NEWS IS IT LEGAL?

LIBRARIES

Santa Cruz, California

How serious was the breach of patron privacy at the Santa Cruz Public Library (SCPL)?

The Santa Cruz County Grand Jury (which is part of the civil court system, and has no power to issue criminal indictments, only reports and recommendations) said that SCPL from 2016 through 2018 used a data analysis tool from Gale Analytics on Demand that may have violated patron privacy policies. A grand jury report issued on June 24, 2019, entitled *Patron Privacy at Santa Cruz Public Libraries,* said the software blended patron data with other data from Experian Mosaic.

With more than three hundred pieces of additional consumer data per patron, "the library holds significantly more household-level data in its computer system than patrons originally provided," the Grand Jury reported. The information was used to help the library's long-term strategic planning, but the program was inconsistent with SCPL's privacy policy, and library administrators did not inform library patrons that it was being used, and did not seek their consent, according to the grand jury report.

The report also found that library administrators did not review the contract provided by Gale Analytics on Demand, and found the contract "unclear" and lacking in language that protects patrons.

SCPL Director Susan Nemitz said the software was intended to help the library system focus its programs and services.

"Because we collect so little data about our patrons it can help us better understand them," she said. "A lot of libraries have embraced this in a big way." Nemitz said that the library used the program to study whether it was reaching people of color and low-income people and to learn who was using the libraries geographically.

Under state law, organizations typically have ninety days to respond to grand jury reports. They are not, however, required to implement any of the suggested changes.

Prior to release of the grand jury report, SCPL had stopped using Gale Analytics on Demand, and reworked its privacy policy. Reported in: co.santa-cruz.ca.us, June 24, 2019; *Register-Panjaronian,* June 28.

Boise, Idaho

How much content will be blocked for Wi-Fi users in Idaho's public libraries when a new internet filtering law takes effect next year?

In early April 2019, Republican Governor Brad Little signed into law legislation that adds publicly accessible wireless internet to a law that requires libraries to filter access on their internet services so that obscene and pornographic material can't be accessed.

The amendment is intended to prevent minors from using personal laptops, tablets, smartphones, or other devices to access pornographic sites. Previously, the law only dealt with publicly accessible computers. The new law goes into effect on July 1, 2020.

Officials say public libraries will have to update their policies, and that up to 35 rural libraries might need to install equipment. The estimated cost is up to $2,500 per library, but possibly much less depending on the type of system. Reported in: *Associated Press,* April 8, 2019.

Worcester County, Maryland

Should a lecture on the US Constitution at a public library be cancelled when critics calling themselves patriots threaten violence?

Worcester County Commissioners praised Worcester County Library Director Jennifer Ranck for putting safety first when deciding not to proceed with a lecture on impeaching the president in an area where he has widespread support.

The lecture was part of a series on the Constitution hosted by Howard Sribnick, the president of the Worcester County Library Foundation and a former Worcester County Democratic Central Committee chairman. It was scheduled for Wednesday, March 6, 2019, at the Worcester County Library's Berlin branch.

The Main Street Patriots Eastern Shore, Maryland, started a campaign on Facebook on Friday, March 1, posting a caption above an article entitled, "America's Second Civil War Has Already Begun." They wrote, "How many of you local folks will be at the Berlin library on Wednesday . . . for the primer (hosted by Democrats of course) on how to either impeach Trump or remove him from office via the 25th Amendment? They will collude and conspire to take away your vote (Trump won here in Worcester County by almost a 2 to 1 margin), will you be there to stand up for the truth?"

"Someone should take them out," another person commented.

The session was canceled. "When people threatened to disrupt the presentation, we thought that would raise a safety issue for those who may be trying to attend the program, or just those who were using the library at that particular time on that particular day," Ranck said in an interview.

Nearly three weeks later, some of the commissioners brought up the incident when she appeared at Worcester County Commission's meeting on March 26 on an unrelated library funding issue. They thanked Ranck and the library board for acting

"professionally" during "the situation down at the library." Reported in: *Ocean City Times,* March 29, 2019.

Columbus, Newark, and Delaware County, Ohio

Was it wrong for two Ohio public libraries to give in to pressure and withdraw their support for events focusing on drag queen and LGBTQ (lesbian, gay, bisexual, transgender, and queer) culture, or wrong for them to schedule such events in the first place?

The Delaware County Library had scheduled "Drag Queen 101" for Wednesday, June 5, 2019. The library said several teens had requested a class focused on the theatrical craft of drag performances. Selena T. West, a well-known drag queen from Columbus, was to be the instructor for the workshop.

But library director George Needham announced on May 29 that the event was canceled after the library received threatening messages, some from outside the area. The sponsors moved the event to a privately-owned bookstore nearby called Secret Identity Comics.

Elsewhere in the same state at nearly the same time, the Emerson R. Miller library in Newark, in Ohio's Licking County, scheduled "Galaxy of Diversity: A LGBTQ Teen Event" for Friday, June 7. A powerful Republican politician, Ohio House Speaker Larry Householder, issued an open letter on May 31 stating, "Taxpayers aren't interested in seeing their hard-earned dollars being used to teach teenage boys how to become drag queens. I expect this to end immediately." His letter did not name any libraries, but a spokesperson confirmed that Householder had the Delaware County and Licking County libraries in mind. Householder represents neither; his district is in Perry County.

Licking County Library Director Babette Wofter said she canceled the "Galaxy of Diversity" event because it became too difficult for the organization to control the misinformation circulating about it.

The Newark County Pride Coalition, which was co-sponsoring the "Galaxy of Diversity" event, stated in an open letter of its own that the event was meant to be an arts and crafts project and safe-sex educational program, with only an "optional make-up tutorial." The coalition asked Householder to respect the civil liberties of Newark residents, noting that the US Supreme Court has affirmed the freedoms of speech and expression for the LGBTQ community.

Householder dismissed the concerns about free speech. "Let me be crystal clear: This isn't about banning books or banning thought or any other red herring argument," he wrote. "This is about right and wrong. This is about being good stewards of the public's money."

The Newark coalition noted that no public money would have been used for the program, which would have taken place after library hours and would have been funded by a non-governmental grant.

A group of House Democrats from Central Ohio, in a news release, called Householder's comments "unfortunate." The Democrats' statement said, "the promise of America is . . . we all agree to let everyone have their voice. That is certainly true for the nearly 500,000 LGBTQ Ohioans."

West, who led the Delaware County's "Drag Queen 101," said the June 5 class went even better than expected. She said only about five people had signed up through the library, but 30 were in attendance for the event at the Secret Identity store. Reported in: ThisWeekNews.com, May 21, 2019, June 1; *CityBeat Cincinnati,* June 1; cleveland.com, June 2.

Austin, Texas

When should police be called on teenagers in a public library, and can library staff find another way to intervene rather than having a 13-year-old arrested in front of younger children?

Njera Keith, a teacher at an alternative school that holds some of its classes in the Carver Branch of the Austin Public Library, said she was entering the library with a six-year-old student when they saw a police officer patting down thirteen-year-old LaTashia Milligam. The teenager was handcuffed and had no shoes on.

Keith said her young student immediately began shaking. "She's shocked that this little girl that we were just interacting with is now in handcuffs," she said.

According to library staff, LaTashia was arrested for an existing warrant, after the parent of another student called police and accused her of threatening to attack her daughter.

Keith, who is also the executive director of an advocacy group called Black Sovereign Nation, said authorities should never have been called. Instead, a staff member or other responsible adult should have intervened. After the incident, Black Sovereign Nation members tried to speak with library staff to address concerns about library policies regarding minors. When they finally did, there was no consensus about how to move forward.

Austin Public Library policy states that children under ten cannot be left unsupervised in the library unless accompanied by someone who's at least seventeen. If staff members feel a child is unsafe or has nowhere else to go, they should refer the child to the Austin Police Department.

Keith said there was "no concrete policy" to guide staff members in LaTashia's case.

Black Sovereign Nation and Counter Balance: ATX launched a campaign called No Sanctuary for Black Futures aimed at changing Austin library policies. They are asking for more diversity training for staff and more comprehensive policies regarding minors. Organizers are also asking for a citywide policy requiring staff to contact the guardian of a child if they come in contact with police or have some other conflict.

Kristina Brown, Black Sovereign Nation's deputy director, said libraries "are spaces for oftentimes marginalized people to have internet access and obviously to read books and have access to information. And we are not against that, obviously, we just want those spaces to be safe," with patrons not at risk of harsh treatment due to stereotyping. Reported in: *Austin Monitor,* May 9, 2019.

SCHOOLS

Houston, Texas

When a school institutes a parental dress code for when they visit the school, is this discrimination on the basis of race or class?

Under a new dress code at James Madison High School in Houston, parents can't be on campus if they're wearing hair rollers, a shower cap, or pajamas. Other banned clothing includes revealing leggings, low-cut tops, sagging pants, torn jeans, and Daisy Duke shorts. In a memo, the school's principal said that if parents break the rules, they will not be permitted inside Madison High until they return "appropriately dressed for the school setting."

The principal said this maintains the school's "high standards."

Others said this discriminates against women of color who use caps and rollers to protect their hair.

"The first thing I thought was this is anti-blackness," said Roni Burren, who teaches at the University of Houston's College of Education. She's also an activist who successfully campaigned against a major textbook company after her son showed her his book calling slaves "immigrants."

Burren said this kind of dress code is part of a long history of policing black women's hair and appearance in the United States, and it reflects that internalized racism is real.

What's more, she said that a dress code for parents doesn't have any connection to instruction and discourages parents from coming to school.

The Texas Education Agency leaves it up to local school districts to set dress codes. The Houston district declined to comment.

The dress code at Madison High was issued after KPRC-TV reported the school turned away a mom who tried to enroll her daughter at Madison because she was wearing a T-shirt dress and headscarf. Reported in: *Houston Public Media,* April 24, 2019.

Madison, Wisconsin

Is a public school teacher's proclamation of their personal transsexual identity in class an exercise of the teacher's First Amendment right of free speech—or is telling students what pronoun to use for the teacher a violation of the students' First Amendment rights?

A science teacher at Allis Elementary School in the Madison (Wisconsin) Metropolitan School District had been known as Mark "Vince" Busenbark, and was addressed as "Mr. B." by students. The teacher and the teacher's wife (whose last name is Steel) produced a home video explaining the teacher's "non-binary" identity. The video introduced the teacher's new name, Vica Steel. It requested that students call the teacher "Mix Steel" or "Mx. Steel" instead of "Mr. B," and refer to the teacher as "they" instead of "he."

In the video, the teacher reads a book titled *They Call Me Mix*. A passage in the book says: "'BOY or GIRL?' Are you a boy or a girl? How can you be both? 'Some days I am both. Some days I am neither. Most days I am everything in between.'"

On Facebook, the teacher said the purpose of the video was "all so [the children] can know who I am and who I am becoming."

Liberty Counsel (LC), an activist Christian ministry with offices in central Florida, Virginia, and Washington, DC, called it "inappropriate activism in the classroom" when the teacher showed the video to every student in grades K-5 at the school. In a letter sent in June 2019 to Superintendent Jennifer Cheatham, LC said this "appears to violate several district policies, as well as the constitutional prohibition against schools enforcing any kind of 'orthodoxy.'"

That restriction, stated by the US Supreme Court, is, "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein."

Under provisions of Wisconsin law, Liberty Counsel asked for any emails, flyers, notes, text messages, and other district communications asking parental permission to show the "coming out" video to students. It also requested all communications from Allis Elementary Principal Sara Cutler, Vice Principal Andrea Alrichichi, or Busenbark "notifying the district of the plan to show the video, or

requesting district permission to show the video to the children."

LC also wants to see all emails referencing the video as the cause of confusion to children, communications approving Busenbark's use of "Mix" or "Mx.," and any other communications referencing the controversy.

LC claims the teacher's actions may conflict with the school district's wellness policy, which states instruction should be "age-appropriate, medically accurate, and non-stigmatizing," and its policies regarding controversial issues, the use of district resources, and "political activities." Reported in: WND TV, June 4, 2019.

COLLEGES AND UNIVERSITIES

Montgomery, Alabama

Should free speech be guaranteed on college and university campuses, even if the speakers are controversial or unpopular, and they might induce violent reactions?

Alabama Governor Kay Ivey signed a bill into law on June 6, 2019, that will prevent Alabama's taxpayer-funded public universities from limiting free expression and student speech to "free speech zones" on campus. In particular, the speech policies must make clear that the outdoor areas of a public college's campus shall be deemed a public forum for members of the campus community.

Known as House Bill 498, the law also ensures that if hecklers choose to protest and intimidate guest speakers on campus, the universities cannot capitulate to the hecklers by forcing the speaker to pay for security costs that have arisen from the protest. The law will go into effect next year, on July 1, 2020.

Free speech zones, which have been touted by some as ways to allow students to express a variety of opinions, even if the speech might trigger strong, possibly violent reactions, often require school faculty or administrators to be notified in advance and approve demonstrations in the zones. Critics say such a process places an undue restriction on First Amendment rights.

The bill's sponsor, Republican state Representative Matt Fridy, called such efforts by universities "unfair" attempts to crack down on viewpoints with which they disagree. "Alabama's university campuses should be places where ideas are freely debated and students are exposed to a variety of viewpoints. Unfortunately, across the nation—occasionally even here in Alabama—college administrators have used unfair, arbitrary speech codes to silence speech that is deemed 'offensive.' Oftentimes, politically and religiously conservative groups are targeted," Fridy said in an interview after the bill was signed.

During the House floor debate, Democratic state Representative Napoleon Bracy opposed the bill, saying that university administrators should focus on the safety of students on campus and citing concerns that certain speech could incite violence in some students. Bracy said college administrators should be able to determine which speakers are invited to speak at their institutions.

Most Alabama colleges had opposed the bill, according to *Alabama Political Reporter.*

The bill would not apply to private colleges and universities, because as private entities they have the right to set their own standards. Public institutions, on the other hand, are covered by the First Amendment, Fridy said.

H.B. 498 was approved by a bipartisan 24 to 1 vote in the Alabama State Senate and a 73 to 26 vote in the House of Representatives. Reported in: *Alabama Political Reporter,* June 7, 2019; *The Hill,* June 8.

Des Moines, Iowa

Will a new "free speech" law in Iowa change how public universities and community colleges uphold the "fullest degree of intellectual freedom and free expression"?

The law, which Governor Kim Reynolds signed on March 27, 2019, requires state universities and community colleges to adopt policies respecting free speech on campus. But Democrats argued one section in the new law will pave the way for discrimination.

Conservative students and groups across the country have claimed their free speech rights have been restricted on liberal campuses in recent years, causing a rash of new proposals from state lawmakers. Reynolds, a Republican, said she was proud to sign the Iowa law. "Our public universities and community colleges should always be places where ideas can be debated, built upon, and creative thoughts flourish without limits," she said in a news release.

Katherine Tachau president of the University of Iowa (UI) chapter of the American Association of University Professors (AAUP), said freedom of expression is at the heart of universities. It's not clear how the law will change the UI campus, but the AAUP worries about "undesirable unintended consequences." Tachau said, "As a public university we are bound by constitutional law on freedom of expression, so we were not at all convinced that we needed a new law to achieve what we achieve most of the time," Tachau said.

During floor debate in the Iowa House this month, Democrats stressed that they support free speech but said one sentence in the bill kept them from voting for it. That sentence

would allow student groups that receive public university funding to bar certain students from leadership positions based on their identity, Democrats argued. The AAUP also takes issue with the section.

Versions of the Iowa law have been debated for years, but lawmakers doubled their efforts after a federal court ruled in favor of a Christian group that argued UI discriminated against it. The group, Business Leaders in Christ, was accused of barring a student from a leadership position because he is openly gay. The university later revoked the group's status as a registered student organization, but the court found the university was not uniformly applying its human rights policy. Republicans have touted the incident as evidence that free speech on Iowa campuses is being stifled.

The law directs the governing boards of the state's three public universities and numerous community colleges to adopt policies that state, in part, that "the institution must strive to ensure the fullest degree of intellectual freedom and free expression."

The law also designates outdoor areas on campus as public forums. The law specifies "that it is not the proper role of an institution of higher education to shield individuals from speech protected by the First Amendment to the Constitution of the United States, which may include ideas and opinions the individual finds unwelcome, disagreeable or even offensive."

The Senate approved the measure 35–11 earlier this month, with some Democrats in support. But in the House, where it passed 52–44, Democrats all voted against it or said they opposed it. Reported in: *Des Moines Register,* March 27, 2019.

Frankfort, Kentucky

Will Kentucky institutions of higher education stop limiting controversial expression to "free speech zones" without waiting for court rulings, or will students need to sue, as they now can under a new law?

Kentucky Governor Matt Bevin on March 26, 2019, signed HB 254 into law, protecting free speech at the commonwealth's public colleges and universities by granting students the "broadest possible latitude to speak, write, listen, challenge, learn, and discuss any issue." The bill requires institutions to maintain "a marketplace of ideas where the free exchange of ideas is not suppressed," and explicitly prohibits the use of restrictive free speech zones.

"College leaders should promote the fact that their campuses host diverse viewpoints, not corral dissenting speakers into pre-approved areas where they determine it's 'safe' to have an opinion," said Robert Shibley, executive director of the Foundation for Individual Rights in Education (FIRE). "We commend Kentucky legislators for making free speech a priority, and encourage other states to follow their lead."

Ten percent of colleges and universities surveyed by FIRE maintain a free speech zone, according to FIRE's *Spotlight on Speech Codes 2019* report. Free speech zones have repeatedly been struck down by courts or voluntarily revised by colleges as part of lawsuit settlements brought by students.

The University of Kentucky, Morehead State University, and Murray State University are among the institutions that will need to change or clarify their policies to comply with the law.

Under the law, Kentucky's public colleges and universities are prohibited from charging students security fees based on the expressive content of their campus events or the ideas of their invited guest speakers. The law also prevents institutions from "disinviting" speakers invited by a student, student organization, or faculty member.

The new legislation also provides a cause of action, which allows students to sue institutions in state court for violations of the act. Reported in: thefire.org, March 26, 2019.

Cambridge, Massachusetts

Is it hypocritical for a university that was once associated with slavery and segregation to deny admission to an incoming freshman because he at one time wrote and shared a document that used the word "nigger"?

That is the question Kyle Kashuv, a pro-gun rights survivor of the 2018 mass shooting in Parkland, Florida, raised after Harvard University rescinded its offer of admission, apparently because after he was admitted, racist comments he had made two years earlier surfaced online.

Kashuv became an activist for gun rights shortly after the Parkland shootings. He was accused in May 2019 of having used racial slurs in a shared Google Doc in 2017. He wrote the N-word multiple times in the document and followed the slurs with "practice uhhhhhh makes perfect." Shortly after the comments became public, he posted a statement on Twitter calling the racist language he had used "callous and inflammatory," but did not formally apologize for it.

In June 2019, Kashuv posted documents to Twitter that appeared to show Harvard had second thoughts about granting him admission. According to the documents, the university's admissions committee had decided that Kashuv's language in 2017 violated the conditions of his acceptance, and therefore threatened to rescind his admission following an investigation.

"We have become aware of media reports discussing offensive statements allegedly authored by you," said a letter, dated May 24. "As you know, Harvard reserves the right to withdraw an offer of admission under various conditions, including 'if you engage or have engaged in behavior that brings into question your honesty, maturity, or moral character.'"

On Twitter, Kashuv said that his response to the committee took "full responsibility for the idiotic and hurtful things I wrote two years ago."

But on June 3, he said, the university wrote that he would no longer be accepted into Harvard's Class of 2023, this fall's freshman class. (Rachael Dane, director of media relations at Harvard, said it does not comment publicly on the admissions status of individual applicants.)

Kashuv criticized Harvard's decision on Twitter, relating the situation to the institution's own past associations with slavery and segregation. "If Harvard is suggesting that growth isn't possible and that our past defines our future, then Harvard is an inherently racist institution," Kashuv tweeted. "But I don't believe that."

Kashuv's status as a right-wing activist grew considerably after the 2018 shootings, which claimed 17 lives at Marjory Stoneman Douglas High School. He gained attention mostly for his advocacy for campus safety through gun rights. Kashuv has made frequent appearances on Fox News and has met with President Trump. Reported in: *Chronicle of Higher Education,* June 17, 2019.

Crete, Nebraska

Was it offensive for a library at Doane University to display historical photos of students in blackface? Was it a violation of academic freedom when the university closed the exhibit and put the librarian on leave?

In April 2019, a student complained about two photos in a display called "Parties of the Past" in Doane University's Perkins Library on the Crete campus. This was part of an exhibit of historical photographs that Library Director Melissa Gomis had curated in March, of memorabilia from student scrapbooks housed in university archives. The two photos showed students attending a 1926 Halloween party, apparently in blackface. A blurb from a local newspaper at the time indicated it was a campus masquerade party. But there was no accompanying note from the curators explaining why the photos were included.

After speaking with the concerned student, Gomis decided to remove the blackface photos due to concern for the student.

Then, under orders from the provost, the entire exhibit was removed. That same day, Gomis was told to collect her things from her office, and was suspended indefinitely.

Doane University administrators said that displaying the photos ran counter to the university's values and, as presented, served no educational purpose.

Some members of the faculty who support the librarian disagree. They said that Doane interfered in a learning moment, albeit a painful one, that their colleague was already working to right.

"Were some of our students genuinely offended or hurt by the library display? Yes," said Brian Pauwels, associate professor of psychology at Doane and vice president of the campus's American Association of University Professors (AAUP) advocacy chapter. "Was suspending the librarian in response to that hurt heavy-handed and in violation of the academic freedom that is necessary to do her difficult job every day?"

Pauwels continued, "Can't the answer to both questions be yes? Because lots of people want us to pick one or the other. These are values that are hard to define, and now they're colliding with one another."

Doane's AAUP chapter approved a statement condemning Gomis's suspension.

Other professors think Doane University made the right call.

Many historians have argued that there is value in showing racism that existed in the past at universities and in other parts of society, even if seeing it makes people uncomfortable today. Yet many also argue that this kind of content should be put into context.

The AAUP said Gomis's suspension was a "consequence of a grievance complaint" without due process nor an investigation.

Citing censorship guidelines from the American Library Association, Doane's AAUP chapter described the university's forced removal of the exhibit as "an unambiguous example of censorship," coming from "outside the library, performed by a person with no training in library and archival science." That is in contrast to Gomis's initial self-censorship, which was "driven by her genuine concern to respond to the student and to avoid external censorship."

When an educator "is pressured to remove content from a lecture, lesson or display that was created according to the current methods of the profession, then a violation of academic freedom has occurred," the AAUP said.

Doane President Jacque Carter sent an all-campus memo saying that blackface "has a history of dehumanization and stereotyping, which perpetuates systemic racism in society." He apologized for the photos and the hurt they had caused. "Such an insensitive action is unacceptable and will

not be tolerated now or in the future," Carter wrote.

Doane's AAUP chapter took issue with that statement, saying that an environment in which a president can judge exhibits as "sufficiently controversial or offensive that they must be removed partially or in their entirety at the president's discretion" constitutes "an infringement of the academic freedom that is essential to the work of Director Gomis, all other faculty and, by extension, the students of the university."

Mark Orsag, a professor in Doane's history department, said the photos, without context, were "clearly disrespectful to the African American faculty, staff and students on this campus." Given national controversies over similar pictures, he added, "putting those photos up in that manner was tone-deaf in the extreme and demonstrated a fundamental lack of common sense." Academic freedom "carries with it the responsibility to act respectfully, with fairness and with common sense," he added, arguing that "such offensive displays" are explicitly against Doane's anti-harassment policy.

Amanda McKinney, executive director of Doane's Institute for Human and Planetary Health and director of its Open Learning Academy, said the key issue is not content but context. "There was nothing there with the pictures to indicate whether this was right or wrong, racist or not, condoned by the librarian or not," McKinney said. Given the display title, one "might even think we were celebrating it. That's the crux of the issue," she added.

Quoting AAUP's policy on academic freedom, McKinney said that teachers "are entitled to freedom in the classroom in discussing their subject, but they should be careful not to introduce into their teaching controversial matter that has no relation to their subject." Additionally, she continued, quoting the AAUP, professors' "special position in the community imposes special obligations. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their utterances."

McKinney said that Doane was within its rights to suspend Gomis under its anti-harassment policy, pending the investigation. She said she thinks it is unlikely that Gomis would be fired.

Do librarians have academic freedom? Doane's AAUP chapter declared, "We assert that the library is a fundamental classroom, where knowledge and learning begin." Doane's AAUP chapter further argues that librarians "are particularly vulnerable to sanctions resulting from public disapproval of their collections and exhibits," since they deal with an "enormous range of materials that inevitably will include items that some, and perhaps even many, will find objectionable." And unlike professors in a dynamic classroom setting, the chapter wrote, librarians can't "respond instantly to questions or reactions from their audience, or explain in the moment their decision-making process in presenting such materials."

Pauwels argued that the broader issue is that one instance of even well-meaning censorship sets the stage for worrisome instances of censorship going forward. Defending academic freedom "here and in the long term" ultimately ends up benefiting students, he said. Reported in: *Inside Higher Ed,* May 6, 2019.

Plymouth, New Hampshire

Should the free speech of faculty members be limited when they speak in defense of someone accused of sexual assault?

University System of New Hampshire (USNH) and Plymouth State University (PSU) signed an agreement on February 15, 2019, to pay a former adjunct lecturer $350,000 to avoid a potential lawsuit after she lost her job for speaking in support of a former Exeter High School guidance counselor who sexually assaulted a student.

Nancy Strapko, a local mental health counselor, reached the settlement with the university system after controversy arose when Strapko and several educators and other professionals pleaded for leniency at Kristie Torbick's sentencing in Rockingham County Superior Court in July 2018. The thirty-nine-year-old Torbick had pleaded guilty to four counts of sexual assault on a fourteen-year-old student.

Strapko, an associate professor emeritus and former graduate school health education coordinator at PSU, was one of twenty-three people who wrote letters supporting Torbick. Strapko also testified at Torbick's sentencing on July 9, 2018, asking for leniency. Judge Andrew Schulman sentenced Torbick to two-and-a-half to five years in prison. The sentence was lighter than the five to ten years prosecutors sought.

PSU dismissed Strapko on August 1, 2018, saying in a public statement that she would not be rehired as an adjunct teaching lecturer nor employed in any other capacity at the university.

In her letter to the court, Strapko wrote, in part, "Kristie takes full responsibility for her actions with her 'victim.' I put this in (quotes) because I am aware that her 'victim' was truly the pursuer in this case."

Strapko's description of the victim as the "pursuer" outraged many, including advocates for sexual assault survivors.

In its statement announcing her dismissal, the university wrote, "In

PSU's opinion, portraying a fourteen-year-old sexual assault victim as a 'pursuer' is legally wrong and morally reprehensible."

USNH general counsel Ronald Rodgers, along with Strapko's attorneys, released a joint public statement on the settlement: "The University System of New Hampshire and Dr. Nancy Strapko have reached a mediated resolution of their concerns arising out [of] an assessment Dr. Strapko provided in a criminal sentencing hearing. The parties abhor all forms of interpersonal exploitation, in particular the sexual abuse of children. They also agree on the importance of witnesses participating in the criminal justice process, including criminal sentencing."

The amount of the settlement was released in response to a request for information under the Right-to-Know law, filed by the *New Hampshire Union Leader.*

PSU professors Michael L. Fischler and Gary Goodnough also came under fire for their letters of support.

Fischler, a professor emeritus of counselor education and school psychology, and Goodnough, a professor of counselor education who served as Torbick's adviser and internship supervisor, both agreed to complete additional training on sexual assault and to work closely with PSU faculty, students, and staff to address the issues and the concerns created by their letters, the university said in a statement.

But Manchester-based attorney Jon Meyer, who is representing Fischler, has criticized PSU for disciplining his client, insisting that he was punished for exercising his constitutional and statutory free expression rights.

Meyer also argued that the action will have a "chilling effect" on people who are asked to testify during future sentencing proceedings.

Fallout from the Torbick sentencing also led to the resignation of Bedford school superintendent Chip McGee. He faced pressure after Bedford High School educators also supported Torbick, who was a Bedford counselor before she was hired in Exeter.

Newfound Regional High School guidance counselor Shelly Philbrick also resigned after she spoke at Torbick's sentencing.

The Foundation for Individual Rights in Education (FIRE) wrote to PSU in September 2018 to explain that the First Amendment prohibits a public university from punishing its professors for testifying in judicial proceedings.

"Professor Strapko was fired for nothing more than her witness testimony—and that is a blatant violation of her First Amendment rights and a clear violation of Plymouth State's free speech promises," said Zach Greenberg, program officer in FIRE's Individual Rights Defense Program. "Plymouth State disregarded the profound societal importance of ensuring that people with relevant information come forward when called to testify in criminal trials—a civic responsibility that forms the backbone of any functional system of justice."

After the settlement was announced, FIRE's Greenberg said, "This settlement represents the high costs of failing to uphold the First Amendment rights of faculty at a public university. Universities should learn from Plymouth State's mistake by committing to protect free speech on campus—and honoring those commitments in practice." Reported in: *New Hampshire Union Leader,* April 29, 2019; thefire.org, April 30.

New York, New York

Is a policy asking university students to show identification after 11 p.m. discriminatory? It might be, if the policy is selectively enforced.

Barnard College placed several public safety officers and a supervisor on administrative leave following accusations of racial profiling.

The issue arose when a video recorded by a Columbia University student showed what happened at the Barnard library on April 11, 2019, at 11:30 p.m. The student was held and asked for identification while trying to enter the library.

Current college policy states that students must show ID after 11 p.m., but students say that policy is not routinely enforced.

Barnard's president apologized to the Columbia University student and said the college will review its policies. Reported in: CBS New York, April 15, 2019.

Philadelphia, Pennsylvania

Do principles of academic freedom and free speech mean that a university should grant a platform to a professor whose "dangerous" ideas may cause harm and incite violence?

At the University of the Arts (UArts) in Philadelphia, where the critic Camille Paglia has taught for thirty years, a faction of art-school students wants her fired and banned from holding speaking events or selling books on campus. Their petition says her ideas "are not merely 'controversial,' they are dangerous."

Others believe this would set a dangerous precedent that would undermine freedom of expression and free academic inquiry.

Conor Friedersdorf, a staff writer for the *Atlantic* magazine, covered the controversy in a lengthy article. It is rare for student activists to argue that a tenured faculty member *at their own institution* should be denied a platform, Friedersdorf's magazine pointed out.

Paglia has been outspoken and controversial ever since her first book, *Sexual Personae: Art and Decadence From Nefertiti to Emily Dickinson*, was published in 1990. The book criticized feminist thinking about rape and argued that sex differences are rooted in biology. It was savaged by feminist critics, but became an unexpected, 700-page bestseller. And it sparked a national debate about art, history, gender, ideas that offend, free inquiry, and political correctness.

The latest student protests against Paglia began in the spring of 2019, when it was announced that she would give a lecture titled "Ambiguous Images: Sexual Duality and Sexual Multiplicity in Western Art."

According to a letter that two student activists released, "Joseph McAndrew (they/them), a gender non-binary creative writing major, brought this lecture to the student body's attention through social media and raised their concerns to Title IX and other University administration about the school giving Camille a platform. This led to the University reaching out to Deja Lynn Alvarez, a local transgender activist, to facilitate a talk-back after Camille's lecture. Students were informed the day before the lecture that Camille had no plans to stay for the talk-back."

UArts administrators declined to cancel the public lecture that Paglia was scheduled to deliver. The student activists responded by protesting the event. Before the event was over, someone pulled the fire alarm in the building, causing it to be evacuated.

To help justify the effort to suppress Paglia's speech, student activists pointed to an interview posted to YouTube in which she dismissed some allegations of campus sexual assault. For example, one student wrote in an email: "As a survivor of sexual assault, I would never feel comfortable taking a class with someone who stated that 'It's ridiculous . . . that any university ever tolerated a complaint of a girl coming in six months or a year after an event,' or that 'If a real rape was committed, go friggin' report it to police.' Perhaps this is an 'opinion,' but it's a dangerous one, one that propagates rape culture and victim-blaming. For this and other reasons, I find her place as an educator at this university extremely concerning and problematic."

After Paglia's interrupted speech, UArts President David Yager released a long statement defending free expression. Its core message:

> Across our nation it is all too common that opinions expressed that differ from one another's—especially those that are controversial—can spark passion and even outrage, often resulting in calls to suppress that speech. That simply cannot be allowed to happen. I firmly believe that limiting the range of voices in society erodes our democracy. Universities, moreover, are at the heart of the revolutionary notion of free expression: promoting the free exchange of ideas is part of the core reason for their existence. That open interchange of opinions and beliefs includes all members of the UArts community: faculty, students and staff, in and out of the classroom. We are dedicated to fostering a climate conducive to respectful intellectual debate that empowers and equips our students to meet the challenges they will face in their futures. I believe this resolve holds even greater importance at an art school. Artists over the centuries have suffered censorship, and even persecution, for the expression of their beliefs through their work. My answer is simple: not now, not at UArts.

Later, when student activists launched their online petition, they included the demand, "Yager must apologize for his wildly ignorant and hypocritical letter."

To better understand the student-activist perspective, Friedersdorf emailed Sheridan Merrick, who posted the Change.org petition against Paglia, asking how have the professor's "dangerous" ideas harmed students.

In reply, Merrick cited statistics about the percentage of transgender adults who report having attempted suicide or suffered hate crimes. From there she reasoned:

> Paglia's comments have echoed the hateful language that pushes so many transgender people to contemplate suicide, and encourage transphobic people to react to transgender people violently. . . . I personally know at least one person who, due to Paglia's comments, has experienced suicidal thoughts and has considered leaving the University. The comments that many of us have been receiving online have caused public safety at our school to be told to up their security game, in case our (very queer) student body is targeted by angry supporters of hers. This is what we mean when we say that her views are not merely controversial, but dangerous."

Friedersdorf disagrees. The *Atlantic* article concludes that the argument that

> a speaker is responsible for harms that are theoretical, indirect, and so diffuse as to encompass actions of strangers who put themselves on the same side of a controversy—is untenable. Suppressing speech because it *might* indirectly cause danger depending on how people other than the speaker *may* react is an authoritarian

move. And this approach to speech, applied consistently, would of course impede the actions of the anti-Paglia protesters as well.

. . . What's more, when student activists strategically engage in protests, callouts, and other behavior expressly calculated to "make life more difficult" for others, they could indirectly inspire outside parties to engage in threats or even attacks. . . . adopting different standards for different identity groups—which would of course never fly in a legal context—would ultimately hurt historically marginalized groups.

. . . The identitarian conceit is that trans people and survivors of sexual assault can't learn from Paglia, because she renders them "unsafe." Meanwhile, cis [non-trans] white males are acculturated to believe that they can always learn from anyone, even professors overtly hostile to their race, sexual orientation, or gender identity. In this way, left-identitarianism encourages historically marginalized groups to believe that they are less resilient and less capable than their white, male classmates. They suggest, falsely, that "harm" is the only possible result of listening to controversial (or even offensive) ideas.

There are, finally, political costs of illiberal activism. By targeting Paglia's job, student activists may alienate people who are open to substantive critiques of her ideas, yet insistent on the absolute necessity of safeguarding a culture of free speech, regardless of whether the speech in question is "correct" or "incorrect." They fail to heed Henry Louis Gates's prescient warning not to divide the liberal civil-rights and civil-liberties communities.

The activists also fail to heed a much older lesson that art students ought to know best: Nothing makes an act of free expression more intriguing than an attempt to censor it.

Reported in: *The Atlantic,* May 1, 2019.

Pierre, South Dakota

Are colleges really protecting free speech when they limit it to "free speech zones" on campus?

On March 20, 2019, South Dakota Governor Kristi Noem signed into law HB 1087, which will codify free speech protections for students at South Dakota's public colleges and universities. The law prohibits South Dakota public colleges and universities from quarantining student expression into small, misleadingly labeled "free speech zones."

According to a count maintained by the Foundation for Individual Rights in Education (FIRE), this made South Dakota the 13th state to pass legislation banning public colleges and universities from relegating student expression to free speech zones. The others are Virginia, Missouri, Arizona, Kentucky, Colorado, Utah, North Carolina, Tennessee, Florida, Georgia, Louisiana, and Arkansas. [*After South Dakota, Alabama and Iowa passed similar laws (see page 41). This raised the total to fifteen states with laws against restricting free speech on the campuses of public institutions of higher education.*]

South Dakota's HB 1087 also prevents institutions of higher education from discriminating "against any student or student organization based on the content or viewpoint of their expressive activity." The law guarantees that funds distributed to student organizations are allocated in a nondiscriminatory manner. It further states that belief-based student organizations are free to maintain policies that require leaders or members of the organization to "affirm and adhere to the organization's sincerely held beliefs."

FIRE Executive Director Robert Shibley said "'Free speech zones' send the false and illiberal message that a student's First Amendment rights are dangerous, and should be constrained within tiny, pre-approved areas of campus. We commend legislators in South Dakota for recognizing the critical importance of free speech to higher education, and encourage other states to follow their lead."

"HB 1087 is an important step toward ensuring no viewpoints are silenced at public institutions in South Dakota," said FIRE Legislative and Policy Director Joe Cohn. "By enacting this legislation, South Dakota is standing up for all students who wish to speak their minds freely on campus."

According to FIRE's *Spotlight on Speech Codes 2019* report, approximately 10 percent of top colleges nationwide maintain a free speech zone, despite the fact that the practice violates the First Amendment. Free speech zones have been repeatedly struck down by courts or voluntarily revised by colleges as part of settlements to lawsuits brought by students. Reported in: thefire.org, March 21, 2019.

San Marcos, Texas

What is the difference between a vote by the student government and official action by their university?

The Texas State University student government provoked outrage on April 8, 2019, by voting to ban a conservative student group, Turning Point USA, from campus.

The outrage of Charlie Kirk, founder of Turning Point USA, was quickly retweeted by his followers and picked up by conservative media sites. Greg Abbott, Texas' Republican governor, jumped into the fray, tweeting

that he looked forward to signing a bill to uphold free speech on college campuses, passed by the state Senate.

Lost in the initial outrage was a response from Margarita Arellano, the university's dean of students, who issued a statement saying that, while the student government has a right to pass a resolution calling for a ban of any student group, it does not have the authority to actually kick Turning Point USA off campus. Student organizations can be banned only if they are facing disciplinary sanctions, she wrote, and the campus chapter of Turning Point is not.

The resolution approved by the student government, but not acted on by the administration, called on the university to ban the campus chapter of Turning Point USA, citing its "consistent history of creating hostile work and learning environments through a myriad of intimidation tactics aimed against students and faculty." The resolution criticized the group's "Professor Watchlist," which "exposes" faculty members accused of discriminating against conservative students and promoting a liberal agenda.

Stormi Rodriguez, president of Turning Point's campus chapter, spoke during an open forum before the vote. Her remarks were interrupted by chants of "No more harassment, no more hate, remove Turning Point from Texas State!" The taunts continued as she left the meeting. She recorded them on Twitter. "If the left wants an example of what it looks like to be threatening and intimidating students, they should look in a mirror at #txst," she tweeted.

The Foundation for Individual Rights in Education (FIRE) said the university made the right call in rejecting the attempt to ban Turning Point USA. "The student government is free to call on the university to ban TPUSA, but it's a request that the university's administration cannot grant," Adam B. Steinbaugh, director of FIRE's Individual Rights Defense Program, wrote in an email. "Nor can the student government take steps to deprive the TPUSA chapter of benefits provided to other organizations due to objections to TPUSA's views." Reported in: *Chronicle of Higher Education,* April 10, 2019.

PRISONS
New York, New York

How much of a right to read do incarcerated people have? Are library book carts, rather than actual libraries, enough for prisoners to exercise that right?

On February 26, the New York City Council's Criminal Justice Committee heard testimony on Councilmember Daniel Dromm's bill, Int. 1184, that requires the Department of Corrections (DOC) to provide access to the library for all incarcerated people within 48 hours of entering the jail system. The Department would be required to report on the number of books they receive, the source of those books and, if books are censored, the reason for the censorship.

Only two of the city's eleven jail buildings at Rikers Island have permanent libraries—and these were created only recently, in July 2016 and April 2018. A third library only exists for a few hours one day a week, when librarians from the New York Public Library bring books into a gymnasium. Men in that particular jail are escorted to the makeshift library to peruse and check out books. Then, the remaining books are packed away into a closet until the following Friday.

For people in New York's other eight jail buildings, that leaves the book cart. Librarians of the city's public library systems bring a book cart around to the housing units where people can check books out. There's no uniformity as to how often a book cart is allowed onto a housing unit—for some units, it's once a week; for others, books might only come every other week or as often as twice a week.

For people in punitive segregation (129 inmates, as of November 30, 2018) who can spend anywhere from 17 to 23 hours in their cell, access seems to be even more spotty. DOC officials testified that people in punitive segregation do not have access to either a physical library or the library's book carts, a declaration that shocked and appalled Dromm and his colleagues. But librarians from the New York, Queens and Brooklyn public libraries later testified that they do indeed provide access to books and magazines for people in segregation as well as in the city's Enhanced Supervision Housing. In some units, they are able to meet the readers face to face; at others, the would-be reader receives a list of available genres. They choose one, submit the slip and in return receive a book.

Michael Tausek, the DOC's deputy commissioner for programming and community relationships, told the Committee that the DOC does not support the bill. "We do not believe that this bill would have the desired outcome of actually increasing the level of access to reading materials," he testified.

The librarians who actually work in the city's jails disagree. Nick Higgins, the chief librarian for the Brooklyn Public Library, told the committee that if each jail had a dedicated library, "we can do so much more." Reported in: *Gothamist,* February 27, 2019.

GOVERNMENT SPEECH
Washington, D.C.

When government agencies remove references to certain types of

discrimination from government websites, does this mean the government will no longer try to prevent such discrimination?

In the Spring of 2017, the Office for Civil Rights (OCR) at the Department of Health and Human Services quietly changed information on its website related to Section 1557 and discrimination against transgender and gender nonconforming people in healthcare settings. The changes were documented by the Web Integrity Project in 2018 (*see* JIFP, *Fall 2017–Winter 2018, page 70*).

New regulations announced on May 24, 2019, would roll back protections for transgender and gender nonconforming patients in healthcare settings. The proposed new rules reinterpret Section 1557 of the Affordable Care Act to exclude "gender identity" as a prohibited basis for discrimination.

With both the proposed changes to the rule, and the changes to text on the OCR website, "The current administration has rewritten large swaths of the implementing regulations of Section 1557 to limit the definition of discrimination, meaning women, LGBTQ people and limited English proficient individuals may again be shut out of vital health services and care because of biases against them," said National Health Law Program Executive Director Elizabeth G. Taylor in a press release.

At issue was whether Section 1557 of the Affordable Care Act, which prohibits discrimination based on sex, could be interpreted to also prohibit discrimination on the basis of gender identity and termination of pregnancy. The Obama administration had determined that the law did empower HHS to enforce prohibitions on such discrimination. But a federal court in Texas ruled against that view of the law, and issued a nationwide injunction prohibiting OCR from enforcing discrimination on the basis of gender identity.

The Sunlight Foundation wrote at the time that more content about prohibitions on sex discrimination was removed than appeared necessary to reflect the injunction.

The new rules indicate that advocates were right when they suspected that the Trump administration might seek to officially reinterpret Section 1557 to exclude transgender and gender non-conforming individuals from sex discrimination protections.

The administration framed the new rules as reflecting lawmakers' intent when Section 1557 was first enacted. Reported in: SunlightFoundation.com, May 29, 2019.

INTERNET

United States

Are students' rights to an education curtailed when they have no computer or internet at home?

An Associated Press analysis of census data indicates that nearly three million students around the United States struggle to keep up with their studies because they have no home internet. Unlike classrooms, where access to laptops and the internet is nearly universal, at home, the cost of internet service and gaps in its availability affect both urban and rural areas, the AP found.

In this "homework gap," an estimated 17 percent of US students do not have access to computers at home, and 18 percent do not have home access to broadband internet.

Students without home internet consistently score lower in reading, math, and science.

Students without internet at home are more likely to be students of color, from low-income families, or in households with lower parental education levels.

A third of households with school-age children that do not have home internet cite the expense as the main reason, according to federal Education Department statistics gathered in 2017 and released in May. The survey found the number of households without internet has been declining overall but was still at 14 percent for metropolitan areas and 18 percent in nonmetropolitan areas. Reported in: *Associated Press,* June 10, 2019.

Augusta, Maine

Can state laws effectively replace national "net neutrality" regulations issued by Federal Communications Commission under the Obama administration, then rescinded under the Trump administration?

Maine joined a growing number of states passing net neutrality laws. On June 25, 2019, Governor Janet Mills signed into law a bill that prohibits the state from using funds to pay internet service providers (ISPs) unless they adhere to "net neutral" services. Specifically, the bill defines "net neutral" services as a promise not to block lawful content, not to throttle internet speeds, and to not engage in paid prioritization.

"The internet is a powerful economic and educational tool that can open doors of opportunity for Maine people and small businesses," Mills said in a statement announcing her signing of the bill. "That potential should not be limited by internet service providers interested in increasing their profits. I hope net neutrality will be fully restored in federal law, but in the meantime I welcome this new law as a positive step forward for Maine and as a sign that we will protect a free and open internet for Maine people."

Maine's new law is similar to ones working their way through state legislatures in New York and New Jersey.

In 2018, two states—California and Vermont—passed net neutrality bills, but both states agreed to halt their implementation in the midst of being sued. Those bills will not go into effect while a federal court battle over the Federal Communications Commission's (FCC) repeal plays out. A decision from the United States Court of Appeals District of Columbia Circuit is expected this year. Reported in: *Daily Dot,* June 26, 2019.

FREE SPEECH
San Antonio, Texas

Are business owners' First Amendment rights violated when a government stops them from opening a store because of their religious beliefs and political donations?

The San Antonio City Council voted to exclude Chick-fil-A from the city's airport because the restaurant chain's Christian owners have donated to organizations that champion the belief that marriage is between a man and a woman. In mid-April 2019, the council narrowly rejected a proposal to reconsider its decision.

"Such censorship is blatantly unconstitutional," declared an editorial in the *San Antonio Express-News.* The newspaper wrote, "This incident is symptomatic of deeper problems. Many people believe they have the absolute truth with regard to issues of morality, sexuality, religion or politics, and that those who disagree are evil and must be censored or excluded. Similarly, many see people as fragile and argue that offensive speech is violence."

The editorial concludes, "This outlook corrodes our free speech foundations and should be rejected by all those who value the First Amendment." Reported in: *San Antonio Express-News,* April 21, 2019.

PRIVACY
Washington, D.C.

How much information should the government collect from foreigners who want to enter the country?

The US State Department is now requiring nearly all applicants for US visas to submit their social media usernames, previous email addresses, and phone numbers. In a vast expansion of the Trump administration's enhanced screening of potential immigrants and visitors, the department announced updated immigrant and nonimmigrant visa forms that now request additional information, including "social media identifiers," from almost all applicants.

The change, first proposed in March 2018, is expected to affect about 15 million foreigners who apply for visas to enter the United States each year.

Social media, email, and phone number histories had only been sought in the past from applicants who were identified for extra scrutiny, such as people who had traveled to areas controlled by terrorist organizations. An estimated 65,000 applicants per year had fallen into that category.

The department says collecting the additional information from more applicants "will strengthen our process for vetting these applicants and confirming their identity."

The new rules apply to virtually all applicants for immigrant and nonimmigrant visas. When it filed its initial notice to make the change, the department estimated it would affect 710,000 immigrant visa applicants and 14 million nonimmigrant visa applicants, including those who want to come to the United States for business or education.

The new visa application forms list a number of social media platforms and require the applicant to provide any account names they may have had on them over the previous five years. They also give applicants the option to volunteer information about social media accounts on platforms not listed on the form.

In addition to their social media histories, visa applicants are now asked for five years of previously used telephone numbers, email addresses, international travel and deportation status, as well as whether any family members have been involved in terrorist activities.

Only applicants for certain diplomatic and official visa types are exempted from the requirements. Reported in: Associated Press, June 1, 2019.

Washington, D.C., and many localities

Should federal agents have access to state and local license plate and drivers' records—including automated license plate readers that can track a vehicle's location—to help them deport undocumented immigrants?

More than 80 law enforcement agencies in the United States have agreed to share with US Immigration and Customs Enforcement (ICE) license plate information that supports its arrests and deportation efforts, according to the American Civil Liberties Union (ACLU), which obtained a trove of internal agency records.

The documents acquired by the ACLU show that ICE obtained access to a database with license plate information collected in dozens of counties across the United States—data that helped the agency to track people's locations in real time. Emails revealed that police have also informally given driver information to immigration officers requesting those details in communications that the ACLU said appeared to violate local laws and ICE's own privacy rules.

The files, which the ACLU obtained through a Freedom of Information Act request, have raised fresh concerns about ICE's monitoring of immigrants and the way local police aid the Trump administration's deportation agenda.

ICE has taken advantage of expanded automated license plate recognition technology, which allows cameras to take images of plates and link them to specific locations.

The documents show that ICE allowed agents—more than 9,000 of them, according to one email—working on civil immigration cases to search a license plate reader database maintained by Vigilant Solutions, a private data analytics company, for files going back five years.

"It's a huge invasion of privacy," Vasudha Talla, an ACLU staff attorney, told *The Guardian*. "Location surveillance and location data can really paint such an intimate portrait of someone's life, down to what they do minute by minute." The five-year broad timeframe, Talla argued, risked dragging in associates of the individual being investigated, or anyone who had a tie to a license plate over that period.

An ICE spokesperson, Matthew Bourke, defended the use of license plate information for investigations, saying the agency was not building its own database and that it would not use the data to track individuals with no connection to ICE enforcement. ICE doesn't take action against someone solely based on license plate data, he wrote in an email, adding that the agency limited database access to ICE employees who "need [license plate] data for their mission-related purposes."

The ACLU has called on cities to reject contracts for license plate surveillance, to stop sharing this kind of data with ICE, and to pass proactive privacy ordinances that require oversight when police buy surveillance technology. Reported in: *The Guardian,* March 13, 2019.

Washington, D.C.

How much data does the US Department of Homeland Security (DHS) collect from social media? Is the information accurate, free from bias, and effective in enhancing national security?

DHS has dramatically expanded its monitoring of social media monitoring in recent years, collecting a vast amount of user information in the process—including political and religious views, data about physical and mental health, and the identity of family and friends. DHS increasingly uses this information for vetting and analysis, including for individuals seeking to enter the United States and for both US and international travelers. In a new report, *Social Media Monitoring*, the Brennan Center provides an overview of DHS social media monitoring programs and the new set of challenges that they are surfacing.

The Brennan Center says, "There is little indication that social media monitoring programs—or the algorithms that sometimes power them—are effective in achieving their stated goals. Additionally, there is evidence that DHS is using personal information extracted from social media posts to target protestors and religious and ethnic minorities for increased vetting and surveillance."

According to the Brennan Center, the social media monitoring is used across various arms of DHS, including Customs and Border Protection (CBP), the Transportation Security Administration (TSA), US Immigration and Customs Enforcement (ICE), and US Citizenship and Immigration Services (USCIS).

Despite their expansion, the DHS programs have not proven successful, even based on the department's own measures. For example, after USCIS piloted five social media monitoring programs in 2016, the agency's own evaluations found the programs largely ineffective in identifying threats to public safety or national security.

The Brennan Center lists several of the central challenges associated with social media monitoring. One is the difficulty of interpreting what's in the social media messages and connecting them to actual threats. These interpretation problems become even more complex when a non-English language or unfamiliar cultural context is involved. The programs themselves also carry civil liberties risks. "They give the government a pool of information about people's personal lives and political and religious beliefs that can easily be abused. And research shows that people censor themselves when they know the government is watching," said Rachel Levinson-Waldman, senior counsel in the Brennan Center's Liberty and National Security Program.

Another concern in social media monitoring programs is the increasing use of algorithmic tools to review social media posts. These tools, which include natural language processing and algorithmic tone and sentiment analysis, have high error rates. This makes it questionable that they are actually capable of achieving DHS objectives, particularly because of the open-ended nature of the evaluations they are used for, such as identifying national security threats. Further, the algorithms are susceptible to bias.

"Our experience with algorithmic tools shows that they tend to operate in a discriminatory fashion," said Faiza Patel, co-director of the Brennan Center's Liberty and National

Security Program. "They make judgments based on proxies, and when these proxies reflect biases, the results produced by an algorithm simply reproduce those biases. For example, the biases evident in the early versions of the Trump administration's Muslim ban could be coded into an algorithm, resulting in the flagging of many Muslims as a national security threat." Since even before the ban, federal agencies such as the FBI and the Department of Defense have used religious beliefs as markers of dangerousness.

One barrier to addressing DHS's expansion of its social media monitoring programs is the lack of visibility into the full scope of the department's surveillance capabilities, a gap the Brennan Center report seeks to address.

"Congress should look closely at these DHS programs and ask the basic questions," said Patel. "In what contexts is the Department monitoring social media? How is it verifying the accuracy of accounts being attributed to individuals? What kinds of decisions is it using this data for? How is the information being shared? And how is the effectiveness of these programs being measured?" Reported in: brennancenter.org, May 22, 2019.

Mountain View, California

For users concerned that Google collects too much of their personal data, will Google's new security and privacy features satisfy them?

At its annual I/O developer conference in Mountain View, California, on May 7, 2019, Google touted new settings that allow anyone with a Google account to start limiting how long their data gets stored. The company also announced changes to its Nest home security system.

The new data settings allow users to set a time limit for Google to retain certain types of data, either three months or eighteen months. After that, the information is automatically deleted. For now, the auto-delete feature is only available for "Web & App Activity," which tracks searches and other browsing data. The company will offer options across more services in the future.

By default, however, Google will continue to indefinitely retain the web and app activity data according to users' current settings. When auto-delete is not turned on, the web and app activity page says, "Your activity is being kept until you delete it manually."

At the same I/O conference, Google announced a "privacy pledge" for its smart home devices, apparently in response to revelations that some Nest devices contained a previously undocumented microphone.

The company also announced a new measure meant to expand the security offerings for Nest accounts—perhaps because of an epidemic of Nest account takeovers. Beginning this summer, users will be able to migrate their Nest accounts into a new or existing Google account so they can have access to Google security features like suspicious activity monitoring and expanded options for two-factor authentication. (Nest already offers two-factor authentication, so users can activate that to ward off takeovers without linking even more data to their Google account.) Reported in: wired.com, May 7, 2019.

San Francisco, California; Detroit, Michigan, and nationwide

"What are we going to do about all the cameras?"

That question keeps *New York Times* columnist Farhad Manjoo up at night, he related in an opinion column in the *Time*'s "Privacy Project" series. In an overview of how new camera technology threatens privacy he, wrote:

> Advances in computer vision are giving machines the ability to distinguish and track faces, to make guesses about people's behaviors and intentions, and to comprehend and navigate threats in the physical environment. In China, smart cameras sit at the foundation of an all-encompassing surveillance totalitarianism unprecedented in human history. In the West, intelligent cameras are now being sold as cheap solutions to nearly every private and public woe, from catching cheating spouses and package thieves to preventing school shootings and immigration violations.

Among recent developments cited in Manjoo's column:

- In May, San Francisco's board of supervisors voted to ban the use of facial-recognition technology by the city's police and other agencies.
- Detroit signed a $1 million deal with DataWorks Plus, a facial recognition vendor, for software that allows for continuous screening of hundreds of private and public cameras set up around the city.
- Some police departments want to use "facial recognition on forensic sketches . . . a process riddled with the sort of human subjectivity that facial recognition was supposed to obviate."

Manjoo concluded:

> What sort of rules should we impose on law enforcement's use of facial recognition? What about on the use of smart cameras by our friends and neighbors, in their cars and doorbells? In short, who has the right to surveil

others—and under what circumstances can you object?

It will take time and careful study to answer these questions. But we have time. There's no need to rush into the unknown. Let's stop using facial recognition immediately, at least until we figure out what is going on.

Reported in: *New York Times,* May 16, 2019.

San Francisco, California

When people store, share, or save personal photos on a commercial website, should they be informed if the corporation will use their photos in its facial recognition technology?

The Ever AI website promotes that the company possesses an "ever-expanding private global dataset of 13 billion photos and videos" from what the company said are tens of millions of users in 95 countries. Ever AI uses the photos in developing its face recognition technology, which the company says can estimate emotion, ethnicity, gender, and age. A company representative confirmed in an interview with NBC News that those photos come from users of the firm's Ever app, which offers people a way to store photos and save memory space in their electronic devices.

After NBC News asked the company in April if users had consented to their photos being used to train facial recognition software that could be sold to the police and the military, the company posted an updated privacy policy on the app's website.

Previously, the privacy policy explained that facial recognition technology was used to help "organize your files and enable you to share them with the right people." The app has an opt-in face-tagging feature much like Facebook that allows users to search for specific friends or family members who use the app. This means that many people in the photos have no knowledge of or control over their images being uploaded, even if the Ever app user consented to the firm's privacy policy.

And the privacy policy was vague. In the previous privacy policy, the only indication that the photos would be used for another purpose was a single line: "Your files may be used to help improve and train our products and these technologies."

On April 15, one week after NBC News first contacted Ever, the company added a sentence to explain what it meant: "Some of these technologies may be used in our separate products and services for enterprise customers, including our enterprise face recognition offerings, but your files and personal information will not be," the policy now states. Reported in: NBC News, May 9, 2019.

Chicago, Illinois, and Detroit, Michigan

How invasive and pervasive are facial recognition technologies used by police and other authorities in US cities?

A report by the Center on Privacy and Technology at the Georgetown University law school, published on May 16, 2019, and entitled *America Under Watch: Face Surveillance in the United States,* uncovered unregulated systems in Chicago and Detroit that give police the ability to identify faces from surveillance footage in real time. Both cities purchased software from a South Carolina company, DataWorks Plus, according to contracts obtained by the Georgetown researchers. A description on the company's website says the technology, called FaceWatch Plus, "provides continuous screening and monitoring of live video streams."

Chicago claims it has not used its system; Detroit says it is not using its system currently. But no federal or state law would prevent use of the technology.

Facial recognition has long been used on static images, but using the technology with real-time video is less common. It has become practical only through recent advances in AI and computer vision, although it remains significantly less accurate than facial recognition under controlled circumstances.

Privacy advocates say ongoing use of the technology in this way would redefine the traditional anonymity of public spaces. "Historically we haven't had to regulate privacy in public because it's been too expensive for any entity to track our whereabouts," says Evan Selinger, a professor at the Rochester Institute of Technology. "This is a game changer."

According to the report, Detroit first purchased a facial recognition system capable of real-time analysis in July 2017 as part of a three-year contract related to an unusual community policing program called Project Greenlight. To deter late-night crime, gas stations and other businesses hooked up cameras that fed live surveillance footage to police department analysts. The program expanded over the years to stream footage to police from more than 500 locations, including churches and reproductive health clinics.

Chicago's adoption of FaceWatch Plus goes back to at least 2016, the report says. According to a description of the program—found in DataWorks Plus' pitch to Detroit—the "project objective" involved tapping into Chicago's 20,000 street and transit cameras. Chicago police told the researchers the system was never turned on. Illinois is one of only three states with biometric-identification laws that require consent from people before companies collect biometric markers,

like fingerprints and face data, but public agencies are exempted.

Georgetown's findings show how the lack of federal rules on facial recognition may create a patchwork of surveillance regimes inside the United States. In Chicago and Detroit, citizens in public are watched by cameras that could be connected to software checking every face passing by. Police in Orlando and New York City are testing similar technology in pilot projects.

For millions of others in New York City, Orlando, and Washington, D.C., face surveillance is also on the horizon. And for the rest of the country, there are no practical restrictions against the deployment of face surveillance by federal, state, or local law enforcement.

The Georgetown report said there has been little public oversight of such systems in Chicago, Detroit, or elsewhere.

Such surveillance "risks fundamentally changing the nature of our public spaces," according to the Georgetown report. It lists specific concerns:

- **Free Speech**. When used on public gatherings, face surveillance may have a chilling effect on our First Amendment rights to unabridged free speech and peaceful assembly.
- **Privacy**. If mounted on churches, health clinics, community centers, and schools, face surveillance cameras risk revealing a person's "familial, political, professional, religious, and sexual associations," the very "privacies of life" that the Supreme Court in *Carpenter v. United States* (2018) suggested receive protection under the US Constitution.
- **Bias.** The risks of face surveillance are likely to be borne disproportionately by communities of color. African Americans are simultaneously more likely to be enrolled in face recognition databases and to be the targets of police surveillance use. Compounding this, studies continue to show that face recognition performs differently depending on the age, gender, and race of the person being searched. This creates the risk that African Americans will disproportionately bear the harms of face recognition misidentification.

The Center on Privacy & Technology said the in the two years since it issued an earlier report on police use of face recognition technology in the United States, "a dramatic range of abuse and bias has surfaced."

Therefore, the Georgetown report ends with a recommendation: "We now believe that state, local, and federal government should place a moratorium on police use of face recognition. . . . Once bans or moratoria are in place, communities can stop to think about whether face surveillance should be allowed in their streets and neighborhoods." Reported in: *America Under Watch,* May 16, 2019; wired.com, May 17.

Augusta, Maine

Will a new law protecting consumers' privacy online in Maine affect how internet service providers (ISPs) do business in other states as well, or will court challenges prevent the law from going into effect?

On June 6, Maine Governor Janet Mills signed into law a bill that the *Portland Press Herald* said requires ISPs to provide "the strictest consumer privacy protections in the nation."

Before the bill's passage, several technology and communication trade groups told the Maine legislature that it may be in conflict with federal law and would likely be the subject of legal action.

The new law, which goes into effect on July 1, 2020, would require providers to ask for permission before they sell or share any of their customers' data to a third party. The law would also apply to telecommunications companies that provide access to the internet via their cellular networks.

The law is modeled on a US Federal Communications Commission rule, adopted under the administration of President Obama but overturned by the administration of President Trump in 2017. The rule blocked an ISP from selling a customer's personal data, which is not prohibited under federal law.

According to the *Press Herald,* "The law is unlike any in the nation, as it requires an ISP to obtain consent from a consumer before sharing any data. Only California has a similar law on the books, but it requires consumers to "opt out" by asking their ISP to protect their data."

The Maine bill passed with strong bipartisan support. Reported in: *Portland Press Herald,* June 6, 2019.

Lockport, New York

Which school district will become the first in the United States to implement a facial recognition system to track all the visitors, students, faculty, and staff members in its schools?

The Lockport City School District in Western New York state was set to activate a pilot version of its Aegis system on June 3, 2019, and planned make the whole system operational throughout its eight schools in September. However, on May 30, the New York State Department of Education asked Lockport to delay its use of facial recognition technology on students.

In March 2018, Lockport announced plans to install facial recognition security, funded through the New York Smart Schools Bond Act—an act meant to help New York schools acquire instructional technology. Instead of buying electronic devices for students and teachers, Lockport proposed a high-tech security system, and allocated much of the $4.2 million it was given toward adding dozens of surveillance cameras in the school and installing the facial recognition system Aegis, from a Canadian firm, SN Technologies. By the end of May 2019, Lockport had spent $1.4 million to get the system up and running.

The American Civil Liberties Union, which wrote to the state Department of Education opposing Lockport's plan, told *BuzzFeed News* that Lockport was about to be the first public school district to begin using a facial recognition system, although other schools have considered such technology.

As described by Lockport officials in an FAQ distributed to the school's parents and obtained by *BuzzFeed News*, "Aegis is an early warning system that informs staff of threats including guns or individuals who have been identified as not allowed in our buildings. Aegis has the ability [to screen] every door and throughout buildings to identify people or guns. Early detection of a threat to our schools allows for a quicker and more effective response."

According to the FAQ, Aegis will track individuals who are "level 2 or 3 sex offenders, students who have been suspended from school, staff who have been suspended and/or are on administrative leave, any persons that have been notified that they may not be present on District property, anyone prohibited from entry to District property by court order . . . or anyone believed to pose a threat based on credible information presented to the District." The *Lockport Journal* reported that Aegis also includes an object recognition system, which is said to be able to detect 10 types of guns.

The FAQ adds that the system "will not generate information on or record the movements of any other district students, staff or visitors," but previous reporting from *BuzzFeed News* has shown that in order to effectively flag the faces of "persons of interest," facial recognition systems must also disregard the faces of persons who are not of interest. In other words, it analyzes them, too.

Explaining its decision to postpone facial recognition in Lockport's schools, the New York State Department of Education emailed a statement:

> The Department is currently reviewing the Lockport CSD's privacy assessment to ensure that student data will be protected with the addition of the new technology. The Department has not come to the conclusion that the District has demonstrated the necessary framework is in place to protect the privacy of data subjects and properly secure the data. As such, it is the Department's continued recommendation that the District delay its use of facial recognition technology.
>
> Regulations are in the process of being finalized that will adopt a standard for data privacy and security for all state educational agencies. We recommended in past communication that the District consider reviewing the standard and related materials in developing and refining its data security and privacy program. We will remain in contact with school district officials.

Reported in: *Buzzfeed,* May 29, May 30, 2019.

Salt Lake City, Utah

Do police need a warrant to obtain citizens' private information from providers of electronic data services? In Utah, the answer is yes.

Utah Governor Gary Herbert on March 17, 2019, signed a new privacy law that made his state the first to protect private electronic data, stored with third-party providers, from government access without a warrant. Under the legislation passed unanimously by the Utah legislature, to go into effect on May 14, law enforcement agencies need a warrant to obtain information about an individual from wireless communications providers, email platforms, search engine providers, or social media companies.

Previously, on both the federal and state levels, law enforcement agencies generally had access to information through third-party providers on the grounds that individuals have no reasonable expectation of privacy when they share their personal information with third parties.

The US Supreme Court limited that access in 2018 in its 5–4 opinion in *Carpenter v. United States,* in which the majority held that the government's search of personal cell phone location information held by a wireless communications provider constitutes a Fourth Amendment search, and therefore requires a warrant. However, the opinion did not extend beyond location information, and the dissenting justices urged that legislation was needed to govern this body of law in a new age of technology.

Utah's new law specifically states that "a law enforcement agency may not obtain, without a search warrant issued by a court upon probable cause," the location information from

an electronic device or "electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider." The law defines "electronic information or data" broadly to include "a sign, signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system."

There are specific exceptions, such as when the third-party provider believes an emergency exists with risk of death, serious physical injury, or sexual abuse.

Among other things the bill:

- Requires a search warrant to obtain certain electronic information or data;
- Specifies when notification must be provided that electronic information or data were obtained;
- Regulates transmission of electronic information or data to a remote computing service, including restrictions on government entities;
- Provides that the individual who transmits electronic information or data is the presumed owner of the electronic information or data; and
- Excludes from evidence electronic information or data obtained without a warrant.

Reported in: le.utah.gov, n.d.; Cyber Adviser, March 28, 2019; *Data Privacy + Security Insider,* April 1.

Richmond, Virginia

Does publication of fake images violate a victim's privacy the same way publication of actual images would?

Virginia has expanded its ban on revenge porn to include "deepfake" images and videos. (Deepfake technology uses artificial intelligence to manipulate images and videos nearly seamlessly, for example to put one person's face on another person's body.) An updated law, which took effect on July 1, 2019, amends an existing law that says anyone who shares or sells nude or sexual images and videos to "coerce, harass, or intimidate" is guilty of a Class 1 misdemeanor. The update adds language about "a falsely created videographic or still image."

The Virginia General Assembly passed the updated bill in March, and it was signed by Governor Ralph Northam in the same month.

Deepfakes are leading to growing concern about privacy. In June 2019, an app called DeepNude, which can morph pictures of clothed women into nudes, shut down. Samsung also developed an artificial intelligence system that can create a fake clip from a single picture. In 2018, Reddit banned deepfake porn. Reported in: cnet.com, July 1, 2019.

Seattle, Washington, and nationwide

Amazon's "Ring" doorbell system "has essentially created private surveillance networks powered by Amazon and promoted by police departments," according to cnet.com.

Police departments across the United States have offered free or discounted Ring doorbells to citizens, sometimes using taxpayer funds to pay for Amazon's products. While Ring owners are supposed to have a choice in providing footage to police, in some giveaways, police require recipients to turn over footage when requested.

Ring said on June 4, 2019, that it would start cracking down on those strings attached. "Ring customers are in control of their videos, when they decide to share them and whether or not they want to purchase a recording plan. . . . Ring does not support programs that require recipients to subscribe to a recording plan or that footage from Ring devices be shared as a condition for receiving a donated device."

More than fifty local police departments across the United States have partnered with Ring over the last two years, giving them access to security footage in suburban neighborhoods that otherwise might not be covered by security cameras.

Amazon bought Ring in 2018 for a reported $1 billion, helping Amazon expand its "smart homes" business.

Multiple cities have laws requiring a public process to debate how police use and buy surveillance technology. But when police and Amazon convince private residents to buy these cameras, this can circumvent that process while saving the city money. Ring cameras can cost between $99 and $500.

Police can get additional information by adding their own technology to that of Ring and Amazon. Depending on how the Ring camera is set up, it can capture motion on the streets, such as cars passing by. Police can enter details on a car from Ring footage into an automated license plate reader system, and figure out the car's owner and address. Reported in: cnet.com, June 5, 2019.

Seattle, Washington

Does Amazon's Echo Dot Kids, a smart speaker designed for children, illegally keep data on children, even after their parents try to delete it?

A coalition of nineteen consumer and public health advocates led by the Campaign for a Commercial-Free Childhood (CCFC) and the Center for Digital Democracy (CDD), filed a complaint asking the Federal Trade

Commission (FTC) to investigate Amazon and its $35 device.

Amazon markets the device as "a kid-friendly study buddy, DJ, comedian, storyteller, and more," and promises "peace of mind" for parents who want to screen explicit music and other potentially harmful content from their kids. But the complaint alleges that parents may be risking their children's privacy, alleging that the kids' version of Amazon's Alexa won't forget what children tell it, even after parents try to delete the conversations.

"These are children talking in their own homes about anything and everything," said Josh Golin, who directs the Campaign for a Commercial Free Childhood. "Why is Amazon keeping these voice recordings?"

The coalition of groups led by Golin's organization, along with Georgetown University's Institute for Public Representation, allege that Amazon is violating the federal Children's Online Privacy Protection Act (COPPA).

Amazon said in a statement that its Echo Dot Kids Edition is compliant with COPPA.

It is unclear whether the FTC will take up the complaint, since its investigations are rarely public. But the agency has been enforcing children's privacy rules more seriously in the past year, said Allison Fitzpatrick, a lawyer who helps companies comply with COPPA requirements and was not involved in the complaint.

For the FTC to take notice, however, Fitzpatrick said there usually needs to be evidence of "real, actual harm," not just the theoretical harm she said advocacy groups often outline. Reported in: CBS News, May 9, 2019.

INTERNATIONAL

Dublin, Ireland

Is Google complying with Europe's new General Data Protection Regulation (GDPR)?

Ireland's Data Protection Commissioner (DPC), a major regulator of internet companies in the European Union, opened its first investigation into Google on May 22, 2019, over how it handles personal data for the purpose of advertising.

The commissioner said the probe was the result of a number of submissions against Google, including from privacy-focused web browser Brave. Brave argued that when a person visits a website, Google collects intimate personal data that describes them and what they are doing online and broadcasts the data to tens or hundreds of companies without the person's knowledge.

The Irish DPC said it would investigate whether processing of personal data carried out at each stage of an advertising transaction was in compliance with the GDPR. The European Union passed the privacy law in 2018.

Many large international technology firms have their European headquarters in Ireland, putting them under the watch of the Irish DPC.

The regulator said earlier this month that it had fifty-one large-scale investigations under way, seventeen of which related to large technology firms, including Twitter, LinkedIn, Apple, and Facebook and its WhatsApp and Instagram subsidiaries.

Under the EU's GDPR, regulators have the power to impose fines for violations of up to 4 percent of a company's global revenue, or 20 million euros, whichever is higher.

When Brave raised its privacy concerns about Google in September 2018, Google said it had already implemented strong privacy protections in consultation with European regulators and is committed to complying with the GDPR. Reported in: Reuters, May 22, 2019.

Luxembourg City, Luxembourg

Should internet service providers and other electronic platforms be held responsible when users post material that infringes on the content creator's copyright? And will the European Union's new Copyright Directive lead to excessive censorship as platforms try to protect themselves from liability?

In March 2019, the European Union passed the burden for copyright infringement from users to platforms under its new Copyright Directive. In May 2019, Poland, a member of the EU, filed a legal challenge to the directive, saying that it will lead to "preventive censorship."

The Copyright Directive was first proposed in 2016, and went through numerous failed votes and subsequent tweaks before it was passed. Proponents of the law said that it was about making sure fair compensation went to content creators—news sites, musicians, or artists, for example.

Yet critics—including the Polish government—say the law's vague definitions and a lack of clarity about how to enforce such measures means that platforms are likely to over-filter content rather than leave themselves open to legal risks.

In its filing with the European Union's Court of Justice in Luxembourg, the Polish government says that the Copyright Directive "may result in adopting regulations that are analogous to preventive censorship, which is forbidden not only in the Polish constitution but also in the EU treaties."

Alongside the announcement, Polish Prime Minister Mateusz Morawiecki, tweeted that the new law is "a

disproportionate measure that fuels censorship and threatens freedom of expression."

Under prior copyright law, platforms were not responsible for their users breaching rules as long as the company took reasonable steps to remove anything infringing. Under the new system, a platform would be liable the moment a user uploads something they don't own the rights to. Reported in: techspot.com, May 27, 2019.