NEWS IS IT LEGAL?

LIBRARIES

Iowa City, Iowa

The American Civil Liberties Union of Iowa is asking the Iowa City Public Library to remove security cameras from its bathrooms over privacy concerns raised by a patron.

The ACLU of Iowa emailed the letter January 13 on behalf of University of Iowa sophomore Kellsie Pepponi, who in September had used one of the bathrooms and afterward noticed a camera on the bathroom ceiling.

Pepponi saw a sign outside the bathroom noting cameras were in use but, in seeing cameras outside the bathroom, believed the sign was referencing those cameras, the letter said. She did not notice the camera inside the bathroom on her way in because they are near the entrance, but noticed it while standing inside one of the stalls, the letter said.

In the letter, the group asks that the cameras, located in the common areas of the bathrooms, be removed because of violation of patrons' privacy. If that is not possible, the letter said, the group asks the library to post more adequate notice that the cameras are located inside the bathrooms, that the recordings are subject to open records requests, and to make clear what is being recorded and who maintains the recordings.

In 2013, the ACLU of Iowa obtained recordings from the common areas of men's and women's restrooms via a public records request, the letter said. The footage showed patrons changing, getting dressed and "adjusting themselves."

"While individuals are given notice that they are being recorded, library patrons have an expectation that these private acts should not be observed nor recorded by a government entity," said Rita Bettis, ACLU of Iowa Legal Director, in a news release.

Library Director Susan Craig said that the cameras record only the common areas and do not collect video from inside the stalls.

"I absolutely understand concerns people have about what exactly we're taking pictures of, but usually once they understand that it's only in the common space, not in the stall area of the restrooms, they are more understanding," Craig said. "It's just part of the security camera system in the library, and it is there for the safety and security of people. It is also there to protect against theft and vandalism."

Footage from the bathrooms is not actively monitored by library staff, she said, and is deleted after seven days. If footage is required for criminal investigations, there are four employees authorized to examine the footage, she said. Those employees are Craig, the administrative business office manager, the head of the library's IT department, and a staff member who works in the community and access services department.

In the past, the library has provided police with footage that has led to arrests related to theft, vandalism, and an assault, Craig said.

"The cameras have been quite invaluable since they were installed," she said. "The city attorney has said that as long as it is the common area only, it is legal and that there should be no expectation of privacy in the common area of a public bathroom. That's why we have them."

The library opened its new building in 2004, Craig said, and the cameras have been functioning for more than ten years. Signs stating "security cameras are in use" are posted outside of the bathrooms and inside some of the bathrooms.

Veronica Lorson Fowler, communications director for the ACLU of Iowa, reiterated that at least, according to the complaint, the signage should be updated. She said the situation is different than a department store placing security cameras in common areas near changing rooms and in bathrooms.

"There's a problem there and, obviously we love libraries and we love the Iowa City Public Library, but there's a problem that needs to be addressed. Right now, any footage they take, because they are a government agency, is subject to open records," she said. "At the very, very least they need to update their signage, because people are not aware that they are being, in some of their more private moments, recorded. That would seem a very straightforward solution to part of the problem."

Craig said the city attorney's office and the library's board of directors are reviewing the complaint. She said the nine-member board will review any recommendations made by the attorney's office.

"Ultimately, it's the board's decision," Craig said. Reported in: *Iowa City Press-Citizen*, January 13.

Kansas City, Missouri

A patron and a library director face charges stemming from an event at the Kansas City Public Library in May.

Jeremy Rothe-Kushel, a documentarian and activist who lives in Lawrence, asked provocative questions of a diplomat, who had just concluded a talk about U.S. presidents' attitudes toward Israel.

Kansas City police said they arrested Rothe-Kushel because he was disruptive. Steven Woolfolk, the library's director of programming and marketing, was charged with interfering with that arrest.

Library officials say the arrests were unwarranted. R. Crosby Kemper III, the executive director of the library, said the police infringed

on Rothe-Kushel's First Amendment rights, and he stands by Woolfolk, who tried to intervene as Rothe-Kushel was removed from the auditorium of the library's Plaza branch.

The police say Rothe-Kushel was arrested because of his actions, not the content of his beliefs. "It was his behavior that was disrupting the flow of the event," Capt. Stacey Graves, a police spokeswoman, says.

But free speech is not the only issue at stake. The case also raises questions about the lines that blur when police officers exercise their powers while working for private employers.

Off-duty Kansas City police officers made the arrests at the May 9 event, a talk by Dennis Ross, an ambassador who has worked in the Middle East. A sergeant and two detectives were hired by the Truman Library Institute, which sponsored the event with the library and the Jewish Community Foundation of Greater Kansas City.

The officers' point of contact at the event was Blair Hawkins, the Jewish Community Foundation's director of community security. The foundation hired Hawkins, a former Seattle police detective, after a white nationalist murdered three people in the parking lots of two Jewish facilities in Overland Park in 2014.

Hawkins was an assertive presence at the May 9 event. He requested that one of the off-duty officers search Rothe-Kushel and a friend before they entered the auditorium where Ross was speaking. During the question-and-answer period, he closed in on Rothe-Kushel, who was trying to extend his exchange with Ross.

In the police's version of events, Hawkins approached Rothe-Kushel and "advised him that he was done speaking and needed to leave." A video of the incident recorded by Rothe-Kushel's friend indicates a forceful "advising." Rothe-Kushel is leaning into the microphone as two men in suits descend on him, their arms extended. Hawkins is the first to arrive, and he grasps Rothe-Kushel by the arm.

Woolfolk tried to intervene as Hawkins and the other man removed Rothe-Kushel. Woolfolk said he was trying to deescalate the situation. Police claim he did the opposite. "When an officer is effecting arrest, whether you agree with it or not, you cannot interfere with that arrest," Graves said.

For months, library officials protested that the arrests and charges were a violation of the First Amendment, but did not go public with its objections until late September. That prompted ALA President Julie Todaro to issue this statement:

"The ALA commends the Kansas City Public Library for its commitment to fostering public deliberation and the exchange of a wide spectrum of ideas by offering meeting rooms and other spaces for lectures, educational programs, and organizational meetings. Its long history of support for free speech in public programming exemplifies the library profession's mission to influence positive and lasting change within their communities by providing opportunities for patrons to freely express opposing viewpoints without fear of persecution.

"Libraries are public institutions that serve as catalysts for public discussions that help solve community challenges. Such efforts are not possible when patrons are not allowed to engage in open debate in a public forum, but rather are arrested for asking difficult questions.

"The ALA commends Steve Woolfolk for defending a patron's right to question and debate matters of public concern. The association will continue to extend resources to library staff as the Kansas City (Mo.) Public Library moves forward with its legal efforts."

Woolfolk said he has hosted dozens of library events where more provocative questions have been asked, and no one was arrested. The only time anyone has been asked to leave was when an audience member fell asleep and started snoring.

The library ordinarily does not have security or off-duty police at such events, but on occasion allows it if a speaker, such as an author on abortion issues, may be in danger.

In this case, the library agreed to have the Jewish Community Foundation bring security, in part out of sensitivity to the 2014 shootings that left three dead at Jewish sites in Overland Park. But library officials said they had specified that no one was to be removed for asking uncomfortable questions and not without permission of library staff, unless there was an imminent threat.

Kemper, the library director, said the security guards and police officers violated that agreement, along with the library's core reason for existence as a place to exchange ideas.

"We're going to be living in a different kind of country" Kemper said, if people can be arrested for asking questions at a library. "If this kind of behavior is unacceptable to the police, then I guess we're going to have to shut the library down." Reported in: *The Pitch*, October 11; *Kansas City Star*, September 30, October 4; nybooks.com, October 14.

Omaha, Nebraska

If a child were kidnapped at an Omaha library, staffers would want to turn over security video to police immediately. But the current library policy says officers would first have to obtain a court order. So Director Laura

Marlane has proposed loosening that policy so that library officials could release security video if police needed to take immediate action to save a life.

But at least one board member wants to further loosen the policy to allow police access to footage any time there is reasonable suspicion that a crime has occurred.

Twice in recent years, law enforcement officials have asked the library to loosen its policies on releasing information, including the security video policy. In one instance, the police chief appeared before the board to ask the library to provide video to police without requiring a court order. Library leaders resisted, saying patrons should expect privacy in libraries.

Marlane's proposal doesn't go as far as police have requested. She suggests allowing some library staffers to turn over security video in situations that require "immediate action to prevent imminent danger to life, or to identify a person currently in custody on the premises."

Marlane said that if, for example, a child were kidnapped at a library branch, the staff would want to turn over video footage immediately. "I wanted to change the policy to reflect real situations," Marlane said.

But board member Kathleen McCallister, who is married to an Omaha police captain, said the proposed change doesn't go far enough.

"I think we're being too nice to the bad guys," she said.

She offered an alternate proposal that says staff can release video to police in any "situation where there is a reasonable suspicion that a crime has occurred, or to identify a person currently under investigation, including medical emergencies."

That would greatly broaden the types of situations where the library would provide video to police. McCallister said that if someone was suspected of exposing themselves to a library patron, she would want staff to be able to turn over the video.

Libraries generally resist releasing information that could identify patrons or reveal what they are reading. The American Library Association's guidelines on patron privacy include the following: "Libraries should not share personally identifiable user information with law enforcement except with the permission of the user or in response to some form of judicial process (subpoena, search warrant, or other court order)."

In 2014, Mayor Jean Stothert's chief of staff, Marty Bilek, and Metropolitan Community College Police Chief Dave Friend appeared before the board to ask that the library release patron names, addresses, and phone numbers to police in emergencies. They cited a situation at the South Omaha branch, a joint facility between the library system and Metro. Friend said a drunk man was harassing other patrons and wouldn't give police his name. The chief said that prevented officers from taking the man to a treatment facility and tied up officers for about two hours.

The ACLU of Nebraska stepped in, saying the change would be unconstitutional. The mayor's office withdrew the request.

Last year, Police Chief Todd Schmaderer and Captain Katherine Belcastro-Gonzalez told the board that the downtown library was draining police resources. At that time, Belcastro-Gonzalez asked the board to enact a policy that would allow library officials to turn over footage from security cameras to police without requiring a subpoena. She also suggested searching patrons' bags to make sure they don't have weapons or open containers of alcohol.

The board didn't make those changes but did beef up the library's misconduct policy, including lengthening a ban from library premises for infractions such as breaking items and public intoxication.

At its meeting, the board voted to take no action on Marlane and McCallister's proposals but rather to send them back for more work.

Marlane said that if someone suspects that a nonemergency crime has occurred—such as a theft of a purse or a hit-and-run car crash in the parking lot—library staffers save the security footage until police can obtain a court order.

"We want to keep the library safe for everybody and we want to work with police the best we can," Marlane said. "But preserving patron privacy is also a very important part of what we do." She said she plans to work with McCallister on striking the right balance.

Assistant City Attorney Michelle Peters noted that the Fourth Amendment comes into play and said obtaining a warrant or subpoena is common. She said in libraries people have a "heightened expectation of privacy."

Board member Mike Kennedy said there are legitimate privacy concerns. "We're not going to zoom in the camera to see if you checked out *Fahrenheit 451*, " he said. Reported in: *Omaha World-Herald*, October 26.

Roselle Park, New Jersey

A public official's tribute to America's military veterans has stirred controversy in a New Jersey town. Outside of Veterans Memorial Library in Roselle Park is a silhouette of a soldier kneeling at a cross. It's become the center of controversy among residents including Gregory Storey.

"It's a very touching memorial, but the problem is there's a cross in it. It singles out veterans of one religion, and in doing so ignored and

disrespects veterans of all other religions, or no religion," Storey said.

The memorial—paid for by Mayor Carl Hokanson—was installed on July 29 by city workers and came as a surprise to the board that runs the library.

After sixty-eight days in front of the Roselle Park Veterans Memorial Library, the "Kneeling Soldier At Cross" memorial was removed in early October at the behest of Mayor Hokanson.

What started out as a donation from Hokanson, acting as a private resident, has led to a lawsuit filed by the American Humanist Association and Gregory Storey along with his wife, Councilwoman-At-Large Charlene Storey—acting as a private citizen—against Hokanson in his capacity as mayor and the Borough of Roselle Park for approving its placement at the library.

Although Mayor Hokanson said he would "temporarily remove the 'Kneeling Soldier' while the Storey lawsuit plays out in court," his action did not end the lawsuit that was filed on September 30. This is due, in part, to the mayor's use of the word 'temporary' in his statement.

David Niose, the legal director of the Appignani Humanist Legal Center, which is the legal arm of the American Humanist Association, commented, "As far as the removal goes . . . it doesn't really change anything as far as the lawsuit. I think the mayor made it pretty clear that he's just removing it temporarily, for some reason; presumably due to the litigation. He has every intention of putting it back up and he thinks it belongs up so the issue still needs to be resolved in the courts."

When asked whether the organization's concerns would have been resolved if the mayor had removed the memorial before the lawsuit was filed, Niose stated, "It may have, as long as he acknowledged that it wasn't going to be put back up."

Additionally, an acknowledgement from the borough regarding the Establishment Clause violation also may have resolved the matter, according to the AHA spokesman.

Charlene Storey stated that she would not comment on the matter due to litigation other than to say, "This doesn't end the lawsuit. First of all, it's temporary. The mayor stated it was temporary. Secondly, it's not just a matter now with the mayor, it's actions by council. If it [was removed] before council voted to accept it and to place it at the library, there would have been no lawsuit."

The council approved accepting the donation and its placement at an August 18 mayor and council meeting. At that meeting, Roger Byron, senior counsel for First Liberty Institute—a law firm that has offered to defend the municipality in case of a lawsuit—was in attendance.

"The mayor is my boss, we listen to him, but it was not put through the board of trustees," Interim Library Supervisor Kit Rubino said when Storey first raised his complaint. However, Storey claimed that the mayor told him, "This was approved by the Board of Trustees of the library. Don't talk to me, talk to them.'"

Jeff Regan, vice president of the Roselle Park Library board of trustees, claimed a quorum was present at a library board meeting where a vote was taken to accept the statute. However, the library board of trustees website shows no meetings were scheduled in July or August. It seems, therefore, that a majority conducted business without following proper channels. Five of the nine members of the library board of trustees are also members of either the Roselle Park Democratic Committee or the Roselle Park Democratic Club, so there was speculation that an illegal meeting may have taken place during a political event. Patricia Butler, the library board president, stated that she herself was not aware of any approval.

On October 6, the council voted unanimously to reverse its previous decision to accept a donation of the memorial and to approve its placement in front of the Roselle Park Veterans Memorial Library. The action was believed to have been taken to put an end to the lawsuit filed against the municipality to have the memorial removed from public property. Reported in: cbsnews.com, August 16; *New Jersey Today*, September 11; *Roselle Park News*, August 23, October 7, 12.

New York, New York

In an apparent response to the election of Donald Trump, libraries are promising to destroy user information before it can be used against readers and backing up data abroad.

The New York Public Library (NYPL) changed its privacy policy November 30 to emphasize its data-collection policies. The previous week, the NYPL website stated that "any library record or other information collected by the Library as described herein is subject to disclosure pursuant to subpoena, court order, or as otherwise authorized by applicable law."

Now, the page reads, "Sometimes the law requires us to share your information, such as if we receive a valid subpoena, warrant, or court order. We may share your information if our careful review leads us to believe that the law, including state privacy law applicable to Library Records, requires us to do so."

The NYPL also assured users that it will not retain data any longer than is necessary. "We are committed to

keeping such information, outlined in all the examples above, only as long as needed in order to provide Library services," the librarians wrote.

Meanwhile the digital library Archive.org, which keeps a searchable database of public websites, announced that it would create a new Canada-based backup of its huge information repository to respond to the increased threat of invisible government scrutiny. The group's services include the Internet Archive and a search engine cataloging it called the Wayback Machine.

"We have statements by President Trump saying he's against net neutrality and he wants to expand libel laws," Archive.org founder Brewster Kahle said. "Librarians are wary of storing hoards of precious information 'along faultlines,' whether those faultlines were literal or ideological. Trump has called for surveillance of Muslims and nominated Jeff Sessions as his attorney general; the Alabama senator called plans to stop the NSA's warrantless domestic wiretapping 'idiotic.'"

Archive's director of partnerships, Wendy Hanamura, said the decision had been a sober one. "We didn't pick Canada out of a hat," she said. "Law in Canada has shifted recently, making it a really great place for libraries to experiment."

"Even before the election we had made the decision to host at least Canadian materials in Canada," Kahle said. "They have rigorous privacy rules because they don't particularly like patients' privacy information going to the United States." The response to the fundraising campaign had been overwhelming, he said.

The Wayback is a popular tool among journalists; one of its key features is the ability to see what changes were made to a given website and when. The project automatically captures some 300 million webpages every week and devotes some of its resources to splitting its archived material into collections of similar material, such as political ads and books in the public domain.

Backlash from the librarian community to Trump's election was so rapid that the American Library Association (ALA) issued an apology for its November 18 statement, saying its members would "work with President-elect Trump" and his transition team.

"We understand that content from these press releases, including the 11/18/16 release that was posted in error, was interpreted as capitulating to and normalizing the incoming administration," the ALA president, Julie B Todaro, wrote in *American Libraries*. Todaro said that the ALA's core values remained unchanged: "free access, intellectual freedom, privacy and confidentiality."

"It is clear that many of these values are at odds with messaging or positions taken by the incoming administration," she wrote. Reported in: *The Guardian*, November 30.

Longview, Texas

A Longview High School librarian has been suspended for two days without pay after she posted life-size cutouts of presidential candidates with modified versions of campaign trail quotes at the library entrance.

Longview ISD board President Chris Mack said he was uncertain when librarian Linda Bailey will take the two days of unpaid suspension, and noted that would be a decision for administrators to make.

Trustees took the action against Bailey on October 10 after a closed session hearing in which they were scheduled to consider suspension without pay for a district employee.

Bailey put the cutouts of Donald Trump and Hillary Clinton at the library doors with text attached to each. The Trump comment read, "Sign in or you will be deported." The Clinton comment read, "This is the only door to use. Only deplorables use the other door."

After being alerted to the signs October 5, the school district immediately had the cutouts removed. The district issued an apology for the librarian's actions.

District officials said the cutouts, particularly the one of Trump, offended some students, staff, and community members.

Veronica Lu, whose nephew sent her a picture of the Trump cutout at the library, said last week it was offensive to her, her nephew, and many of his peers. Lu's family is Hispanic.

"My nephew was upset about it, and there were several other students who were upset about it," she said. "Some students felt like they don't belong here—like a certain race of people do not belong here."

Before the closed session hearing, two men spoke in open forum urging trustees to consider cultural sensitivity training in the district.

Longview immigration attorney Jose Sanchez called the cutouts "offensive and definitely not appropriate." He said the word "deported" on the Trump note has enhanced "fear" for the undocumented and the documented community.

"To hear that Longview High School students were upset and to hear that some of them felt like they don't belong here—like a certain race doesn't belong here—is sickening," Sanchez told trustees. He added that the cutout of Clinton and the note attached to it also was "a disgrace."

Sanchez said that he didn't believe Bailey should be fired for her actions. He said the librarian should issue a personal apology to students, staff, and the community, as well as be

reprimanded. Reported in: *Longview News-Journal*, October 11.

SCHOOLS
Mountain View, California

A Mountain View High School history teacher was placed on paid leave after comparing Donald Trump to Adolf Hitler in an effort to show students that the 2016 election is a reflection of the past.

Frank Navarro, a Holocaust scholar who has taught at Mountain View High School for forty years, said the school's principal and district superintendent asked him to leave after a parent complained about the parallels he was drawing in his world studies class.

"This parent said that I had said Donald Trump was Hitler, but I would never say that," Navarro said. "That's sloppy historical thinking."

He did, however, point out the connections between Trump's presidential campaign and Hitler's rise to power: Both had promised to eject foreigners and make their countries "great again," Navarro said.

"I think it makes sense," he said. "It's factual, it's evidence-based." He added: "It reminds students that history is real."

But Principal Dave Grissom and Superintendent Jeff Harding feared that the lessons may have been inappropriate in the tempestuous aftermath of the election.

"Regardless of their political affiliation, many of our students show signs of emotional stress," Grissom wrote in a letter to parents. He said he has an obligation to maintain an "emotionally safe environment" for students while protecting teachers and staff against unsubstantiated allegations.

Grissom called the paid leave process a "time-out" for the staff member under investigation.

The school's newspaper, the *Oracle*, published an article about the investigation, prompting outrage among parents and students.

"Emails started flowing in to the principal late that night," Navarro said. Two days later, a Mountain View High School alumnus started a Change.org petition, demanding that Grissom revoke Navarro's leave and publicly apologize "for attempting to intimidate a respected educator."

Within two days the petition had gathered almost 4,000 signatures. Reported in: *San Francisco Chronicle*, November 13.

COLLEGES AND UNIVERSITIES
Orlando, Florida

Knight News, an independent student news website at the University of Central Florida, has been forced to sue the University of Central Florida three times in the past three years for access to records and meetings. In response, UCF has repeatedly asked the courts to force the student-run outlet to pay the university's legal bills—an unusual move, since public-records laws generally provide compensation only to the requester, not to the government agency.

On April 7, the Student Government Association (SGA) at UCF, a campus of more than 60,000 students located in Orlando, passed an $18.6 million budget in a meeting closed to public comment.

This followed an incident in December where the SGA held committee meetings on the allocation of the Activities and Services Fee during the time the campus was closed for winter break. Students at UCF are not allowed to stay in the dorms over the holiday, and anyone wishing to attend the meeting would have had to arrange for alternate accommodations.

Knight News asked to inspect copies of SGA budget requests along with an electronic copy of the Activites and Services Fee financial database. The requests for budget documents went unanswered for more than a month, and the news outlet filed a lawsuit against the university on May 23 requesting the release of the documents and a permanent injunction to require SGA to allow public comment.

In response to the lawsuit, the university released a heavily redacted version of the documents June 3, including removing student names, citing the Family Educational Rights and Privacy Act (FERPA), which protects students' education records.

Michael Williams, a government reporter for *Knight News*, said reporters' ability to cover the news was compromised by the redactions.

The university didn't stop at withholding the documents under FERPA. They claimed that the lawsuit was so baseless that *Knight News* should pay UCF's legal fees—an unorthodox move, as the normal practice in Florida open-government lawsuits is that only the requester is entitled to recover attorney fees.

"If we had to pay attorney's fees it would cripple us," Williams said. "We're not a money-making machine. We're not *The New York Times*. We are student-run, independent publication."

Knight News is a 501(c)(3) nonprofit launched in 2009. Students run the newsroom and do all the reporting, but the website is neither affiliated with nor funded by the university.

Last summer, the campus's only official student newspaper, the *Central Florida Future*, closed after forty-eight years.

UCF argues that *Knight News*' request for the documents is "meritless," and therefore the journalists and their attorney should be responsible for the

financial resources the university must expend to fight the case.

In refusing to release the documents, the university is concealing the use of government funds, Justin Hemlepp, a local attorney representing *Knight News*, said. Not only is their legal position indefensible, but he also finds it "preposterous" that a university would ask for attorney's fees from a student paper.

"What this is really about is a university spending $250,000 in taxpayer money in asserting the ridiculous ideas that budget records are private and that student government can spend taxpayer money in secret," Hemlepp said.

Hemlepp said the budget documents and database records are necessary to report on how SGA will allocate its $18.6 million budget. Hemlepp argues that UCF's FERPA defense has no legal basis, as the budget documents are not educational records and the students waived their claim to privacy in taking an SGA position.

On August 11, the Ninth Florida Judicial Circuit Court ordered the university to release the documents to the paper within forty-eight hours, without redactions, and denied the university's request for attorney's fees.

The ruling was consistent with Hemlepp's position, with Judge John Jordan deciding that budget documents are not educational records, and that SGA participants implicitly waive their right to privacy with relation to their participation in governmental activities.

The university filed a stay to the ruling almost immediately, following it up with an appeal on August 22.

In previous years, UCF has released these records without a fight, and neither the student journalists nor the lawyer can determine why releasing in this instance has become such an issue.

"This information is and always has been public and for reasons I cannot understand, UCF has engaged in creative interpretation of what these rules mean," Hemlepp said.

If the court had ruled that the paper would be responsible for the fees, Hemlepp said it could have easily bankrupted the independent student news outlet.

Brigitte Snedeker, the editor-in-chief of *Knight News*, said it is unfortunate their university is willing to seek the destruction of a news outlet where students learn journalism.

"In my mind [seeking attorney's fees] is aggressive behavior because the university knows how small we are," Snedeker said.

Not only is the lawsuit using the financial resources of the site and taking time away from other reporting, Williams said the *Knight News*'s persistence in getting the records is causing students to feel that the news organization is antagonistic.

"It's leading students to believe that we're one-sided or that we're only going after SGA because we have some kind of grievance with them," he said.

And even if or when the records become available, the delay is still costly because of the loss of timely coverage about SGA spending, Williams said.

"We would prefer to have gotten them as soon as possible so students would have been more aware of what was happening in the university community as it was happening and not months after the fact," he said. Reported in: splc.org, September 12.

Lexington, Kentucky

The University of Kentucky filed a lawsuit against its student paper, the *Kentucky Kernel*, over an unfavorable decision by the state's attorney general regarding a records request. This action came in response to the paper's request for documents relating to the firing of a professor accused of sexual assault.

On August 8, the university announced its decision to sue the *Kentucky Kernel*, the independent student newspaper, over their open records request. On August 31, they made good on that threat.

The lawsuit came in response to an opinion by Attorney General Andy Beshear's office stating that the university had violated the state's Open Records Act by withholding records concerning a former associate professor's sexual misconduct case from the *Kernel*.

The day the complaint was filed, the university posted a statement to Twitter asserting that the lawsuit was necessary to protect those who report harassment under a promise of confidentiality: "We appealed the Office of AG's opinion to protect the rights of victim-survivors—today and those that follow."

Because of the way Kentucky's law is structured, a lawsuit is the only way for the university to appeal the attorney general's decision.

The issue began in April, when then editor-in-chief Will Wright requested documents detailing the university's investigation and subsequent dispensation into sexual harassment and assault complaints against former associate professor James Harwood.

The university did release documents that showed the final agreement between administrators and the accused professor, and the paper was able to report that the university entered into an agreement with Harwood allowing him to resign his position and continue to receive pay and benefits until he resigned August 31.

But Wright said there were still major gaps in the coverage because

reporters knew almost nothing else about the case without the remaining documents UK withheld. The documents the newspaper did receive were basically a conclusion of the case with few details, leaving journalists unable to confirm what actually took place, Marjorie Kirk, the *Kernel*'s current editor-in-chief said.

After the university declined to release additional records detailing their investigation, citing privacy concerns, the paper appealed to Beshear's office for an opinion. Beshear's office issued a memorandum on August 8, stating that the university had refused to release the documents to the attorney general's office for review and ruling the university must release the records—with names and identifiers of the witnesses redacted—as they were not proven to be protected under any exemptions to the open records law.

Beshear's decision prompted UK President Eli Capilouto to send a campus-wide email threatening to sue the *Kernel*. In the email, Capilouto cited the confidentiality and privacy of the victims as the reason for sealing the documents. Capilouto called the investigation "preliminary," and therefore not open to public record laws—though the case is closed.

But the *Kernel*, which has been in contact with the victims' spokesperson since they were first approached in March, reported that the victims wanted the documents to be public, with names and identifiers redacted. The spokesperson, the *Kernel* reported, said the victims were not contacted before Capilouto's email was sent—they only heard about it when they later saw an article about it.

And for Tom Miller, the attorney representing the *Kernel* in the suit, the university's claim for protecting the victims' privacy doesn't hold up.

"With the redaction of the names and of any identifying information, the students are not identifiable—therefore there is no privacy right being protected here," Miller said. "The victims have reported to the *Kernel* that they want the documents' information disclosed. To the extent the university is claiming that privacy is an interest, let [the university] go ask the victims—who they never talked to, according to the *Kernel*—and let them say if they want their rights protected."

Shortly after Beshear's decision and UK's announcement of the suit, a 122-page investigation document, with the victims' names and identifiers redacted, was handed over to the *Kernel* by a source related to the case. University officials would not confirm the authenticity of the documents acquired by the *Kernel*, but the newspaper reported that the report was signed by the university's deputy Title IX coordinator, Martha Alexander.

UK's lawsuit claims that Beshear erred in ordering disclosure of the records about UK's investigation because the documents are protected from disclosure for three reasons: because they are confidential "education records" under FERPA, because they are "preliminary" and do not represent the final outcome of the investigation, and because they contain attorney-client privileged material.

In a statement issued with the lawsuit, Jay Blanton, UK's executive director of public relations and marketing, said, "Our argument is not with the *Kentucky Kernel*. Respectfully, it is with an opinion from the Office of Attorney General that, if allowed to stand, would force the university to turn over private information about victim survivors to anyone, including the media, other students, employers, and strangers."

Blanton stated concerns about a possible chilling effect on the trust students and others on campus might have in the university and their willingness to report crimes of a similar nature were the attorney general's decision to stand up in court.

"The decision of the Attorney General, if it stands, would mean confidential and private information relative to a survivor wouldn't just have to be turned over to the *Kernel* or another newspaper. It would have to be turned over to a private citizen, fellow student or faculty or staff member. There would be no discretion," he said in an email.

But, according to the report, the case's complainants came forward only after finding there were other victims.

The *Kernel's* advisor, Chris Poore, said the students' appeal to the attorney general followed a common course of action—one that would elicit a decision backed by the force of law.

According to a statement from Capilouto, the university fully complies with 90 percent of open records requests, but in a small minority of cases, they feel they must deny the requests. "But in a handful of very specific cases, we are faced with the decision of whether transparency is more important than the need to protect the privacy and dignity of individual members of our community. It is not," Capilouto said in the statement.

The university will never release the names of victims of violence, not only for the safety of victims that are named in the documents, but also so that victims who have not yet come forward will feel comfortable doing so, he said.

However, it is the policy of the *Kernel*—and most newsrooms—to not print victims' names, and the attorney general's decision specified that the names and possible identifiers for the victims must be redacted from the documents.

But for Miller, who is fielding two other cases involving the university and its noncompliance with open records laws, UK might be toeing a thin legal line. "This is just a pattern of conduct the university has recently displayed by just refusing to comply with the Open Records Act," he said.

For Kirk, as the *Kernel* moves on in its legal proceedings and coverage of the new school year, she hopes the case could provide a stepping stone to amending policies that might undermine student safety nationally.

Because of a provision in his employment agreement with the university, Harwood was able to tender his resignation and forego a hearing—a policy that is recognized as a permissible resolution in federal Title IX guidelines. And because his resignation precluded a hearing, the victims who filed complaints against Harwood will not be able to appeal the decision and the investigation will not be disclosed if he applies for a job elsewhere.

"I would hope that instead of the legacy of this year being the year our university decided to sue our student newspaper, rather it would be the year our university was the first to take a stand against broken policies all over the country," Kirk said. Reported in: splc.org, September 12.

New York, New York

Fordham University has denied an application to form a Students for Justice in Palestine (SJP) chapter on campus, citing as its rationale the group's political goals—including its support for the boycott, divestment, and sanctions movement against Israel—and the potential for polarization.

Keith Eldredge, the dean of students at the Manhattan campus of Fordham, a Jesuit institution, outlined the reasons for the denial in a December 22 email. "While students are encouraged to promote diverse political points of view, and we encourage conversation and debate on all topics, I cannot support an organization whose sole purpose is advocating political goals of a specific group, and against a specific country, when these goals clearly conflict with and run contrary to the mission and values of the university," Eldredge wrote.

"There is perhaps no more complex topic than the Israeli-Palestinian conflict, and it is a topic that often leads to polarization rather than dialogue," Eldredge's letter continued. "The purpose of the organization as stated in the proposed club constitution points toward that polarization. Specifically, the call for boycott, divestment and sanctions of Israel presents a barrier to open dialogue and mutual learning and understanding."

The civil rights and legal advocacy organizations Palestine Legal and the Center for Constitutional Rights first publicized the email from Eldredge as part of an eleven-page joint letter to Fordham's president. The letter describes in detail a protracted application process for the students who proposed the club—they first submitted an application in November 2015—and outlines the types of questions they report facing from administrators about their political beliefs and their plans to collaborate with Jewish organizations on campus. Those questions included "What does BDS mean to you?" "Does BDS mean the dissolution of the state of Israel?" and "Why use the term 'apartheid'?"

SJP chapters across the country have regularly attracted controversy with, for example, their programming marking "Israeli Apartheid Week" or with "mock eviction" events meant to draw attention to the removal of Palestinians from their homes. In its profile of the organization, the Anti-Defamation League (ADL), a civil rights group focused on anti-Semitism, describes SJP as "the primary organizer of anti-Israel events on U.S. college campuses and the group most responsible for bringing divestment resolutions to votes in front of student governments." ADL writes that "since its founding in 2001, SJP has consistently demonized Israel, describing Israeli policies toward the Palestinians as racist and apartheid-like, and comparing Israelis to Nazis or Israel to the Jim Crow-era U.S."

Yet SJP has organized on many campuses, with many college and university leaders viewing the group as a part of the student organizing landscape (one that often includes pro-Israel groups). Various SJP chapters have had run-ins with college administrators before—Palestine Legal has written previously about what it describes as the differential treatment of student groups that focus on Palestinian issues, writing in a 2015 report that "universities often respond to complaints from Israel advocacy groups by investigating and disproportionately disciplining students and student groups for events and actions in support of Palestinian rights"—but Radhika Sainath, a staff attorney for the organization, said this is the first case of which they're aware in which a SJP chapter has been preemptively banned.

"All evidence indicates that the denial was based on the viewpoint of students' message and/or their national origin," the joint letter from Palestine Legal and the Center for Constitutional Rights states. The letter observes that all four of the original applicants for the SJP chapter's executive board were students of color, three were Muslim and one was Palestinian American.

The letter continues, "The denial violates free speech and association

principles, the university's commitment to protect free inquiry, and could give rise to a violation of Title VI of the Civil Rights Act," which prohibits discrimination on the basis of race, color, or national origin.

The Foundation for Individual Rights in Education, or FIRE, which advocates for free speech on campuses, has also taken an interest in the case and plans to send its own letter to Fordham, according to Ari Cohn, the director of FIRE's individual rights defense program. "In this case, I think that the justification for denying SJP recognition is completely without merit and cannot stand at any university that proclaims that it values freedom of expression, which Fordham's written policies do," said Cohn.

Cohn noted that Fordham has chapters of the College Democrats and College Republicans, both of which advocate for specific political goals. "The fact that the group [SJP] is oriented toward advocating a specific political viewpoint is not out of the ordinary, and student organizations at every campus across the country do just that," Cohn said. "It's a little bit baffling to see that justification used to deny a student organization recognition."

Eldredge, the dean of students who wrote the email outlining the reasons for the denial, referred an interview request to a college spokesman, Bob Howe, who issued a written statement. "Fordham has no registered student clubs the sole focus of which is the political agenda of one nation, against another nation," the statement said. "For the university's purposes, the country of origin of the student organizers is irrelevant, as is their particular political stance. The narrowness of Students for Justice in Palestine's political focus makes it more akin to a lobbying group than a student club. Regardless of the club's status, students, faculty and staff are of course free to voice their opinions on Palestine, or any other issue."

Ahmad Awad, a graduating senior at Fordham and the would-be president of the SJP chapter, said the group is still pushing for recognition on campus. He said Eldredge's reasoning for denying the organization club status is contradictory to Fordham's mission statement, which articulates a commitment to freedom of inquiry and to the promotion of justice and protection of human rights.

"Yet we were declined when that's what we were trying to advocate for," said Awad. "We're advocating for a free Palestinian people. We're advocating for a Palestinian people who are not oppressed and occupied." Reported in: insidehighered.com, January 18.

NET NEUTRALITY
Washington, DC

The U.S. Federal Communications Commission's two Republican members told internet service providers December 19 that they will get to work on gutting net neutrality rules "as soon as possible."

FCC Republicans Ajit Pai and Michael O'Rielly sent a letter to five lobby groups representing wireless carriers and small ISPs; while the letter was mostly about plans to extend an exemption for small providers from certain disclosure requirements, the commissioners also said they will tackle the entire net neutrality order shortly after President-elect Donald Trump's inauguration on January 20.

"We will seek to revisit [the disclosure] requirements, and the Title II Net Neutrality proceeding more broadly, as soon as possible," they wrote, referring to the order that imposed net neutrality rules and reclassified ISPs as common carriers under Title II of the Communications Act. Pai and O'Rielly noted that they "dissented from the Commission's February 2015 Net Neutrality decision, including the Order's imposition of unnecessary and unjustified burdens on providers."

Pai and O'Rielly will have a 2–1 Republican majority on the FCC after the departure of Democratic Chairman Tom Wheeler on January 20. Pai previously said that the Title II net neutrality order's "days are numbered" under Trump, while O'Rielly said he intends to "undo harmful policies" such as the Title II reclassification.

The net neutrality order gave ISPs with 100,000 or fewer subscribers a temporary exemption from enhanced transparency requirements that force operators to provide more information about the plans they offer and their network performance. ISPs can comply with the rules by adopting "nutrition labels" that give consumers details about prices (including hidden fees tacked onto the base price), data caps, overage charges, speed, latency, packet loss, and so on.

The exemption for small providers lapsed on December 15 after the FCC couldn't agree on a deal to extend it. Pai and O'Rielly tried to convince fellow commissioners to extend the exemption for small providers and apply it to any ISP with up to 250,000 subscribers.

To make things more complicated, the enhanced transparency rules haven't yet taken effect for ISPs of any size because that portion of the net neutrality order required an additional review by the Office of Management and Budget (OMB) to comply with the Paperwork Reduction Act. The OMB finally approved the new requirements in December, and they are now set to take effect on January 17.

"We want to assure you and your members that we would not

support any adverse actions against small business providers for supposed non-compliance with the 'enhanced transparency' rules after that date [January 17]," Pai and O'Rielly wrote. That means small ISPs won't have to worry about complying even when the rules are technically in effect.

More broadly, the Title II net neutrality order prohibits ISPs from blocking or throttling traffic or giving priority to web services in exchange for payment. The order also set up a complaint process to prevent "unjust" or "unreasonable" pricing and practices. The threat of complaints to the FCC helped put an end to several disputes between ISPs and other network operators over network interconnection payments; this in turn improved internet service quality for many subscribers.

All of that is in jeopardy with the Pai/O'Rielly promise to undo the entire Title II net neutrality order. The process could take months, even if they get started right away, because of requirements to seek public comment. The Republican-controlled Congress could act more quickly, since Trump has opposed net neutrality rules and isn't likely to veto a bill overturning the Title II order. When either the FCC or Congress do act, the biggest question will be whether the net neutrality regime is replaced with a weaker set of rules or scrapped entirely.

Shortly after his inauguration, President Trump appointed Pai to succeed Wheeler as chair of the FCC. Although consistent with Trump's largely deregulatory agenda, Pai's appointment breaks from the president's habit of appointing Washington outsiders to key roles. A former lawyer for Verizon and the Justice Department, Pai is well-versed in the minutiae of America's telecom law. He has pushed for streamlining the FCC's operations, accelerating the rollout of airwaves for mobile broadband and knocking down regulatory barriers that he claims deter companies from investing in wired internet. In a December speech, he said it was time to fire up the "regulatory weed whacker."

Consumer advocates urged Pai to safeguard consumer protections and prevent large corporations from unreasonably raising prices.

"Chairman Pai has a record of promising to undo the agency's landmark 2015 net neutrality rules as well as targeting consumer privacy while refusing to stand against consolidation among telecommunications and media giants," the advocacy organization Public Knowledge said in a release.

Pai's opposition to the commission's net neutrality rules could give Republicans in Congress the political room to craft a legislative deal with Democrats who view net neutrality protections as a key to preserving competition, policy analysts said. Senator John Thune (R-S.D.), chair of the Senate Commerce Committee, said he is committed to drawing up a "long-term legislative solution to protecting the open Internet." Reported in: arstechnica.com, December 20; *Washington Post*, January 23.

SOCIAL MEDIA
Washington, DC

The U.S. government quietly began in December requesting that select foreign visitors provide their Facebook, Twitter, and other social media accounts on arriving in the country, a move designed to spot potential terrorist threats that drew months of opposition from tech giants and privacy hawks alike.

Since December 20 foreign travelers arriving in the United States on the visa waiver program have been presented with an "optional" request to "enter information associated with your online presence," a government official confirmed. The prompt includes a drop-down menu that lists platforms including Facebook, Google+, Instagram, LinkedIn, and YouTube, as well as a space for users to input their account names on those sites.

The new policy came as Washington tries to improve its ability to spot and deny entry to individuals who have ties to terrorist groups like the Islamic State. But the government has faced a barrage of criticism since it first floated the idea last summer. The Internet Association, which represents companies including Facebook, Google, and Twitter, at the time joined with consumer advocates to argue the draft policy threatened free expression and posed new privacy and security risks to foreigners.

Now that it is final, those opponents are furious the Obama administration ignored their concerns.

"There are very few rules about how that information is being collected, maintained [and] disseminated to other agencies, and there are no guidelines about limiting the government's use of that information," said Michael W. Macleod-Ball, chief of staff for the American Civil Liberties Union's Washington office. "While the government certainly has a right to collect some information . . . it would be nice if they would focus on the privacy concerns some advocacy groups have long expressed."

A spokeswoman for Customs and Border Protection, who said the government approved the change on December 19, said the new policy is meant to "identify potential threats." Previously, the agency had said it wouldn't prohibit entry to foreigners who didn't provide their social media account information.

The question itself is included in what's known as the Electronic

System for Travel Authorization (ESTA), a process that certain foreign travelers must complete to come to the United States. ESTA and a related paper form specifically apply to those arriving here through the visa-waiver program, which allows citizens of thirty-eight countries to travel and stay in the United States for up to ninety days without a visa.

As soon as the government unveiled its draft proposal in June, however, consumer protection advocates expressed outrage. In a letter sent in August, the ACLU, Center for Democracy and Technology charged it posed immense privacy risks, given that social media accounts serve as "gateways into an enormous amount of [users'] online expression and associations, which can reflect highly sensitive information about that person's opinions, beliefs, identity and community." The groups also predicted the burden would "fall hardest on Arab and Muslim communities, whose usernames, posts, contacts and social networks will be exposed to intense scrutiny."

After the policy changed, Nathan White, the senior legislative manager of Access Now, again blasted it as a threat to human rights.

"The choice to hand over this information is technically voluntary," he said. "But the process to enter the U.S. is confusing, and it's likely that most visitors will fill out the card completely rather than risk additional questions from intimidating, uniformed officers—the same officers who will decide which of your jokes are funny and which ones make you a security risk."

Opponents also worry that the U.S. change will spark similar moves by other countries.

"Democratic and nondemocratic countries—including those without the United States' due process protections—will now believe they are more warranted in demanding social media information from visitors that could jeopardize visitors' safety," said Internet Association general counsel Abigail Slater. "The nature of the DHS' requests delves into personal information, creating an information dragnet." Reported in: politico.com, December 22.

Parma, Ohio

Anthony Novak, who was arrested for creating a parody of the Parma, Ohio, police department's Facebook page, has filed a federal lawsuit accusing seven officers of violating his constitutional rights by using the legal system to punish him for making fun of them.

In August, Novak was acquitted of using a computer and the internet to "disrupt, interrupt, or impair" police services, a felony punishable by up to eighteen months in prison. Now he is trying to get some compensation from the city for the injuries inflicted by that charge, arguing that the police did not have probable cause to arrest him or search his apartment. He also argues that the statute used to prosecute him is "unconstitutionally overbroad because it provides the police unfettered discretion to wrongfully arrest and charge civilians in the State of Ohio with a crime for exercising their First Amendment rights."

Novak's parody, which he posted on March 1 and deleted on March 3 after the Parma Police Department issued an indignant press release about it, copied the logo from the department's actual Facebook page but was in other respects notably different. It included notices announcing "our official stay inside and catch up with the family day," during which anyone venturing outside between noon and 9 p.m. would be arrested; advertising a "Pedophile Reform event" where sex offenders who visited all of the "learning stations" could qualify to be removed from the state's sex offender registry; and offering teenagers abortions, to be performed in a van in the parking lot of a local supermarket "using an experimental technique discovered by the Parma Police Department."

There was also a warning that anyone caught feeding the homeless would go to jail as part of "an attempt to have the homeless population eventually leave our city due to starvation," along with an ad seeking applicants for jobs with the police department that said "Parma is an equal opportunity employer but is strongly encouraging minorities to not apply."

The police were not amused. "The Parma Police Department would like to warn the public that a fake Parma Police Facebook page has been created," said a Facebook notice posted on March 2. "This matter is currently being investigated by the Parma Police Department and Facebook. This is the Parma Police Department's official Facebook page. The public should disregard any and all information posted on the fake Facebook account. The individual(s) who created this fake account are not employed by the police department in any capacity and were never authorized to post information on behalf of the department."

Despite the implication that people might think officers really were performing abortions in a van or really did plan to promote family togetherness by forcibly confining people to their homes, it is hard to believe anyone mistook the parody for the real thing. "The Facebook page was not reasonably believable as conveying the voice or messages of the City of Parma Police Department," Novak's complaint notes. "Mr. Novak had no intention of deceiving people into believing that the account was actually

operated by a representative of the police department, and no reasonable person could conclude such an intent from the content of the page."

Parma police nevertheless launched an investigation that involved at least seven officers, a subpoena, and three search warrants, and a raid on Novak's apartment, during which police surprised his roommate on the toilet and seized two hard drives, a laptop, two tablets, two cellphones, and two video game systems. After his arrest on March 25, Novak spent four days in jail before he got out on bail, and then he had to report weekly to a probation officer if he wanted to keep his freedom.

Explaining the justification for Novak's arrest, Lieutenant Kevin Riley, a department spokesman and one of the officers named in the lawsuit, said "the material that Novak posted on the fake account crossed the line from satire to an actual risk to public safety." How so? Riley complained that "Novak posted derogatory and inflammatory information that purported to be from the Parma Police Department."

The police knew it was inflammatory because people had posted negative comments about the department on the parody page, including "Fuck the Parma Police."

It was obvious how Novak had offended the police but not so clear how he had disrupted police services. Even after settling on that charge, Novak's lawsuit notes, the police had no "supportive evidence or facts that any of the functions of the Parma Police Department had been disrupted or that Mr. Novak intended his Facebook page to in fact disrupt any function of the Parma Police Department." When they applied for a search warrant demanding that Facebook surrender the records associated with the parody page, the police "failed to mention any function or service that Mr. Novak purportedly disrupted." The post-arrest press release likewise "mentioned nothing about any police function that Mr. Novak intentionally disrupted through the exercise of his constitutional rights."

Someone in the Cuyahoga County Prosecutor's Office evidently had second thoughts about the case because Novak was offered a plea deal under which the felony charge would have been reduced to an unspecified misdemeanor. Novak turned the offer down, by that point eager to have his day in court. By the time his trial rolled around, prosecutors had settled on the theory that Novak's Facebook gag had disrupted police services by generating phone calls to the police department—a grand total of ten in twelve hours. The jury did not buy it.

To this day Riley maintains that "we were just doing our job." Which is true, if you assume an officer's job includes hunting down online speech that offends him, making sure it is scrubbed from the internet, and trying to imprison the people responsible for it. Reported in: *Reason*, September 21.

PRIVACY
San Francisco, California

Yahoo secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials, according to people familiar with the matter. The company complied with a classified U.S. government demand, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said three former employees and a fourth person apprised of the events.

Some surveillance experts said this was the first case to surface of a U.S. internet company agreeing to an intelligence agency's request by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time.

It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.

Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request.

According to two of the former employees, Yahoo Chief Executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook.

"Yahoo is a law abiding company, and complies with the laws of the United States," the company said in a brief statement in response to Reuters questions about the demand. Yahoo declined any further comment.

The request to search Yahoo Mail accounts came in the form of a classified edict sent to the company's legal team, according to the three people familiar with the matter.

U.S. phone and internet companies are known to have handed over bulk customer data to intelligence agencies. But some former government officials and private surveillance experts said they had not previously seen either such a broad demand for real-time web collection or one that required the creation of a new computer program.

"I've never seen that, a wiretap in real time on a 'selector,'" said Albert Gidari, a lawyer who represented

phone and internet companies on surveillance issues for twenty years before moving to Stanford University last year. A selector refers to a type of search term used to zero in on specific information.

"It would be really difficult for a provider to do that," he added.

Experts said it was likely that the NSA or FBI had approached other internet companies with the same demand, since they evidently did not know what email accounts were being used by the target. The NSA usually makes requests for domestic surveillance through the FBI, so it is hard to know which agency is seeking the information.

Alphabet's Google and Microsoft, two major U.S. email service providers, separately said that they had not conducted such email searches.

"We've never received such a request, but if we did, our response would be simple: 'No way,'" a spokesman for Google said in a statement.

A Microsoft spokesperson said in a statement, "We have never engaged in the secret scanning of email traffic like what has been reported today about Yahoo." The company declined to comment on whether it had received such a request.

Under laws including the 2008 amendments to the Foreign Intelligence Surveillance Act, intelligence agencies can ask U.S. phone and internet companies to provide customer data to aid foreign intelligence-gathering efforts for a variety of reasons, including prevention of terrorist attacks.

Disclosures by former NSA contractor Edward Snowden and others have exposed the extent of electronic surveillance and led U.S. authorities to modestly scale back some of the programs, in part to protect privacy rights.

Companies including Yahoo have challenged some classified surveillance before the Foreign Intelligence Surveillance Court, a secret tribunal.

Some FISA experts said Yahoo could have tried to fight last year's demand on at least two grounds: the breadth of the directive and the necessity of writing a special program to search all customers' emails in transit.

Apple made a similar argument earlier last year when it refused to create a special program to break into an encrypted iPhone used in the 2015 San Bernardino massacre. The FBI dropped the case after it unlocked the phone with the help of a third party, so no precedent was set.

"It is deeply disappointing that Yahoo declined to challenge this sweeping surveillance order, because customers are counting on technology companies to stand up to novel spying demands in court," Patrick Toomey, an attorney with the American Civil Liberties Union, said in a statement.

Some FISA experts defended Yahoo's decision to comply, saying nothing prohibited the surveillance court from ordering a search for a specific term instead of a specific account. So-called "upstream" bulk collection from phone carriers based on content was found to be legal, they said, and the same logic could apply to web companies' mail.

As tech companies become better at encrypting data, they are likely to face more such requests from spy agencies.

Former NSA General Counsel Stewart Baker said email providers "have the power to encrypt it all, and with that comes added responsibility to do some of the work that had been done by the intelligence agencies."

Mayer and other executives ultimately decided to comply with the directive last year rather than fight it, in part because they thought they would lose, said the people familiar with the matter.

Yahoo in 2007 had fought a FISA demand that it conduct searches on specific email accounts without a court-approved warrant. Details of the case remain sealed, but a partially redacted published opinion showed Yahoo's challenge was unsuccessful.

Some Yahoo employees were upset about the decision not to contest the more recent edict and thought the company could have prevailed, the sources said. They were also upset that Mayer and Yahoo General Counsel Ron Bell did not involve the company's security team in the process, instead asking Yahoo's email engineers to write a program to siphon off messages containing the character string the spies sought and store them for remote retrieval, according to the sources.

The sources said the program was discovered by Yahoo's security team in May 2015, within weeks of its installation. The security team initially thought hackers had broken in.

When Stamos found out that Mayer had authorized the program, he resigned as chief information security officer and told his subordinates that he had been left out of a decision that hurt users' security, the sources said. Due to a programming flaw, he told them hackers could have accessed the stored emails.

Stamos's announcement in June 2015 that he had joined Facebook did not mention any problems with Yahoo.

In a separate incident, Yahoo last month said "state-sponsored" hackers had gained access to 500 million customer accounts in 2014. The revelations have brought new scrutiny to Yahoo's security practices as the company tries to complete a deal to sell its core business to Verizon for $4.8 billion. Reported in: reuters.com, October 4.

Washington, DC

Federal officials approved broad new privacy rules October 27 that prevent companies like AT&T and Comcast from collecting and giving out digital information about individuals—such as the websites they visited and the apps they used—in a move that creates landmark protections for internet users.

By a 3-to-2 vote, the Federal Communications Commission clearly took the side of consumers. The new rules require broadband providers to obtain permission from subscribers to gather and give out data on their web browsing, app use, location and financial information. Currently, broadband providers can track users unless those individuals tell them to stop.

It was the first time the FCC has passed such online protections. The agency made privacy rules for phones and cable television in the past, but high-speed internet providers, including AT&T and Verizon, were not held to any privacy restrictions, even though those behemoth companies have arguably one of the most expansive views of the habits of web users.

The passage of the rules dealt a blow to telecommunications and cable companies like AT&T and Comcast, which rely on such user data to serve sophisticated targeted advertising. The fallout may affect AT&T's $85.4 billion bid for Time Warner, which was announced in October, because one of the stated ambitions of the blockbuster deal was to combine resources to move more forcefully into targeted advertising.

"There is a basic truth: It is the consumer's information," Tom Wheeler, the chairman of the FCC, said of the necessity of protecting internet users who want more control over how companies treat their private information. "It is not the information of the network the consumer hires to deliver that information."

Privacy groups applauded the new rules, which they said brought the United States more in line with European nations that have moved aggressively to protect their citizens' online privacy.

"For the first time, the public will be guaranteed that when they use broadband to connect to the internet, whether on a mobile device or personal computer, they will have the ability to decide whether and how much of their information can be gathered," said Jeffrey Chester, executive director of the Center for Digital Democracy.

The outcry from industries that depend on online user data was also swift. Cable lobbying groups called the rules a result of "regulatory opportunism," while the Association of National Advertisers labeled the regulations "unprecedented, misguided, counterproductive, and potentially extremely harmful."

Even with the new rules, online privacy remains tricky. Many people have been lackadaisical about what information they give up online when they register for websites or digital services. The convenience of free services like maps also appeals to people, even though they give companies access to personal information. And some people unknowingly forgo their privacy when allowing apps or other services to track their location or follow their browsing across websites.

The FCC rules also have their limits. Online ad juggernauts, including Google, Facebook, and other web companies, are not subject to the new regulations. The FCC does not have jurisdiction over web companies. Those companies are instead required to follow general consumer protection rules enforced by the Federal Trade Commission. That means Google does not have to explicitly ask people permission first to gather web browsing habits, for example.

AT&T, Verizon, and Comcast will also still be able to gather consumers' digital data, though not as easily as before. The FCC rules apply only to their broadband businesses. That would mean data from the habits of AT&T's wireless and home broadband customers would be subject to the regulations, but not data about AT&T's DirecTV users or users of the HBO Now app, which would come with the merger with Time Warner, for example.

The companies also have other ways to collect information about people, including the purchase of data from brokers.

AT&T, which has criticized the privacy regulations for internet service providers, would not comment on how the rules would affect its proposed purchase of Time Warner. But it emphasized the benefits of ads that allow for free and cheaper web services.

"At the end of the day, consumers desire services which shift costs away from them and toward advertisers," said Robert W. Quinn Jr., AT&T's senior executive vice president for external and legislative affairs. "We will look at the specifics of today's action, but it would appear on its face to inhibit that shift of lower costs for consumers by imposing a different set of rules on" internet service providers.

Comcast said that the rules were not needed and that the FCC did not prove that broadband providers were hurting consumers.

For over two decades, internet service providers "and all other internet companies have operated under the FTC's privacy regime and, during that time, the internet thrived; consumer privacy was protected," said David L. Cohen, Comcast's senior executive vice president.

Major broadband providers will have about one year to make the changes required by the new rules; the companies must notify users of their new privacy options in ways like email or dialogue boxes on websites. After the rules are in effect, broadband providers will immediately stop collecting what the FCC deems sensitive data, including Social Security numbers and health data, unless a customer gives permission.

The new rules are among a set of last-ditch moves by Wheeler to make the FCC a stronger watchdog over the broadband industry. Since he was appointed FCC chairman in 2013, he has tried to open the cable box market in an effort to promote streaming videos, among other actions. Wheeler is entering what are probably the last few months of his tenure at the agency, as he was not expected to be reappointed by whoever becomes the next president.

The FCC proposed the broadband privacy rules in March. That followed the reclassification of broadband last year into a utilitylike service, a move that required broadband to have privacy rules similar to those imposed on phone companies.

Once the rules were proposed, the FCC immediately faced a backlash. Cable and telecom companies created a lobbying group called the 21st Century Privacy Coalition to fight off the regulations. The group is led by Washington heavyweights like Jon Leibowitz, the former chairman of the FTC, and former Representative Mary Bono, Republican of California. Henry A. Waxman, former chairman of the House Energy and Commerce Committee and a Democrat, was also hired by the 21st Century Privacy Coalition and wrote an op-ed article in The Hill to protest the rules.

Even some web companies protested the proposed rules. Google said in comments filed to the FCC this month that the regulations should not include web browsing, because that does not necessarily include sensitive personal information.

"Consumers benefit from responsible online advertising, individualized content, and product improvements based on browsing information," wrote Austin Schlick, Google's director of communications law.

In the end, the objections had little effect on the FCC.

"Hopefully, this is the end of what has been the race to the bottom for online privacy, and hopefully the beginning of a race to the top," said Harold Feld, senior vice president at Public Knowledge, a nonprofit public interest group. Reported in: *New York Times*, October 27.

Washington, DC

A broad coalition of over fifty civil liberties groups delivered a letter to the Justice Department's civil rights division October 18 calling for an investigation into the expanding use of face recognition technology by police. "Safeguards to ensure this technology is being used fairly and responsibly appear to be virtually nonexistent," the letter stated. The routine unsupervised use of face recognition systems, according to the dozens of signatories, threatens the privacy and civil liberties of millions—especially those of immigrants and people of color.

These civil rights groups were provided with advance copies of a watershed 150-page report detailing—in many cases for the first time—how local police departments across the country have been using facial recognition technology. Titled "The Perpetual Lineup," the report, published October 18 by the Georgetown Center on Privacy and Technology, reveals that police deploy face recognition technology in ways that are more widespread, advanced, and unregulated than anyone has previously reported.

"Face recognition is a powerful technology that requires strict oversight. But those controls by and large don't exist today," said Clare Garvie, one of the report's co-authors. "With only a few exceptions, there are no laws governing police use of the technology, no standards ensuring its accuracy, and no systems checking for bias. It's a wild west."

Of the fifty-two agencies that acknowledged using face recognition in response to 106 records requests, the authors found that only one had obtained legislative approval before doing so. Government reports have long confirmed that millions of images of citizens are collected and stored in federal face recognition databases. Since at least 2002, civil liberties advocates have raised concerns that millions of drivers license photos of Americans who have never been arrested are being subject to facial searches—a practice that amounts to a perpetual digital lineup. This report augments such fears, demonstrating that at least one in four state or local law enforcement agencies have access to face recognition systems.

Among its findings, the report provides the most fine-grained detail to date on how exactly these face recognition systems might disproportionately impact African Americans. "Face recognition systems are powerful—but they can also be biased," the coalition's letter explains. While one in two American adults have face images stored in at least one database, African Americans are more likely than others to have their images captured and searched by face recognition systems.

In Virginia, for instance, the report shows how state police can search a mug shot database disproportionately populated with African

Americans, who are twice as likely to be arrested in the state. Not only are African Americans more likely to be subject to searches, according to the report, but this overrepresentation puts them at greatest risk for a false match.

These errors could be compounded by the fact that some face recognition algorithms have been shown to misidentify African Americans, women, and young people at unusually high rates. In a 2012 study co-authored by FBI experts, three algorithms that were tested performed between 5 and 10 percent worse on black faces than on white faces. And the overall accuracy of systems has been shown to decrease as a dataset expands. The Georgetown report interviewed two major facial recognition vendors which said that they did not test for racial basis, despite the fact that systems have been shown to be far from "race-blind."

A slideshow on San Diego's privacy policy obtained by the researchers reveals that people of color in the county are between 1.5 and 2.5 times more likely to be targeted by its surveillance systems. San Diego County uses a mugshot-only system, and repeated studies have shown that African Americans are twice as likely as white people to be arrested and searched by police.

The Georgetown report shows for the first time that at least five major police departments have "run real-time face recognition off of street cameras, bought technology that can do so, or expressed a written interest in buying it." They warn that such real-time surveillance tracking could have serious implications for the right to associate privately.

"This is the ability to conduct a real time digital manhunt on the street by putting people on a watchlist," explained Alvaro Bedoya, the executive director of the Georgetown Center and one of the report's co-authors. "Now suddenly everyone is a suspect." Real-time recognition, he added, could have a chilling effect on people engaging in civil conduct. "It would be totally legal to take picture of people obstructing traffic and identify them."

Indeed, as the ACLU revealed the previous week, face recognition systems were used to track Black Lives Matter protesters in Baltimore. "There's a question of who is being subjected to this kind of facial recognition search in the first place," David Rocah, a staff attorney at the ACLU of Maryland, told the *Baltimore Sun*. "Is it only Black Lives Matter demonstrators who get this treatment? Are they drawing those circles only in certain neighborhoods? The context in which it's described here seems quintessentially improper."

Bedoya pointed out that these systems in Baltimore uploaded social media photographs of protestors into these systems to conduct real-time street surveillance. "It turns the premise of the Fourth Amendment on its head," he added.

The Georgetown report shows that some departmental policies allow for face recognition algorithms to be used in the absence of an individualized suspicion, which means the technology could conceivably be used to identify anyone. At least three agencies, according to the report, allow face recognition searches to identify witnesses of a crime in addition to criminal suspects.

As privacy organizations have previously noted, the FBI's federal database includes and simultaneously searches photographic images of U.S. citizens who are neither criminals or suspects. The Georgetown report likewise shows that some state databases include mug shots, while others include both mug shots and driver's license photos.

In a landmark Supreme Court decision on privacy, in which the justices unanimously concluded that the prolonged use of an unwarranted GPS device violated the Fourth Amendment, Justice Sotomayor wondered whether "people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."

Of the fifty-two agencies found by the report to have used face recognition, however, only one department's policy explicitly prohibited officers from "using face recognition to track individuals engaging in political, religious, or other protected free speech."

Apart from some news stories focusing on the policies of specific departments, most notably those of San Diego County, reporting on law enforcement's use of face recognition technology has been scarce. Departments themselves have not been forthcoming about their use of the technology to identify suspects on the streets and to secure convictions. And many of the documents obtained by privacy organizations about face recognition programs largely date to 2011, prior to the federal face program's full implementation.

This is partly due to how little information is available. There is no national database of departments using these programs, how they work, what policies govern them, who can access them, and how the passive information is being collected and queried. The Georgetown report, compiling tens of thousands of records produced in response to Freedom of Information requests sent to fifty of the largest police departments across the country, provides the most comprehensive

snapshot to date of how and on whom face recognition systems are used—and what policies constrain their use, if any. But even this picture continues to be partial, given the continued lack of transparency of several large law enforcement agencies with some of the most advanced systems.

The researchers state that despite several news articles and descriptions of the New York Police Department's face recognition program, the NYPD denied their records request entirely, arguing that the records fell under a "non-routine techniques and procedures" exemption. Likewise, while the Los Angeles Police Department has claimed to use real-time, continuous face recognition and has made decades of public statements about the technology, the department found "no records responsive to [their] request" for information about this or any other face recognition system. "We followed up with a number emails and calls inquiring what that meant," Garvie said. "The final word was that they found no records responsive."

Of the fifty-two agencies that did provide responsive records to the researchers, at least twenty-four did not provide a face recognition use policy. Four of those two dozen agencies admitted that they expressly lacked any policy whatsoever to govern their face recognition systems.

Civil rights groups have long described the difficulties of calling for greater oversight for a system whose contours, uses, and abuses are unknown. The amount of up-to-date public records collected by the Georgetown researchers has the potential to change this and spark a national conversation on oversight, Bedoya said.

"I genuinely hope that more and more of the American public has a chance to see what's at stake here," Bedoya said, describing face recognition as "an extraordinarily powerful tool." "It doesn't just track our phones or computers. It tracks our flesh and our bones. This is a tracking technology unlike anything our society has ever seen. You don't even need to touch anything."

No national guidelines, laws, or polices currently regulate law enforcement's use of face recognition technology. To fill this gap, the Georgetown report proposes protective legislation for civil liberties, limits on the amount and types of data stored, and a push for independent oversight and public notice procedures.

Among their recommendations, the Georgetown researchers advise that mug shots, rather than driver's license and ID photos, be used to populate photo databases for face recognition, and for those images to be "periodically scrubbed to eliminate the innocent." They also suggest that financing for police face recognition systems be contingent "on public reporting, accuracy and bias tests, legislative approval—and public posting—of a face recognition use policy."

In Seattle, where a face recognition program was funded by a $1.64 million grant from the Department of Homeland Security, some of these model guidelines are already in place. Only specially trained officers use the software, real-time use is banned, and the software's use is limited to scanning suspicious subjects only.

The ACLU, when it first investigated nascent uses of face recognition technology back in 2002, presciently warned that the "worst-case scenario . . . would be if police continue to utilize facial recognition systems despite their ineffectiveness because they become invested in them, attached to government or industry grants that support them, or begin to discover additional, even more frightening uses for the technology."

The Georgetown report offers a glimpse into this worst-case scenario, but Bedoya is hopeful that the Model Face Recognition Act proposed by the report and endorsed by the letter's signatories provides a "deeply reasonable" solution. He pointed to the fact that state legislatures have previously passed laws to limit geolocation technology by police, automatic license plate readers, drones, wiretaps, and other surveillance tools. "This is very feasible. It's not about protecting criminals. It's about protecting our values." Reported in: *The Intercept*, October 18.

Jackson, Mississippi

Mississippi's Democratic attorney general is again tangling with Google, alleging in a lawsuit that the company is illegally violating student privacy, even as some Republicans seek to muzzle his ability to file such civil suits.

Attorney General Jim Hood sued the California-based computer giant January 13 in Lowndes County Chancery Court. In a news conference, Hood said Google is breaking Mississippi consumer protection law by selling ads using data from services it provides to schools.

"They're building a profile so they can advertise to them," Hood said. "They expressly stated in writing that they would not do that."

Hood said a test involving a student account from the state-run Mississippi School of Math and Science in Columbus showed ads targeted to previous searches. The attorney general wants a judge to order Google, a unit of Alphabet, to stop the practice.

The suit says Google could be fined up to $10,000 for each of its student accounts in Mississippi. With half the state's school districts using Google's email, calendar, and other online services, that amount could top $1 billion.

Hood sent a letter to local school superintendents asking them to preserve evidence to help with the lawsuit. He's advising parents to consult their local school systems.

"When you give a written contract and you don't follow it and you mine the data, then it's a violation of the Mississippi Consumer Protection Act. It's an unfair and deceptive trade practice," he said.

Google sued Hood in 2014, saying his wide-ranging attempts to investigate whether Google was helping music pirating and illegal drug sales were illegal. The U.S. Court of Appeals for the Fifth Circuit ruled in April that Hood's inquiry is legal. Hood said that the investigation continues but denied that he was motivated by personal animus against Google.

"You make decisions based on the facts and the law and you set emotions aside," Hood said.

Some Mississippi Republicans continue to try to trim Hood's ability to file civil lawsuits without outside permission, part of a long-running Republican perception that Hood pursues civil lawsuits in part to provide income to plaintiffs' lawyers who politically support him. Hood said outside lawyers brought the student privacy issue to him after publicity about his earlier dispute with Google.

A committee in the Republican-led House passed House Bill 555, which would require a three-person panel of the governor, lieutenant governor, and secretary of state to approve plans to file any civil lawsuit where the state could win more than $250,000. That panel is supposed to approve hiring outside lawyers for big lawsuits but has never met because Hood has instead hired lawyers according to a preset fee schedule that an earlier law allows as an alternative.

The bill to limit Hood's powers now moves to the full House. Similar measures have failed in previous years.

House Judiciary A Committee Chairman Mark Baker, a Brandon Republican, said Hood's use of civil lawsuits is a "rampant abuse" of his role.

"Every lawsuit that he files is a declaration of public policy" Baker said. "We're the legislators, the setters of public policy. He's the lawyer. He's not also the client." Hood, though, said efforts to limit his power violate the state's Constitution.

The attorney general's victories have contributed tens of millions of dollars to patch state budget holes in recent years. For example, Mississippi will gain $25 million from a settlement with New York-based Moody's over credit ratings the company assigned to various securities before the financial crisis. Last year, Hood collected about $55 million from lawsuits against large companies. Reported in: Associated Press, January 17.