.

SCHOOLS Washington, DC

Schools have become "soft targets" for companies trying to gather data and market to children because of the push in education to adopt new technology and in part because of the rise of computer-administered Common Core tests, according to a new annual report.

The report, titled "Learning to be Watched: Surveillance Culture at School" and published by the National Center for Education Policy at the University of Colorado at Boulder, is the eighteenth annual report about schoolhouse commercialism trends.

It says student privacy is increasingly being compromised by commercial entities that establish relationships with schools—often providing free technology—and then track students online and collect massive amounts of data about them. Then they tailor their advertising to keep the young people connected to them. One important consequence, the report says, is that children who are subjected to "constant digital surveillance and marketing at school" come to accept as normal that corporations play a big role not only in their education but in their lives.

The report says: "Schools have proven to be a soft target for data gathering and marketing. Not only are they eager to adopt technology that promises better learning, but their lack of resources makes them susceptible to offers of free technology, free programs and activities, free educational materials, and help with fundraising. Schools are under relentless pressure to make ever greater use of technology. Our techno-friendly zeitgeist embraces and celebrates the rapid proliferation of education technology in every corner of our lives. In school, teachers are encouraged to integrate technology into their lessons and homework, and to rely on computerized student performance data as a diagnostic tool. State and federal laws now require that schools do extensive data reporting; in addition, the Common Core testing regime requires students to take computerized tests-and therefore to be computer-competent before they approach the tests."

Although some parents try to resist the collection and use of data about their children, the ubiquity of computers makes it easy for children and their parents to accept "constant data gathering and attendance surveillance of children"—and few look through the companies' "long paragraphs of legalese" to understand what is really going on. Americans are, the report says, "to some extent being socialized to ignore and tacitly accept the collection, organization, and sale of information about us."

The report notes that industry officials say that there is no danger to student privacy because much of the data being collected is not directly identified with a particular student. But, it says, "even if companies anonymize student data for security or marketing purposes, however, students' personally identifiable information (PII) may not be fully or permanently protected."

Aside from privacy issues, the report says, marketers can influence the way young people think, feel and behave with data they collect online. It says: "Although companies that collect, sell, analyze, and buy data may not know children's names (though they probably do), that hardly matters if they have the information and tools necessary to model everything about those children-including their interests, social networks, personalities, vulnerabilities, desires, and aspirations-and if they have personalized access to children, via their electronic devices, to shape them. By feeding children ads and other content personalized to appeal specifically to them, and also by choosing what not to show them. marketers influence children's thoughts, feelings and behaviors. As they do, they also test, adjust, and perfect their models of influence—and then track and target some more."

The report says Google and Facebook are probably the largest companies that data mine in schools, and they also spend a lot of money to lobby lawmakers "to keep regulation at bay."

In 2013, Advertising Age noted that Google and Facebook, "two of the most pervasive digital-data collectors," significantly increased their lobbying expenditures between 2011 and 2012—to \$19.6 million for Google and \$4.6 million for Facebook in 2012... According to one Google blog post, it reaches "more than 30 million students, teachers and



administrators globally" via its Google Apps for Education (GAFE).

There are several federal laws that are meant to address student privacy: the Family Educational Rights and Privacy Act, known as FERPA; the Children's Online Privacy Protection Act, known as COPPA, and the Protection of Pupil Rights Act. Each has significant weaknesses, the report says, which leave younger children and teenagers open to having their student records disclosed to commercial entities without parental consent.

Most of the laws dealing with study data apply to the disclosure to third parties of personally identifiable information. There is a voluntary Student Privacy Pledge that businesses can take, but there is no assurance that digital data will not be sold to advertisers or that companies won't track students' online behavior.

It is important to understand why the federal laws don't do a complete job of protecting student privacy. The report notes: "FERPA, which applies to almost all public and private schools, provides the primary set of regulations governing student privacy in the US. Any agency or institution that violates FERPA regulations loses eligibility for federal funds. However, FERPA's scope is limited to 'educational records'; the legislation does not protect such items as data collected by education websites or digital "pupil-generated content" (such as essays), unless PII is included in that information.

"Moreover, several FERPA exceptions allow student records to be disclosed to certain parties or under certain conditions without parental consent. The most significant exception is that without consent, school officials may release student records for any educational purpose they deem legitimate, as when an organizations is conducting studies for or on behalf of a school; records are also available to authorized representatives of the U.S. Comptroller General, U.S. Education Secretary, or state educational authorities.

"Changes to FERPA in 2008 and 2011 expanded the definitions of both school officials and authorized representatives. In one of the most important changes, the U.S. Department of Education now considers 'school officials' to include 'contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform.'

"This change has far-reaching implications for student privacy. For example, when school leaders sign a contract to use Google Apps for Education (GAFE), they assign Google the authority of "school official." The Department also considers "authorized representatives" to be any individuals or entities that local or state educational authorities, U.S. Secretary of Education, or U.S. Comptroller General select as an authorized representative. As a result of these changes, schools may now provide data to private companies without parental consent. Significantly, these private companies are not named 'partners,' but rather 'school officials' or 'authorized representatives.'

"The Children's Online Privacy Protection Act (COPPA), which applies to children under the age of 13, requires companies to obtain parental consent before they can collect personal information from children for commercial purposes. In December 2012, the Federal Trade Commission (FTC) expanded several definitions under COPPA, increasing protection of children by accounting for new tracking technology. While these changes are significant, the law does not apply to teens. Teens are especially at risk because they are online more than young children both in and out of school, and also because developmentally they are particularly susceptible to targeted marketing." Reported in: *Washington Post*, May 17.

Orlando, Florida

Schools in Florida are renewing a program that monitors their students' social media activity for criminal or threatening behavior, although it has caused some controversy since its adoption last year.

The school system in Orange County, where Orlando is located, recently told the Orlando Sentinel that the program, which partners the school system with local police departments, has been successful in protecting students' safety, saying that it led to twelve police investigations in the past year. The school district says it will pay about \$18,000 annually for SnapTrends, the monitoring software used to check students' activity.

SnapTrends collects data from public posts on students' social media accounts by scanning for keywords that signify cases of cyberbullying, suicide threats, or criminal activity. School security staff then comb through flagged posts and alert police when they see fit. Research suggests that 23 percent of children and teens have been cyberbullied. Studies connecting social media and suicide have not shown definitive results, but there has been research that suggests that cyberbullying leads to suicide ideation more than traditional bullying.

Orange County Public Schools adopted the SnapTrends program as part of a "prevention and early intervention" program. After the Newtown, Connecticut, school shootings in 2012, the school participated in a sweeping technical review with law enforcement and state emergency experts with a focus on safety. They

শ্

recommended some sort of social media monitoring program, saying that threats can sometimes be spotted on social media postings. "We felt we needed to deal with these vulnerabilities," Shari Bobinski, who manages media relations in the school system, said.

Orange County schools said that since implementing the software last year, it has run 2,504 automated searches, leading to 215 manual searches by school staff. Details of the police investigations that stemmed from searches in the past year have not been divulged by the school system. The school system said that it doesn't want public details of the program to interfere with its effectiveness.

Bobinski, however, shared one anecdote from last year. The software flagged a female student for using the keyword "cutting" and the phrase "nobody will miss me." Since the software gets a huge number of flags for words and phrases like these, the security staff delved deeper, investigating more posts by the student. They discovered that she had two conflicting social media accounts: one that told the story of a happy, normal girl, and the other of someone suffering from suicidal thoughts and depression. The school staff alerted police, who conducted a welfare check at the student's home and informed her father. She eventually went into treatment.

The story exemplifies the kind of safety checks that social media monitoring offers. But Bradley S. Shear, a privacy and social media lawyer based in Bethesda, Maryland, expressed concerns about the unintended consequences of using software like Snap-Trends. He's uncomfortable with the collection and storing of information on students. "Is this data then gonna be tied to a student's permanent school record? Does the company have proper policies in place that delete this data after a certain period of time? These are some questions that need to be asked," he said.

An example of an appropriate period of time for data to be stored, he suggested, would be until a year after the student graduates or until they turn eighteen—a guideline set by a California state law that aims to protect social media privacy for students monitored by schools.

Kids are very tech savvy, he emphasized, and are likely to find creative ways to evade monitoring. That would put their social media lives even further away from the watchful eyes of parents or other adults.

Shear also expressed fears of the inevitability of highly intrusive monitoring, such as collecting data on students during after-school hours or off school property. A software flag would require school staff and possibly police to track a student more closely. In Bobinski's story of the suicidal student in Orange County, the original flag was set off on school property (SnapTrend's "geofencing" technology limits monitoring within a locational boundary), but investigators delved into her public posts from after-school hours as the checked into her mental health status.

Orange County isn't alone in choosing to monitor students. Schools in Alabama and California have adopted similar social-media-mining software. In Huntsville, Alabama, fourteen kids were expelled because of social media posts in 2014. The content of the posts was not made public, but a school board member said that expulsions result only from serious offenses involving drugs, weapons or sex. Twelve out of the fourteen were black, despite the schools' population of about 40 percent black students and 60 percent white. The expulsions raised concerns from a county

commissioner that social media monitoring unfairly targeted black students. The case raises questions about which students are most vulnerable when digitally tracked by the school and police working in concert.

But Bobinski emphasized that the Orange County system respects student privacy and inspects student social media activity, which is public, only if software-flagged content causes concern. Online activity would only appear on a school record if it led to disciplinary action. "We've been very transparent about what we're looking for," she said. "And that is to keep our students, our staff and our facilities a safe learning environment." She was not able to confirm how long social media data is stored by SnapTrends.

For Shear, the allocation of \$18,000 in school funds to implement Snap-Trends that could be used for digitally minded education is particularly vexing. "[Schools] are not providing children the tools needed to protect their reputation, their privacy and to understand the law. Everything that these kids are doing online might have repercussions down the road," he said.

"I think that's something that's missing in the conversation," Shear continued. "I think that these companies are preying on the fears of these parents." Reported in: *Washington Post*, April 22.

PRIVACY Washington, DC

The Obama administration is seeking to amend surveillance law to give the FBI explicit authority to access a person's internet browser history and other electronic data without a warrant in terrorism and spy cases. The administration made a similar effort six years ago but dropped it after concerns were raised by privacy advocates and the tech industry.



FBI Director James B. Comey has characterized the legislation as a fix to "a typo" in the Electronic Communications Privacy Act, which he says has led some tech firms to refuse to provide data that Congress intended them to provide.

But tech firms and privacy advocates say the bureau is seeking an expansion of surveillance powers that infringes on Americans' privacy.

Now, at the FBI's request, some lawmakers are advancing legislation that would allow the bureau to obtain "electronic communication transactional records" using an administrative subpoena known as a national security letter. An NSL can be issued by the special agent in charge of a bureau field office without a judge's approval.

Such records may include a person's internet protocol address and how much time a person spends on a given site. But they don't include content, such as the text of an e-mail or Google search queries. There's also a limit to how much visibility the bureau would have into which part of a website a person had visited. For instance, according to the bureau, if the person went to any part of the *Washington Post*'s website, law enforcement would see only washingtonpost.com—nothing more specific.

Comey said that making this change to the law is the bureau's top legislative priority this year. The inability to obtain the data with an NSL "affects our work in a very, very big and practical way," he told the Senate Intelligence Committee in February.

The Senate panel recently voted out an authorization bill with the NSL amendment. The Senate Judiciary Committee is considering a similar provision introduced by Sen. John Cornyn (R-Texas) as an amendment to ECPA, a law governing domestic surveillance. Cornyn said that what he characterized as a "scrivener's error" in the law is "needlessly hamstringing our counterintelligence and counterterrorism efforts."

But privacy groups and tech firms are again warning that the expansion of power would erode civil-liberties protections. The fix the FBI seeks would "dramatically expand the ability of the FBI to get sensitive information about users' online activities without oversight," said a coalition of privacy and civil society groups and industry organizations in a letter.

The new categories of information that could be collected using an NSL "would paint an incredibly intimate picture" of a person's life, said the letter, signed by the American Civil Liberties Union, Amnesty International USA, the Computer & Communications Industry Association, Google, Facebook and Yahoo, among others. For example, a person's browsing history, location information and certain email data could reveal details about a person's political affiliation, medical conditions, religion and movements throughout the day, they said.

In addition, the NSL would come with a gag order preventing the company from disclosing it had a received a government request, said Neema Singh Guliani, ACLU legislative counsel. The letter noted that over the past ten years, the FBI has issued more than 300,000 NSLs, most of which had gag orders. "That's the perfect storm of more information gathered, less transparency and no accountability," Gulani said.

But a law passed last year, the USA Freedom Act, requires the Justice Department to review gag orders periodically to assess whether they are still justified.

The amendment being considered by the Judiciary Committee is part of a broader effort by lawmakers to update ECPA to require law enforcement to get a warrant for all email content, regardless of whether it is one day or one year old.

Privacy groups and tech companies support the broader ECPA update, versions of which some lawmakers have sought for years. But the groups and tech organizations in their letter said that if the ECPA bill includes the NSL provision, they will pull their support.

A November 2008 opinion from the Justice Department's Office of Legal Counsel made clear that ECPA allows the FBI to obtain with an NSL only four types of basic subscriber information from internet companies: name, address, length of service and telephone bill records. There is no reference in the law to browser history, for instance. The opinion said the four existing categories were "exhaustive."

The FBI's Office of General Counsel, however, has argued that electronic communication transactional records are the functional equivalent of telephone billing records. To eliminate any uncertainty, the FBI wants the law to explicitly cover such data.

Senators Patrick J. Leahy (D-VT), the ranking minority-party member on the Judiciary Committee, and Mike Lee (R-UT), a committee member, oppose the Cornyn amendment. They say they will push for a clean version of the ECPA update similar to a bill passed by the House earlier this year. Reported in: *Washington Post*, June 6.

Washington, DC

Federal Communications Commission chair Tom Wheeler made his case for an ambitious plan to better defend consumer data privacy on March 10. His proposal would effectively govern how Internet Service Providers (ISPs) can leverage user data for marketing and advertising purposes in the

same way that that the FCC already regulates data collected by phone companies.

"Think about it. Your ISP handles all of your network traffic," Wheeler wrote in a Huffington Post op-ed. "That means it has a broad view of all of your unencrypted online activity when you are online, the websites you visit, and the apps you use."

Basically, since an ISP has access to every piece of unencrypted data its customers send along its network, it can build an incredibly detailed dossier of their online lives. And, up until now, the ISP could use that information anyway it saw fit. Wheeler wants that to change.

"The information collected by the phone company about your telephone usage has long been protected information," he continued. "Regulations of the Federal Communications Commission (FCC) limit your phone company's ability to repurpose and resell what it learns about your phone activity. The same should be true for information collected by your ISP."

To that end, Wheeler has put forth a plan that would "empower consumers to ensure they have control over how their information is used by their Internet Service Provider." In broad strokes, it would demand more transparency from ISPs on what information is being collected, give consumers the right to have meaningful control over that information, make it the ISP's "duty" to secure and protect your data for the duration that it is on the ISP's network.

In terms of user control, Wheeler proposes a three-tiered approach. The basic marketing of services would remain unchanged. "For example, your data can be used to bill you for telecommunications services and ensure your email arrives at its destination, and a broadband provider may use the fact that a consumer is streaming a lot of data to suggest the customer may want to upgrade to another speed tier of service," Wheeler wrote. However, any data used for affiliate marketing or otherwise shared would require an active opt-out from the user and all other forms of marketing would need the user to explicitly opt in.

As for ensuring data security, Wheeler's proposal would only require ISPs to take "reasonable steps" to defend user data from snooping. There's actually a lot less wiggle room for ISPs in that directive than you'd expect. "At a minimum," Wheeler wrote, "it would require broadband providers to adopt risk management practices; institute personnel training practices; adopt strong customer authentication requirements; to identify a senior manager responsible for data security; and take responsibility for use and protection of customer information when shared with third parties."

This proposal only applies Internet Service Providers. Websites like Facebook or Twitter would be exempt from these rule changes—namely because their operations are regulated by the Federal Trade Commission. The FCC will vote on Wheeler's proposition on March 31, after a period of public comment from the American people. Reported in: <u>engadget.com</u>, March 10.

CHURCH AND STATE Dayton, Ohio

Wright-Patterson Air Force Base Medical Center has removed a Bible from a POW/MIA display after the Military Religious Freedom Foundation lodged a complaint, according to a base spokesperson.

Mikey Weinstein, MRFF founder and president, said the organization was contacted by thirty-one people who objected to the Bible as part of the table display, including 10 who identified themselves as Christians. "They objected very clearly that having the Christian Bible on that table provided supremacy to one faith over all the other faiths, and since these are government facilities, that's a direct violation of the no establishment clause of the First Amendment of the Bill of Rights of the US Constitution," Weinstein said.

474

"In this instance, allowing that Christian Bible to be there is a very odious example of fundamentalist Christian triumphalism, supremacy, and exceptionalism and primacy," he said. "Our veterans saw it, our members saw it. They're not going to sit back and take this anymore."

Weinstein said his group, which is based in Albuquerque, New Mexico, and represents more than 45,000 service members and veterans, has received complaints from throughout the country over religious displays. The group's efforts have angered some, and Weinstein said an MRFF staffer resigned last week citing online threats to him and his family over the removal of Bibles at federal facilities.

The installation commander at Wright-Patterson, Colonel John M. Devillier, made the decision to remove the Bible from the display at the medical center last week "after thoroughly assessing the situation," Wright-Patt spokeswoman Marie Vanover said.

"Mutual respect is an essential part of the Air Force culture and we must ensure we create an environment in which people can realize their highest potential regardless of one's personal religious or other beliefs," Vanover said in an email.

Richard Thompson, president and chief counsel of the Ann Arbor, Michigan-headquartered Thomas More Law Center, objected to the removal.

"The courts have said ceremonial displays not meant to proselytize



anyone is not considered an establishment of religion," said Thompson. "It is there for someone to acknowledge or that person does not have to acknowledge it. . . They can either accept the Bible being there or, if they are really offended by the Bible, they could turn away."

Thompson said the base commander "capitulated" to the demand to remove the book. "We cannot separate God and the Judeo-Christian principles upon which our country is founded from the military who dedicate their lives, who put themselves in harm's way, when they are performing their duties," Thompson said. "And certainly had the commanding officer wanted to fight this attempt to intimidate them from removing the Bible, we would have been happy to represent the organization without charge and I think would have won the case."

The center is a member of the Restore Military Religious Freedom Coalition.

Weinstein's group also objected to the inclusion of Bibles in "POW/MIA Missing Man" displays at VA facilities in Akron and Youngstown following complaints, he said. Those too were removed.

"This is not Christian victimization," he said. "This is Christian equalization. Why does the Christian book of faith get put into a solemn and critical memorial to that sacrifice of our wonderful members of the military, POWs and MIAs, over everybody else's faith book?"

Volunteers and veterans organizations donated the Bibles for the two displays at the clinics and made the decision to remove them, according to Kristen Parker, a spokeswoman at the Louis Stokes Cleveland VA Medical Center.

"The Cleveland VA Medical Center honors and respects the humanity of all, and protects the freedoms and rights guaranteed for each of us," she said in an email. "Because the VA cannot endorse, promote or inhibit one religion over another, we couldn't influence the final decision on whether or not the Bibles remained or were removed from the displays as the displays were donated and are maintained by volunteer organizations."

The Cleveland VA brought the concerns of both sides to the groups, she added.

The Bible was removed in the Akron display, and volunteers replaced the religious book in Youngstown with a "prop book" to allow a veteran "to individualize the meaning behind the book when they pay their respects to the POW/MIA table," Parker said. Reported in: *Dayton Daily News*, April 11.

Nashville, Tennessee

Tennessee Governor Bill Haslam has vetoed a controversial bill that would have made the Holy Bible the official state book of Tennessee. Haslam cited an opinion issued in 2015 by state Attorney General Herbert Slatery that said the bill could violate the state and federal constitutions.

"In addition to the constitutional issues with the bill, my personal feeling is that this bill trivializes the Bible, which I believe is a sacred text," Haslam wrote in a letter to House Speaker Beth Harwell.

"If we believe that the Bible is the inspired word of God, then we shouldn't be recognizing it only as a book of historical and economic significance," the Republican governor said. "If we are recognizing the Bible as a sacred text, then we are violating the Constitution of the United States and the Constitution of the State of Tennessee by designating it as the official state book."

Had Haslam signed the bill, Tennessee would have become the first state in the nation to make the Holy Bible its official state book. The veto was just Haslam's fourth in his five years as governor. None of his other three vetoes were overturned. Tennessee's governor has relatively weak veto power: It takes only a simple majority in both chambers to overrule the governor's decision.

The House passed the measure fifty-five to thirty-eight during the 2015 legislative session, but it failed to pass through the state Senate during that legislative session. But senators pushed forward with the legislation again this year, despite opposition from Ramsey and Senate Majority Leader Mark Norris.

Supporters tried to argue the move would highlight the economic and historical impact the Bible has had on Tennessee, saying printing the Bible is a "multimillion-dollar industry" for the state. Opponents argued the bill formalized a governmental endorsement of Christianity, while others, like Haslam, argued the move would trivialize the Bible by placing it next to the tomato—the state fruit—and raccoon—the state animal.

"I strongly disagree with those who are trying to drive religion out of the public square. All of us should and must bring our deepest beliefs to the places we are called, including governmental service," Haslam wrote in the letter to Harwell.

"Men and women motivated by faith have every right and obligation to bring their belief and commitment to the public debate. However, that is very different from the governmental establishment of religion that our founders warned against and our Constitution prohibits."

The potential for a veto override worried Annie Laurie Gaylor, founder and president of the Wisconsin-based Freedom from Religion Foundation. Still, her first word

when told Haslam had vetoed the bill was "hallelujah."

"Government shouldn't take sides on religion," Gaylor said. "I think we're turning a corner in our country that we are seeing a Republican governor in the South write a very firm defense of separation of church and state and understanding of the establishment clause and not apologizing about it."

Hedy Weinberg, executive director of the American Civil Liberties Union of Tennessee, thanked the governor for his decision. The ACLU had opposed the legislation as it made its way through the Tennessee General Assembly.

"We applaud Governor Haslam for his leadership in sending a clear message that Tennessee values and respects the religious freedom of all Tennesseans," Weinberg said in an emailed statement.

"Religion thrives when it is left in the hands of families and faith communities. Publicly elected government officials cannot use their official positions to favor one religious belief over another. The governor's veto of this unconstitutional legislation ensures that religious freedom can flourish in Tennessee."

Roger Gannam, senior litigation counsel for Liberty Counsel, called the governor's veto disappointing and said Haslam's reasoning is based on an "erroneous interpretation of the Constitution."

After lawsuit concerns were raised about the measure, Gannam's organization offered its legal services free of charge if the state opted out of defending the bill. "The government's adoption of the Bible as the state book would not be an endorsement of Christianity or Judaism or the contents of the book as religion," Gannam said. "But certainly could have adopted the Bible as a proper recognition of the influence it had on the foundations of Tennessee law and political thought."

David Fowler is a former state senator and president of the Family Action Council of Tennessee, which supported making the Bible the official state book.

"The legislature has spoken and so has the governor," he said. "Now the ball is back in the legislature's court, and, as before, we defer to their judgment in this matter." Reported in: *The Tennessean*, April 14.