NEWS IS IT LEGAL?

LIBRARIES

Buckner, Missouri

Is an event to educate people about what it means to be transgender appropriate for a public library?

The Mid-Continent Public Library held its first ever Trans 101 event on September 3, 2019, at the library system's Colbern Road branch in Lee's Summit, Missouri; about thirty people attended. A second Trans 101, scheduled for September 26 at the Buckner branch in Buckner, Missouri, was postponed after a contentious library board meeting.

Trans 101, a free event in a library meeting room, "is a presentation to talk about what it means to be transgender. It's to share a little bit about my life story," said Riley Long, the host of the program. One of the organizers of the event at the Colbern Road branch said that the turnout was high for an afternoon event scheduled on a weekday.

At the library board meeting on September 17, four people spoke out against the program; five spoke in favor of Trans 101.

"It's an inappropriate endorsement of a controversial topic," said State Representative Dan Stacy, a Republican from Blue Springs, "a political topic that should have had an opportunity for opposing views."

Inoru, a PhD candidate from Gladstone, said, "It is very apparent that people do not believe that this is a public library but their specific church."

When the second Trans 101 was postponed, "I was shocked," said Long, who had been planning the Trans 101 events with the library for the past year.

Later, a library board member from Platte County, Rita Wiese, penned a lengthy letter to the editor calling for an end to programs focused on topics dealing with gender identity.

"A once safe community setting known as the public library has become a space that, in the guise of intellectual freedom, wants to change thinking on voyeurism and gender confusion, while promoting materials and programs that lead children toward being sexually exploited," Wiese wrote in the November 6, 2019, edition of *The Landmark* newspaper.

Wiese closed out her letter urging others to attend the next library board meeting to speak on out the issue.

Library board meetings usually are sparsely attended, but dozens of people came to the meeting in November. An equal number spoke in favor of and against Trans 101 programs.

Crayola Bolger, a youth librarian with the Mid-Continent Library System, spoke in support of Trans 101. "Every single one of these Mid-Continent Public Library programs, whether we think they should be or not, they are all optional, no one has to go to one," she said.

The board didn't vote on the issue at the November meeting.

Steve Potter, who has been the CEO and library director of Mid-Continent for nine years, says it is the library's intention to get the program rescheduled after the board has time to think about the issue. Reported in: *The Pitch*, September 29, 2019; fox4kc.com, November 19.

Lebanon, New Hampshire

Should internet filters be installed on public library computers to limit the potential for children to access pornography?

The Library Board of Trustees at the Lebanon (New Hampshire) Public Libraries formed a task force to examine the question after concerns were raised in 2018 that two middle-school-age children might have viewed pornography at the downtown Lebanon library.

The panel concluded that filters "are expensive and don't work," according to Amy Lappin, deputy director of the Lebanon Public Libraries, who chaired the task force.

Or as the American Library Association puts it, "Content filters are unreliable because computer code and algorithms are still unable to adequately interpret, assess, and categorize the complexities of human communication, whether expressed in text or in image." The result, said Lappin, is that the software either fails to block inappropriate content or restricts access to legitimate information.

"As a steward of taxpayer funds," Library Director Sean Fleming told *Valley News,* "I don't want to use funds in a way that would be ineffective in addressing the concerns the community may have."

So what's the answer? Lappin says city libraries "intend to up our education game," including hosting an internet security event for parents next month. A *Valley News* editorial approved, stating,

> That seems to us a better approach than filters, and it also aligns with ALA guidance, which says that internet safety, for both children and adults, "is best addressed through educational programs that teach people how to find and evaluate information." That advice also reflects the reality that, when it comes to children, pornography is far from the only internet content that parents and the community at large need to worry about.
>
> It also strikes us that when an individual accesses inappropriate content on a library computer, the correct response is to address that behavior on an individual basis, rather than restricting access more broadly. Lebanon already has a policy on the books

that bars the display of "obscene or objectionable material" on library computers, which appears to cover that base.

Reported in: *Valley News*, October 26, 2019.

Seattle, Washington

Should library meeting rooms be open to groups spreading what many people call "hate speech"?

The Seattle Public Library is resisting calls to cancel an event held by a group called the "Women's Liberation Front" (WOLF). WOLF booked the Microsoft auditorium at the library for an event to be held on February 1, 2020. Critics say the talk, called "Fighting the New Misogyny," is anti-transgender.

The library emphasizes it's not hosting the event and doesn't endorse it, but said any group can book meeting spaces at the library.

On the library's Facebook page there are more than a thousand comments, with many people asking, how can a group that's spreading what they consider hate speech be allowed in a city building?

The Women's Liberation Front's Eventbrite page for their event questions transgender activism, saying, "Are the claims made by these activists actually true, or even coherent? What does it mean to say that people can be 'born in the wrong body'?"

Trans rights activist group, the Gender Justice League, said in a statement on their website, "A hate group using the library as a venue to 'critique' the existence of a minority group creates a hostile environment and is unacceptable."

The American Civil Liberties Union (ACLU) of Washington says the case is fairly cut and dry.

"If the public library canceled it based solely on the views espoused by WOLF, then yes, I think it would be problematic and in violation of the First Amendment," said Lisa Nowlin, a staff attorney for the ACLU. Nowlin has worked on both First Amendment cases and cases involving transgender rights.

"The views espoused by WOLF are harmful to the transgender and gender non-conforming intersex community," Nowlin said. She added, "I will fight for people's rights for free speech, and the ACLU will also fight to end discrimination." Reported in: KIRO-7 TV, December 10, 2019.

SCHOOLS

Loudoun County, Virginia

Should diversity—including diverse sexual orientations—be brought into classroom libraries in a community where many parents don't want their children exposed to LGBTQ themes?

Loudoun County Public Schools' (LCPS) diverse classroom libraries program was a prominent topic at Loudoun County School Board meetings on September 24, October 8, October 24, and November 12, 2019.

Superintendent Eric Williams and the LCPS administration introduced a list of "diverse books," organized by grade level, sorted into three categories: "Diverse Race, Culture, Language [and] Religion," "Disabilities/Abilities" and "LGBTQ."

A number of parents and students have voiced concerns about certain titles in the collection that feature content they consider gratuitously sexual or violent, with some speakers reading such passages verbatim before the dais. Some of these speakers said they support diversity in reading materials and wish only for certain titles to be reviewed; others have asked for the removal of the diverse classroom libraries altogether.

Conversely, other citizens have decried efforts to remove or modify the new collection as censorship and "book burning," opining that the collection should be preserved as is. They argue that the personal, often religious convictions of some parents should not dictate how LCPS controls the reading materials available to all students.

Assistant Superintendent for Instruction Ashley Ellis said that the LCPS Department of Instruction has begun division-level reviews of ten particularly controversial books in the high school diverse libraries. She explained that titles under review will ultimately either be maintained at its current level, "re-leveled" to another grade-level classroom library, moved from classroom libraries to general school libraries, or ousted from circulation altogether.

Board member Joy Maloney said she anticipates policy revisions to ensure uniform solutions to the issue, particularly involving the review process.

"Obviously it's concerning to me to see elementary school books moved to the school counseling office in some schools and not in others," she said. "To me that's something where we should be looking at something more division-wide as opposed to leaving that decision up to the school level."

Two books that drew much comment, both for removing and for keeping them, are picture books at the elementary level: *My Princess Boy* (2009) by Cheryl Kilodavis and *Prince & Knight* (2018) by Daniel Haack, both of which have been subject to numerous requests for reconsideration and division-level reviews.

Vice Chairwoman Brenda Sheridan said, "They're kids' books, they're fairy tales, and they're LGBTQ, and they're for the kids who need to read them." She added, "There's nothing graphic in these, there are no bad

words in these, there's no sex, there's nothing. It is just a story about a little boy who likes to wear a princess dress, and a prince and a knight."

Sheridan concluded by saying, "It is anti-LGBTQ when it comes to some of these book challenges."

Chairman Jeff Morse tried to keep the debate from turning into personal attacks, and to keep either side from making judgmental generalizations about the other. "When I hear the comment that, 'Oh, it's all about hate, that's the only reason those people are against those books,' that's not true," he said. "There are people with deep moral convictions that hold strongly to their faith, and [if] you don't agree with their faith that's fine, but that is their belief, and we support all of our communities and all of our religions and all faiths." Reported in: *Loudoun County Time-Mirror*, November 13, 2019.

COLLEGES AND UNIVERSITIES

Tuscaloosa, Alabama

When an African American university administrator is accused of racism for comments about race relations—his area of study—and immediately leaves the university, is that a violation of academic freedom?

The resignation of the dean of students of the University of Alabama (UA) at Tuscaloosa over a series of tweets about racism threatens to chill academic speech, PEN America said in a statement on September 9, 2019.

On September 4, Dr. Jamie Riley, assistant vice president and dean of students at the University of Alabama, resigned from his position "by mutual agreement" with the university. His resignation occurred the same day that rightwing media outlet Breitbart published an article featuring a series of tweets Riley wrote in 2016 and 2017, in which he commented on the issue of race in the United States.

"It is difficult to see Dr. Riley's 'resignation by mutual agreement' as anything other than a punitive outcome occasioned by the content of his speech," said Jonathan Friedman, project director for campus free speech at PEN America. "Prompted by a Breitbart story aimed to discredit Riley on the basis of past tweets, the university's acceptance of his resignation under pressure sends a chilling message to professors and administrators alike that expression of a controversial opinion could cost them their job."

It later came to light that University of Alabama will pay Dr. Riley $346,200 as a part of his resignation terms. The total sum is made up of $43,750, one quarter of Riley's salary, $175,000 in lost wages equal to one year's salary, and $127,450 as "compensatory damages."

The agreement prohibits Riley or UA from discussing the nature of his resignation or disparaging either party. The resignation agreement was made public in response to a state open records act request filed by AL.com.

Riley, who wrote his doctoral dissertation for his PhD on the subject of black male students on predominantly white campuses, had previously worked in student affairs and taught courses at numerous other colleges and universities prior to his time at University of Alabama.

"Dr. Riley's tweets were related to his area of academic expertise and his speech on political subjects is of precisely the type that a university must vigorously defend," said PEN America's Friedman. "The University of Alabama appears to have opted to have Dr. Riley fall on his sword rather than shoulder its own responsibility to stand up for academic freedom in the face of criticism."

In one of his tweets, from September 2017, Riley wrote, "The [American] flag represents a systemic history of racism for my people. Police are a part of that system. Is it that hard to see the correlation?" In a tweet from October 2017, Riley wrote that he was "baffled about how the 1st thing white people say is, 'That's not racist!' when they can't even experience racism? You have 0 opinion!" and in October 2016, Riley wrote, "Are movies about slavery truly about educating the unaware, or to remind Black people of our place in society?" Reported in: pen.org, September 9, 2019; AL.com, October 12.

Washington, D.C., and Chapel Hill, North Carolina

Does the federal government have a right to influence the content of federally funded college courses and programs that some politicians feel favor Muslims over Christians and Jews, or that may include criticism of Israel? Or is this a violation of academic freedom?

The US Department of Education threatened on August 29, 2019, to strip federal funding from a Middle East studies program run by Duke University and the University of North Carolina (UNC) at Chapel Hill. This has alarmed academics, who are worried about the federal government's apparent interest in the content of college courses and programs—Middle East studies in particular.

After an investigation prompted by a Republican congressman's complaint, the department warned the universities that the Duke-UNC Consortium for Middle East studies lacked viewpoint diversity and didn't offer enough courses and programming that presented the "positive aspects" of religious minorities in the Middle East, such as Christians and Jews.

That supposed lack of balance, a department official wrote in a letter to UNC's vice chancellor for research, suggested that the consortium was out of compliance with the terms of its annual $235,000 Title VI grant. Those grants support foreign-language and international studies programs and centers at many colleges, as well as fellowships for graduate students. The Duke-UNC consortium's funding was renewed in 2018 for four more years.

Under Title VI, federal "resource centers" like the Duke-UNC consortium must "provide a full understanding" of their areas and regions, said the department's letter.

The department's letter has prompted scholars to condemn what they see as a direct threat to academic freedom. While state governments sometimes weigh in on controversial course content, typically in elementary and secondary schools, many academics said this level of federal interest in details of campus offerings crosses a new, troubling frontier.

The letter has also put the field of Middle East studies on edge. Some professors fear that a chilling effect could discourage debates about controversial issues like the Israeli-Palestinian conflict.

Besides the Duke-UNC consortium, fourteen other Middle East centers receive Title VI funding. One is the Middle East Institute at Columbia University. Brinkley Messick, that institute's director and a professor of anthropology, said he was reluctant to comment much on the Duke-UNC investigation because he didn't want to draw the government's attention to the program.

"This concerns the essential role of the research university in a democratic society," Messick wrote in an email. He described the department's letter as "an aggressive demand for program 'balance' from an administration that is itself decidedly unbalanced."

The federal investigation began after the Duke-UNC consortium held a conference called "Conflict Over Gaza: People, Politics, and Possibilities" last spring. The event, which used $5,000 from the center's Title VI grant, according to the university, featured a performance by a Palestinian rapper during which he made anti-Semitic comments. A video of the performance was shared online. Those remarks were later condemned by the consortium itself and by UNC's interim chancellor. Reported in: *Chronicle of Higher Education*, September 22, 2019.

PRISONS
Florida, Nevada, Ohio, West Virginia, and other states

When prisons limit inmates' access to printed books, are e-books the solution—or does the cost of electronic editions still limit prisoners' ability to read the books they want?

Prisons sometimes justify limiting the distribution of physical books to inmates by claiming that drugs or other contraband may be smuggled in with the books. As an alternative, on November 1, 2019, JPay (a Securus Technologies company) began to grant free access to e-books for incarcerated individuals in Florida, Nevada, Ohio, and other states that are part of the National Association of Procurement Officials and the Multi-State Corrections Procurement Office.

E-books previously cost $0.99 per title, according to the contract signed by representatives of each state. That $0.99 fee went to JPay and was not distributed among state corrections departments.

The policy change gives those in Ohio prisons, for example, greater access to materials once inaccessible.

In early 2019, Ohio prisons began rejecting book donations from trusted partners, allowing book access only through JPay tablets. Print books were returned to volunteer organizations that work directly with prison systems nationwide, and so those books did not reach incarcerated individuals in Ohio.

Sara French, Deputy Communications Chief for the Ohio Department of Rehabilitation and Corrections (ODRC), said those decisions weren't made on a statewide basis, but instead, were made institution by institution.

In many states, significant latitude is given to individual institutions, while green-lit donors are vaguely defined as "publishers" or "distributors."

E-books do not always guarantee access. In West Virginia, incarcerated individuals are charged $0.05 per minute for access to e-books via state-provided "free" tablets, under a 2019 contract between the West Virginia Division of Corrections and Rehabilitation and Global Tel Link (GTL). Depending on how long it takes to read, an e-book may end up costing more than the price of a mass market paperback.

The Appalachian Prison Book Project, a nonprofit that offers free books and education to inmates, calls the fee structure exploitative.

"If you pause to think or reflect, that will cost you," says Katy Ryan, the group's founder and educational coordinator. "If you want to reread a book, you will pay the entire cost again. This is about generating revenue for the state and profit for the industry. Tablets under non-predatory terms could be a very good thing inside prisons. GTL does not provide that."

The Prison Policy Initiative estimated in 2017 that wages in West Virginia prisons range between $0.04 and $0.58 an hour, so inmates may not be

able to pay for everything they want to read.

GTL is one of JPay's biggest competitors in the market, which may have something to do with JPay's decision to offer e-books for free.

What JPay doesn't say is that it still collects money from incarcerated populations, and has profited off the free work of Project Gutenberg volunteers.

"Project Gutenberg has been informed by third parties that items from its library are being bundled with non-free, for-profit products. In particular, we have been informed that prison populations are being sold electronic tablets, and Project Gutenberg e-books make up some of the content on those tablets," said Gregory B. Newby, chief executive and director of Project Gutenberg. "Project Gutenberg has no relationship with any company that is selling content in prisons." Reported in: *Reason*, November 22, 2019; bookriot.com, December 5.

PRIVACY

Sacramento, California

How much will consumers' privacy be improved when the data brokers who collect and sell personal information are publicly identified?

The largely unregulated industry of data brokers that make billions of dollars annually buying and selling people's personal information will no longer be secret in California. In October 2019, California Governor Gavin Newsom signed into law a bill—AB 1202—that requires data brokers to register with the state attorney general. Their names and contact information for the first time will be available to the public after January 1, 2020.

Only one other state, Vermont, has similarly shined a light on data brokers. There is no similar law at the federal level.

The California bill had bipartisan backing.

"We have an entire data-collecting, data-sharing industry operating in the shadows," said Dylan Gilbert, policy counsel for the advocacy group Public Knowledge. "The average consumer has no idea these companies even exist, let alone what their names might be."

The data broker industry is believed to be worth about $200 billion. Some of the biggest players are known to all, such as the credit bureaus Experian, Equifax, and TransUnion, which maintain files on millions of Americans.

Others are smaller, quieter firms that specialize in gathering people's personal information from public and private sources and making it available to other companies for marketing, employment, financial, and other purposes.

California's new privacy law will allow consumers to instruct companies to delete their personal information and to opt out of having their information shared. It is unclear how this would be enforced.

The law applies to any company doing business in the state. This means consumers will be able to contact their phone or cable company, for example, and tell them to no longer make the consumer's personal information available to others.

The privacy law says consumers can opt out of having their data shared by companies with third parties. But what if that company got its information from elsewhere? Is there still a third party if the first party (the consumer) isn't the direct source of the data?

"I'd say you could still opt out," said Paul Schwartz, co-director of UC Berkeley's Center for Law and Technology. "But there's a little ambiguity."

The onus would be on consumers to contact potentially hundreds of data brokers and opt out from each one individually—a task few people would have the time or patience to embark upon.

"Creating a list of data brokers is a first step in helping consumers know who these actors are, but that does nothing to constrain their practices," said Jen King, director of privacy at Stanford Law School's Center for Internet and Society. Reported in: *Los Angeles Times*, November 5, 2019.

Washington, D.C.

Will the federal government recognize the value of data encryption and stop seeking a backdoor for law enforcement to read private personal and business communications?

On October 22, 2019, the former general counsel of the FBI, Jim Baker, now director of national security and cybersecurity at the R Street Institute, published a lengthy piece called "Rethinking Encryption." In that article, he advised the Justice Department and law enforcement to "embrace reality and deal with it" when it comes to encrypted communications.

Running counter to decades of sporadic pursuit by the Justice Department and law enforcement for a backdoor that would allow access to encrypted communications, Baker wrote that encryption "is one of the few mechanisms that the United States and its allies can use to more effectively protect themselves from existential cybersecurity threats, particularly from China. This is true even though encryption will impose costs on society, especially victims of other types of crime."

What triggered Baker to write the piece is a renewed push by the Justice Department under William Barr to warn that law enforcement is "going

dark." Barr said the rise of end-to-end communications encryption prevents the tracking of terrorists and predators as they carry out their misdeeds. Barr gave a speech on July 23, 2019, in which he called for "lawful access" to encrypted communications. He asked Silicon Valley to come up with technological solutions, warning that a significant incident would sooner or later "galvanize" public opinion against encryption.

In early October, the Justice Department sent a letter to Mark Zuckerberg asking Facebook not to proceed with its end-to-end encryption plans for its Messenger service after the United States agreed with the United Kingdom to allow the two countries' respective law enforcement agencies to demand electronic data regarding serious crimes. The next day, the Justice Department held what it called a Summit on Lawful Access, during which Barr and FBI Director Christopher Wray raised again the need for some encryption solutions that would give law enforcement access to secured communications.

Baker in his piece spelled out a number of reasons why he thinks the feds should just give up on the notion of encryption backdoors. He also wrote, "There is no law that clearly empowers governmental actors to obtain court orders to compel third parties (such as equipment manufacturers and service providers) to configure their systems to allow the government to obtain the plain text (i.e., decrypted) contents of, for example, an Android or iPhone or messages sent via iMessage or WhatsApp." Reported in: csoonline, November 4, 2019.

Las Vegas, Nevada

Is facial recognition technology accurate enough for the US Transportation Security Administration (TSA) to proceed with plans to use biometrics to identify 97 percent of travelers flying out of the country by 2022?

TSA will conduct a short-term "proof of concept" test in Las Vegas' McCarran International Airport to examine how effective facial recognition technology could be at automating travelers' identity verification, according to an August 2019 publication from the Department of Homeland Security (DHS).

For passengers who opt in, the agency will assess the technology's capability to verify travelers' live facial images taken at security checkpoints against the images on their identity documents.

"To participate, passengers will voluntarily choose to enter a lane dedicated to the proof of concept," TSA said.

Ultimately the agency plans to collect live photos of passengers' faces, photos from traveler documents, identification document issuance and expiration dates, travel dates, various types of identification documents, the organizations that issued their identification documents, and the years of passengers' births, as well as the gender or sex listed in the identification documents.

TSA plans to store the data on encrypted hard drives that it will remove daily and transfer to DHS Science and Technology Directorate personnel weekly. Biometric information cannot be recovered from the templates produced and the information will only be used for the purpose of the pilot, it said. The agency also plans to consult with the National Institutes for Standards and Technology during the assessment of the algorithm and to ensure that all methodologies meet industry standards.

"TSA envisions that facial recognition ultimately will deliver a significant increase in passenger throughput and improvement in security at the checkpoint," it said. "This proof of concept will help determine next steps for implementing further automation of the TDC process." Reported in: nextgov.com, August 27, 2019.

Redmond, Washington

Will California's data privacy law give people in other states more control over how their personal data is shared online?

Microsoft said on November 11, 2019, that it plans to follow the California Consumer Privacy Act (CCPA) throughout the United States.

The CCPA, seen as establishing the most stringent data privacy protections in the nation, allows people to request that data be deleted and gives them the opportunity to opt out of having their information sold to a third party. Passed in June 2018, the law went into effect on January 1, 2020.

"CCPA marks an important step toward providing people with more robust control over their data in the United States," Julie Brill, Microsoft's chief privacy officer, wrote in a blog post. "It also shows that we can make progress to strengthen privacy protections in this country at the state level even when Congress can't or won't act."

The European Union last year rolled out new privacy regulations for its citizens, called the General Data Privacy Regulation, but the United States doesn't have a similar law at the federal level. Reported in: cnet.com, November 11, 2019.

INTERNATIONAL

Hong Kong, China; Israel; United Kingdom

How do countries around the world balance citizens' wish for privacy with law enforcement monitoring of citizens' behavior?

The emergence of facial recognition technologies and the fast adoption of street cameras around the world has led to significant enhancement of surveillance and tracking strategies. An overview published on calcalist.com finds that more than sixty-four countries are using facial recognition technologies today, with China in the lead.

The Hong Kong government issued an order in September 2019 that prohibits demonstrators from wearing masks, so that law enforcement authorities can identify them. Demonstrators were also reported to have knocked down smart lamp posts across the city for fear the Chinese government was using the posts to spy on them. Deployed initially to track illegal waste disposal and traffic conditions, including through capturing license plates, the lampposts in Hong Kong have embedded sensors and cameras. As an alternative to masks, demonstrators have resorted to more creative ways, such as jamming the facial recognition cameras by shining laser lights onto the lens.

Non-democratic governments are not the only ones investing heavily in facial recognition technologies. Chinese tech company Huawei Technologies Co. Ltd.'s website lists quite a few European cities as clients among the company's customer success stories in implementing facial recognition technologies.

Most democratic states protect the right to demonstrate under their laws or constitution, based on the understanding that demonstrations allow people, who have no access to decision-makers, to voice their opinion and impact public policy and agenda.

In Israel, the freedom to demonstrate is an integral part of the freedom of speech, classified under Basic Law: Human Dignity and Liberty. The Israeli courts consider freedom of speech a supreme right since it constitutes a precondition for exercising other rights. Nonetheless, it is not unlimited. The right to demonstrate is protected only as long as people exercise it in peaceful ways and according to the instructions of law enforcement. When this is not the case, the police are authorized to take action to ensure the public order is maintained.

In the United Kingdom, the UK Supreme Court ruled that the use of facial recognition cameras for maintaining public order and detecting criminals is lawful under both the European Human Rights Convention and the General Data Protection Regulation (GDPR). (The ruling does not indicate whether Britain will obey the provisions of the GDPR after Brexit is fully implemented.) British police made sure the facial recognition cameras complied with the GDPR prior to implementing them. Among other measures, the British police held a privacy impact assessment and used the findings to design a framework for data collection, processing, and retention policies that would comply with the law.

Opponents of facial recognition technologies argue that use of the technology should be regulated, that the technology is being used disproportionately, and that other means to the same ends exist and have a lesser impact on privacy. They also stress that people are not giving their consent to be photographed and have no control over the biometric data the cameras collect. Worse still, research shows that some software programs base their matches on biased data, which may lead to false positives, in particular when it comes to people of color and women.

There are also concerns that the authorities might retain data and compile blacklists in a manner that infringes on human rights. Even more disturbing is the possibility of using artificial intelligence to combine facial recognition with personal data. While the use of biometric identification on millions of people may help track down a few suspects, thus ensuring the safety of many, it might also create a society that is under constant surveillance, raising grave concerns for democracy and the right to privacy.

Such concerns led California to prohibit the police from using facial recognition technology in the police officers' body cameras, at least for the next three years. Reported in: calcalist.com, October 11, 2019.

Luxembourg City, Luxembourg

Does the European Union's "right to be forgotten" apply to online personal information held in US databases if the US company does business in Europe?

On September 24, 2019, the Court of Justice of the European Union (CJEU) said there are limits on the geographical scope of the right to erasure under Europe's General Data Protection Regulation (GDPR). The court decided that a US-based search engine does not need to remove ("de-reference") search results displayed on all the search engine's global versions. According to the court, it suffices for search results to be deleted from the search engine's European or EU versions (i.e., EU domain name extensions, such as .eu, .fr or .de).

This decision comes in a long-running set of appeals of a case where the French Supervisory Authority on March 21, 2016, imposed a fine of €100,000 euros on Google for not de-referencing a website from its search results on all Google search engine versions. The search engine appealed the decision before the French courts, which led to a referral to the CJEU.

The CJEU decided that "there is no obligation under EU law, for a search engine operator . . . to carry out such a de-referencing on all the versions of its search engine."

The court pointed out that the search engine should use measures that "effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request." In this way, the CJEU addresses the concern that non-EU versions of the search engine may still be accessible in the EU through, for example, a VPN connection or other technologies that disguise the location of the search engine user. Search engines must make reasonable efforts to prevent access to de-referenced results, but are not held to guaranteeing that all searches will be blocked.

However, the court does not specifically comment on whether the use of techniques such as "geo-blocking" are sufficient, but instead the court provides that "it is for the referring court to ascertain whether . . . the measures adopted or proposed by Google meet those requirements."

The CJEU also highlighted that the right to erasure must be weighed against other rights (e.g., freedom of information). This potentially leads to different outcomes in different Member States. To avoid this outcome, however, the court provides that Supervisory Authorities should follow the cooperation procedure under the GDPR "to adopt, where appropriate, a de-referencing decision which covers all searches conducted from the territory of the Union on the basis of that data subject's name." In other words, French or other national authorities should not on their own require de-referencing of search results across all the search engine's EU versions.

Finally, the CJEU also clarified that EU law does *not prohibit* a Member State's Supervisory Authority or courts to order a search engine to de-reference search results from *all* its versions worldwide. Thus France (for example) could thus still decide that the relevant search results must be de-referenced on all versions of the search engine on the basis of French fundamental rights standards, but not on the basis of the GDPR. Reported in: *Inside Privacy,* September 25, 2019.

Moscow, Russia

Will the global internet, originally known as the World Wide Web, be broken into separate national webs as some countries try to control their citizens' access to information?

Over the past year, Russian lawmakers and Kremlin officials have discussed an internet that can be tightly controlled by the state—and potentially disconnected from the global net entirely. In October 2019, Russia planned a so-called disconnection test of the internet sometime in October—right ahead of November 1, when a new law about Russia's domestic internet took effect. Russia plans to repeat this test at least once a year.

In February 2019, a draft law was introduced in the Russian Parliament that aimed to give broader and deeper regulatory oversight of the internet to Roskomnadzor, the Russian internet regulator ("RuNet"). Since then, "equipment is being installed on the networks of major telecom operators," Alexander Zharov, head of Roskomnadzor, told reporters.

Tests will be carried out "carefully" in the first round, he said, in order to ensure that traffic and servers are not affected. Then, "combat mode" tests will be initiated. It's unclear what combat mode means, but presumably this is something closer (at least in theory) to total isolation of the RuNet, perhaps in response to an emergency.

The Russian government has also purportedly started rolling out deep packet inspection, a more sophisticated internet filtering technique.

"Testing a domestic internet," according to a "Future Tense" analysis published in *Slate*, "is not just another step in the pursuit of a practical goal—a controlled, isolatable domestic internet—it signifies the Russian government's commitment to technological sovereignty, especially from the West. . . . As it moves toward the capabilities for an internet disconnection test, this could mark a significant moment in the history of the network we once called truly global." Reported in: *Slate*, October 24, 2019.