SCHOOLS

Which is more valuable: student privacy, or possibly identifying students who may be thinking of harming themselves or others? New "internet safety policies" mean that for some of the 50 million-plus US students in kindergarten through grade 12 this school year, every word they type on a school computer will be tracked.

Under the Children's Internet Protection Act (CIPA), any US school that receives federal funding is required to have an internet-safety policy. For some, this simply means blocking inappropriate websites. Others, however, have turned to software companies like Gaggle, Securly, and GoGaurdian to surface potentially worrisome communications to school administrators.

These Safety Management Platforms (SMPs) use natural-language processing to scan through the millions of words typed on school computers. If a word or phrase might indicate bullying or self-harm behavior, it gets surfaced for a team of humans to review.

In an age of mass school shootings and increased student suicides, SMPs can play a vital role in preventing harm before it happens. Each of these companies has case studies where an intercepted message helped save lives. But the software also raises ethical concerns about the line between protecting students' safety and protecting their privacy.

"A good-faith effort to monitor students keeps raising the bar until you have a sort of surveillance state in the classroom," Girard Kelly, the director of privacy review at Common Sense Media, a non-profit that promotes internet-safety education for children, told *Quartz*. "Not only are there metal detectors and cameras in the schools, but now their learning objectives and emails are being tracked too."

The debate around SMPs sits at the intersection of two topics of national interest—protecting schools and protecting data. As more and more schools go "one-to-one" (the industry term for assigning every student a device of their own), the need to protect students' digital lives is only going to increase. Over 50 percent of teachers say their schools are one-to-one, according to a 2017 survey from Freckle Education, meaning there's a huge market for SMPs.

The most popular SMPs all work slightly differently. Gaggle, which charges roughly $5 per student annually, is a filter on top of popular tools like Google Docs and Gmail. When the Gaggle algorithm surfaces a word or phrase that may be of concern—such as a mention of drugs or signs of cyberbullying—the "incident" gets sent to human reviewers before being passed on to the school. Securly goes one step beyond classroom tools and gives schools the option to perform "sentiment analysis" on students' public social media posts. Using AI, the software is able to process thousands of student tweets, posts, and status updates to look for signs of harm.

Kelly thinks SMPs help normalize surveillance from a young age. In the wake of the Cambridge Analytics scandal at Facebook and other recent data breaches from companies like Equifax, we have the opportunity to teach kids the importance of protecting their online data, he said.

"There should be a whole gradation of how this [software] should work," Daphne Keller, the director of the Stanford Center for Internet and Society (and mother of two), told *Quartz*. "We should be able to choose something in between, that is a good balance [between safety and surveillance], rather than forcing kids to divulge all their data without any control."

To be sure, in an age of increased school violence, bullying, and depression, schools have an obligation to protect their students. But the protection of kids' personal information is also a matter of their safety. Securly CEO Vinay Mahadik agrees that privacy is an important concern, but believes companies like his can strike the right balance of freedom and supervision.

"Not everybody is happy because we are talking about monitoring kids," Mahadik told *Quartz*. "But as a whole, everyone agrees there has to be a solution for keeping them safe. That's the fine line we're walking."

Critics like Keller believe digital surveillance might have a chilling effect on students' freedom of expression. If students know they're being monitored, they might censor themselves from speaking their mind. This would, of course, only occur if the students knew they were being watched.

Though most school districts require parents to sign blanket consent agreements to use technology in the classroom, some districts believe they'll get a more representative picture of behavior if students aren't aware of the software, according to Patterson. In other words, some districts don't let the kids know they're being tracked.

"Parental consent can be a get-out-of-jail-free card for vendors," Bill Fitzgerald, a long-time school technology director, who now consults schools and non-profits on privacy issues, told *Quartz*. "When a parent consents to terms [to a variety of edtech tools] at the beginning of the school year, that's all the third-party really needs to operate."

SMPs market to parents' and school districts' biggest fears. "This might

be the only insight adults get to a student's suffering," Securly's website says, before quoting a director of IT in Michigan public schools: "Just one avoidance of a young person harming themselves or others would be worth a thousand times the subscription price."

Gaggle has gone even further. Not only do SMPs let schools monitor students, but the same software can be used to surveil teachers, it suggests. "Think about the recent teacher work stoppage in West Virginia," a recent blog post reads. "Could the story have been different if school leaders there requested search results for 'health insurance' or 'strike' months earlier? Occasional searches for 'salary' or 'layoffs' could stave off staff concerns that lead to adverse press for your school district."

(The company has since taken the post down. In an email, Patterson told *Quartz* that it was not in line with Gaggle's mission "to ensure the safety and well being of students and schools.")

Avoiding bad press and preventing teacher strikes have little to do with keeping students safe, but the implied message from the post is clear: Gaggle's clients are administrators, not the students or teachers.

The concern, however, is that students' protection is coming at the expense of their privacy. As kids spend more of their formative years online, they also need safe digital spaces to explore their own identities.

"Suppose you are a kid considering suicide and you want to write a diary about it or talk to your friend about the feelings that you're having, but you don't because you're afraid you'll be turned into your parent," Keller said. "I'm not sure that's a good outcome."

When we start monitoring kids' behavior from a young age, Keller believes, it can set a dangerous precedent. As adults reckon with issues of privacy and data protection, she believes kids must also learn what it means to give companies access to their personal information.

"I'm worried about how clearly my kid knows what he's agreed to when receiving that district provided device," Liz Kline, a California parent, told *Quartz*. "It's fine now when he's six, but what about when he's in high school and wants to organize a walk out?" Reported in: *Quartz*, August 19.

Blount County, Alabama

Does a new Alabama law that allows public facilities to display the "In God We Trust" motto violate the separation of church and state that is enshrined in the First Amendment's ban against government "establishment" of religion?

The Blount County school board started the 2018-19 school year as the first system planning to add "In God We Trust" displays under the Alabama law, according to Superintendent Rodney Green, who oversees a school system with more than 7,800 students spread out over 17 schools north of Jefferson County.

Government officials throughout Alabama could follow suit, and some were asking lawyers about the prospects of courtroom battles with organizations that advocate for the separation of church and state.

The *Washington Post* reports that seven states this year passed laws requiring or permitting schools and other public buildings to post "In God We Trust." Americans United for Separation of Church and State identifies six of the states in a September 13 blog post as Alabama, Arizona, Florida, Louisiana, North Carolina, and Tennessee. The *Washington Post* does not identify all the states in its seven-state total—only Florida.

In another move toward less separation of church and state, voters in Alabama overwhelmingly passed a ballot initiative in November that permits the Ten Commandments to be posted on government-funded property.

The Congressional Prayer Caucus Foundation is supporting laws that bring religion back to the schools with an initiative it calls Project Blitz, *Forbes* reported in September. The group has distributed a 116-page manual with bill templates, and the first is for laws authorizing the motto "In God We Trust" in public schools.

Backers hope such laws will be found constitutional by the new conservative majority on the US Supreme Court. Reported in: al.com, August 9; *Washington Post*, December 1; *ABA Journal*, December 5.

COLLEGES AND UNIVERSITIES

Davis and Los Angeles, California

Are university librarians protected by the same guarantees of academic freedom given to professors and other university faculty members?

Librarians from across the University of California system gathered at UCLA last month during contract talks. Their union is seeking explicit recognition of their academic freedom in a new contract. Administrators disagree.

The issue surfaced after Elaine Franco entitled her presentation at the American Library Association's midwinter meeting six years ago "Copy cataloging gets some respect from administrators."

An administrative colleague of Franco's at the University of California at Davis raised concerns about the title, an allusion to Rodney

Dangerfield's "I don't get no respect" catchphrase. When she saw the 2012 slide deck, which Franco had emailed her, the administrator wondered if the title inappropriately implied that copy catalogers had previously been disrespected by administrators, Franco recalled.

The disagreement caught the attention of a union negotiator. And now the episode has helped set off a crusade for academic freedom for employees of the 100-library University of California (UC) System, amid negotiations to replace a contract that was set to expire at the end of September.

Inspired in part by Franco's cautionary tale, the union sought to include a provision in the new contract clarifying that librarians have academic freedom. The union says negotiators for the system rejected the proposal, and librarians and academics nationwide have rallied to support the UC librarians.

The tussle is the latest example of a major research university's struggle to draw the bounds of academic freedom—who has it and under what circumstances. Lawyers representing the University of Texas at Austin argued this year that this core value of academe amounted to a workplace policy, not a First Amendment right. *[See "From the Bench," page 50.]*

And Carol L. Folt, the University of North Carolina at Chapel Hill's chancellor, affirmed her administration's commitment to academic freedom this summer, while disagreeing with a faculty group about the application of the principle.

Claire Doan, a spokeswoman, said UC policies on academic freedom "do not extend to nonfaculty academic personnel, including librarians," adding that the university's goal in the negotiations is to reach agreement on issues including competitive pay and health-care and retirement benefits for librarians. She said librarians play a "crucial" role at the university.

"The provision of academic freedom (or a derivative thereof) is a complex issue that has been rooted in faculty rights, professional standards, and obligations—and requires extensive examination and discussion," Doan wrote in a statement. "Historically, this is also the case at research universities where librarians are not faculty. We will continue negotiating with the University Council-American Federation of Teachers, endeavoring to better understand the union's stance on academic freedom and other pertinent issues."

Martin J. Brennan, a copyright librarian on the Los Angeles campus who is part of the University Council-AFT negotiating team, said he was surprised by what he characterized as the system negotiators' plain rejection of the union's request.

UC librarians never have had reason to doubt that they possessed academic freedom, and adding the statement, Brennan said, should have been just a formality.

A university policy on academic freedom includes guidance specifically for faculty members and students. But it says that the guidance "does nothing to diminish the rights and responsibilities enjoyed by other academic appointees," which Brennan said librarians had interpreted to mean that other university employees hold the right.

Union representatives proposed in late April a guarantee of academic freedom to all librarians so that they could fulfill responsibilities for teaching, scholarship, and research. The union represents about 350 people, more than 90 percent of whom are members of the union, Brennan said.

UC negotiators said in July that academic freedom was "not a good fit" for the librarians' unit, according to the union. They argued, the union said, that academic freedom is for instructors of record and students when they are in the classroom or conducting related research.

Administrators told the union that they would consider a different intellectual-freedom policy for librarians with a name other than "academic freedom," according to the union.

The librarians' crusade has drawn support in the form of a petition signed by about 650 people, including librarians and faculty members from Skidmore College, in New York, to the University of Oregon to the University of West Georgia. For a negotiating session, the union is handing out buttons that say, "Librarians will not be silent" and "Make some noise."

The chair of the American Association of University Professors' (AAUP) committee on academic freedom and tenure has also backed the UC librarians explicitly. Hank Reichman wrote for the AAUP's Academe blog that the UC negotiators "are wrong" to say their position aligns with the AAUP's.

The AAUP has previously said librarians and faculty members have the same professional concerns, calling academic freedom "indispensable" to librarians because they ensure the availability of information to teachers and students. Reported in: *Chronicle of Higher Education*, August 27.

Chapel Hill, North Carolina

Is a university faculty's academic freedom violated when administrators remove a controversial class from the course schedule?

At the University of North Carolina's Chapel Hill campus, faculty leaders have asked Chancellor Carol Folt and Provost Bob Blouin to affirm their commitment to academic freedom after they overturned a faculty grievance committee's decision in

favor of a professor whose sports history class faced administrative interference. In a letter to Blouin, Faculty Chair Leslie Parise said the Faculty Executive Committee had met twice in July to discuss the case of Jay Smith, a history professor whose "Big-Time College Sports and the Rights of Athletes" class explored, in part, the UNC athletic and academic scandal involving no-show classes. Smith's course was kept off the schedule for a time in 2017-18.

In a rare challenge to the administration, Parise asked Blouin and Folt to "publicly reaffirm their commitments to department autonomy, academic freedom, and the process of faculty governance." Parise said the rejection of last year's faculty grievance committee's finding created the concern that academic freedom had been compromised.

"We acknowledge administrators' responsibility to maintain oversight over curricula," Parise wrote. "But to be compatible with the university's commitment to academic freedom, this oversight must be fairly and consistently applied, leaving as many course scheduling decisions as possible to department-level leadership."

In a response posted July 19, Folt and Blouin wrote: "We are pleased to affirm our historic, steadfast commitment to academic freedom and faculty shared governance, and we value the robust and thorough process of faculty governance at this University. We know and appreciate the hard work of our faculty that has upheld and advanced this time-honored tradition."

But, they added that the Smith grievance outcome is a rare instance where the administration and the faculty disagree, adding, "academic freedom is not free from accountability, which we must enforce as leaders of this University."

In a break at a trustee meeting on July 19, Folt called faculty governance "the critical bedrock of a university" and said the administration supports faculty recommendations "nine times out of ten."

However, she added, the university also has rules and regulations from governing boards and accrediting committees and must abide by them. If the faculty is "asking us to provide complete autonomy to any department to do anything that it wants, we will not and cannot state that without violating those policies."

At issue in the grievance was whether the administration meddled in the scheduling of the course taught by Smith, a frequent critic of UNC's handling of the athletic scandal. UNC emails published by the *Raleigh News and Observer* last year showed that history department administrators worried about "blowback" and "a fight on our hands" if Smith's course was offered in 2017-18. It was kept off the schedule.

Forty-five history faculty members signed a statement last year calling scheduling interference "a serious infringement of freedom of inquiry." The professors said their chairman felt concerned about adverse consequences for the history department if the course were offered. Officials in the dean's office denied interfering in the schedule because of the course's content.

A faculty grievance committee reviewed the case and determined that Smith's class was not scheduled because of pressure from administrators; the panel also recommended that UNC officials not interfere in individual courses or threaten a department with financial consequences.

The course was first taught in 2016. University officials had argued that Smith's grievance was moot because his course was eventually offered again in the spring of 2018. Reported in: *Raleigh News & Observer*, July 19.

FREEDOM OF THE PRESS
Trenton, New Jersey

If local news outlets are struggling, is it the government's job to support them? In New Jersey, the answer is "yes."

New Jersey Governor Phil Murphy, a Democrat, approved a line in the state budget that dedicates $5 million to strengthen local media outlets in New Jersey. The state legislature passed the "Civic Info Bill" in late June, according to news website NJ.com.

The bill created the Civic Information Consortium—a unique nonprofit developed with five universities—to promote the spread of news and information throughout the state. The bill was conceived by the Free Press Action Fund, an advocacy group on media issues.

The consortium will share the $5 million with local news organizations, emphasizing "underserved communities, low-income communities and communities of color," the Free Press Action Fund said. The effort is led by the College of New Jersey, Montclair State University, the New Jersey Institute of Technology, Rowan University, and Rutgers University.

The money was included in the fiscal 2019 budget. Murphy signed the budget into law on July 1. Reported in: NJ.com, June 29; *The Hill*, July 2.

PRIVACY
Cupertino, California

Should smart phones users rely on technology to keep their data private—or should law enforcement be able to unlock the phones without the user's password?

In June, Apple said it is closing a technological loophole that had let authorities hack into iPhones,

angering police and other officials, and reigniting a debate over whether the government has a right to get into the personal devices that are at the center of modern life. *[For a related article involving law enforcement's access into Facebook accounts, see "From the Bench," page 61.]*

Apple, selling its iPhone as a secure device that only its owner can open, battled with the FBI in 2016 after Apple refused to help open the locked iPhone of a mass killer. The FBI eventually paid a third party to get into the phone, circumventing the need for Apple's help. Since then, law enforcement agencies across the country have increasingly employed that strategy to get into locked iPhones they hope will hold the key to cracking cases.

Apple said it was planning an iPhone software update that would effectively disable the phone's charging and data port—the opening where users plug in headphones, power cables and adapters—an hour after the phone is locked. While a phone can still be charged, a person would first need to enter the phone's password to transfer data to or from the device using the port.

Such a change would hinder law enforcement officials, who have typically been opening locked iPhones by connecting another device running special software to the port, often days or even months after the smartphone was last unlocked. News of Apple's planned software update has begun spreading through security blogs and law enforcement circles—and many in investigative agencies are infuriated.

"If we go back to the situation where we again don't have access, now we know directly all the evidence we've lost and all the kids we can't put into a position of safety," said Chuck Cohen, who leads an Indiana State Police task force on internet crimes against children. The Indiana State Police said it unlocked 96 iPhones for various cases this year, each time with a warrant, using a $15,000 device it bought in March from a company called Grayshift.

But privacy advocates said Apple would be right to fix a security flaw that has become easier and cheaper to exploit. "This is a really big vulnerability in Apple's phones," said Matthew D. Green, a professor of cryptography at Johns Hopkins University. A Grayshift device sitting on a desk at a police station, he said, "could very easily leak out into the world."

In an email, an Apple spokesman, Fred Sainz, said the company is constantly strengthening security protections and fixes any vulnerability it finds in its phones, partly because criminals could also exploit the same flaws that law enforcement agencies use. "We have the greatest respect for law enforcement, and we don't design our security improvements to frustrate their efforts to do their jobs," he said.

Apple and Google, which make the software in nearly all of the world's smartphones, began encrypting their mobile software by default in 2014. Encryption scrambles data to make it unreadable until accessed with a special key, often a password. That frustrated police and prosecutors who could not pull data from smartphones, even with a warrant.

The friction came into public view after the FBI could not access the iPhone of a gunman who, along with his wife, killed 14 people in San Bernardino, Calif., in late 2015. A federal judge ordered Apple to figure out how to open the phone, prompting Timothy D. Cook, Apple's chief executive, to respond with a blistering 1,100-word letter that said the company refused to compromise its users' privacy. "The implications of the government's demands are chilling," he wrote.

The two sides fought in court for a month. Then the FBI abruptly announced that it had found an undisclosed group to get into the phone, paying at least $1.3 million because the hacking techniques were not common then. An inspector general's report this year suggested the FBI should have exhausted more options before it took Apple to court.

The encryption on smartphones applies only to data stored solely on the phone. Companies like Apple and Google regularly give law enforcement officials access to the data that consumers back up on their servers, such as via Apple's iCloud service. Apple said that since 2013, it has responded to more than 55,000 requests from the United States government seeking information about more than 208,000 devices, accounts, or financial identifiers.

The tussle over encrypted iPhones and opening them to help law enforcement is unlikely to simmer down. Federal officials have renewed a push for legislation that would require tech companies like Apple to provide the police with a backdoor into phones, though they were recently found to be overstating the number of devices they could not access.

Apple probably won't make it any easier for the police if not forced by Congress, given that it has made the privacy and security of iPhones a central selling point. But the company has complied with local laws that conflict with its privacy push. In China, for instance, Apple recently began storing its Chinese customers' data on Chinese-run servers because of a new law there. Reported in: *New York Times*, June 13.

Northridge, California; Armonk, New York; New York City, New York

Are police departments using video cameras and facial recognition software for racial profiling and discriminatory enforcement?

Using video footage from New York City Police Department (NYPD) surveillance cameras, IBM has developed facial recognition software that could search for people based on skin tone and ethnicity. The NYPD says it is not using the new video analytics, but at least one police force—the campus police department at California State University, Northridge, has adopted it.

Civil liberties advocates say they are alarmed by the NYPD's secrecy in helping to develop a program with the potential capacity for mass racial profiling.

The identification technology IBM built could be easily misused after a major terrorist attack, argued Rachel Levinson-Waldman, senior counsel in the Brennan Center's Liberty and National Security Program. "Whether or not the perpetrator is Muslim, the presumption is often that he or she is," she said. "It's easy to imagine law enforcement jumping to a conclusion about the ethnic and religious identity of a suspect, hastily going to the database of stored videos and combing through it for anyone who meets that physical description, and then calling people in for questioning on that basis."

IBM, headquartered in Armonk, New York, did not comment on questions about the potential use of its software for racial profiling. However, the company did send a comment to *The Intercept* pointing out that it was "one of the first companies anywhere to adopt a set of principles for trust and transparency for new technologies, including artificial intelligence (AI) systems." The statement continued on to explain that IBM is "making publicly available to other companies a dataset of annotations for more than a million images to help solve one of the biggest issues in facial analysis—the lack of diverse data to train AI systems."

Few laws clearly govern object recognition or the other forms of artificial intelligence incorporated into video surveillance, according to Clare Garvie, a law fellow at Georgetown Law's Center on Privacy and Technology. "Any form of real-time location tracking may raise a Fourth Amendment inquiry," Garvie said, citing a 2012 Supreme Court case, *United States v. Jones*, that involved police monitoring a car's path without a warrant and resulted in five justices suggesting that individuals could have a reasonable expectation of privacy in their public movements. In addition, she said, any form of "identity-based surveillance" may compromise people's right to anonymous public speech and association.

Garvie noted that while facial recognition technology has been heavily criticized for the risk of false matches, that risk is even higher for an analytics system "tracking a person by other characteristics, like the color of their clothing and their height," that are not unique characteristics.

The story began after the 9/11 attacks in 2001, when the New York City Police Department created a plan to cover Manhattan's downtown streets with thousands of cameras. The department hoped that video analytics would improve analysts' ability to identify suspicious objects and persons in real time in sensitive areas, according to Conor McCourt, a retired NYPD counterterrorism sergeant who said he used IBM's program in its initial stages.

The video analytics software captured stills of individuals caught on closed-circuit TV footage and automatically labeled the images with physical tags, such as clothing color, allowing police to quickly search through hours of video for images of individuals matching a description of interest. The software could also generate alerts for unattended packages, cars speeding up a street in the wrong direction, or people entering restricted areas.

IBM began developing this object identification technology using secret access to NYPD camera footage. *The Intercept* and the Investigative Fund have learned from confidential IBM corporate documents and interviews with many of the technologists involved in developing the software, that NYPD officials gave IBM access to images of thousands of unknowing New Yorkers as early as 2012, as IBM was creating new search features that allow other police departments to search camera footage for images of people by hair color, facial hair, and skin tone.

IBM declined to comment on its use of NYPD footage to develop the software. However, in an email response to questions, the NYPD did tell *The Intercept* that "Video, from time to time, was provided to IBM to ensure that the product they were developing would work in the crowded urban NYC environment and help us protect the City. There is nothing in the NYPD's agreement with IBM that prohibits sharing data with IBM for system development purposes. Further, all vendors who enter into contractual agreements with the NYPD have the absolute requirement to keep all data furnished by the NYPD confidential during the term of the agreement, after the completion of the agreement, and

in the event that the agreement is terminated."

In an email to *The Intercept*, the NYPD confirmed that select counterterrorism officials had access to a pre-released version of IBM's program, which included skin tone search capabilities, as early as the summer of 2012. NYPD spokesperson Peter Donald said the search characteristics were only used for evaluation purposes and that officers were instructed not to include the skin tone search feature in their assessment. The department eventually decided not to integrate the analytics program into its larger surveillance architecture and phased out the IBM program in 2016.

After testing out these bodily search features with the NYPD, IBM released some of these capabilities in a 2013 product release. Later versions of IBM's software retained and expanded these bodily search capabilities. IBM did not respond to a question about the current availability of its video analytics programs.

According to the NYPD, counterterrorism personnel accessed IBM's bodily search feature capabilities only for evaluation purposes, and they were accessible only to a handful of counterterrorism personnel. "While tools that featured either racial or skin tone search capabilities were offered to the NYPD, they were explicitly declined by the NYPD," Donald, the NYPD spokesperson, said. "Where such tools came with a test version of the product, the testers were instructed only to test other features (clothing, eyeglasses, etc.), but not to test or use the skin tone feature. That is not because there would have been anything illegal or even improper about testing or using these tools to search in the area of a crime for an image of a suspect that matched a description given by a victim or a witness. It was specifically to avoid even the suggestion or appearance of any kind of technological racial profiling." The NYPD ended its use of IBM's video analytics program in 2016, Donald said.

Kjeldsen, the former IBM researcher who helped develop the company's skin tone analytics with NYPD camera access, said the department's claim that the NYPD simply tested and rejected the bodily search features was misleading. "We would have not explored it had the NYPD told us, 'We don't want to do that,'" he said. "No company is going to spend money where there's not customer interest."

Kjeldsen also added that the NYPD's decision to allow IBM access to their cameras was crucial for the development of the skin tone search features, noting that during that period, New York City served as the company's "primary testing area," providing the company with considerable environmental diversity for software refinement.

"The more different situations you can use to develop your software, the better it's going be," Kjeldsen said. "That obviously pertains to people, skin tones, whatever it is you might be able to classify individuals as, and it also goes for clothing."

The NYPD's cooperation with IBM has since served as a selling point for the product at California State University, Northridge. There, campus police chief Anne Glavin said the technology firm IXP helped sell her on IBM's object identification product by citing the NYPD's work with the company. "They talked about what it's done for New York City. IBM was very much behind that, so this was obviously of great interest to us," Glavin said.

Campus police at California State University, Northridge, who adopted IBM's software, said the bodily search features have been helpful in criminal investigations. Asked about whether officers have deployed the software's ability to filter through footage for suspects' clothing color, hair color, and skin tone, Captain Scott VanScoy at California State University, Northridge, responded affirmatively, relaying a story about how university detectives were able to use such features to quickly filter through their cameras and find two suspects in a sexual assault case.

"We were able to pick up where they were at different locations from earlier that evening and put a story together, so it saves us a ton of time," Vanscoy said. "By the time we did the interviews, we already knew the story and they didn't know we had known."

Glavin, the chief of the campus police, added that surveillance cameras using IBM's software had been placed strategically across the campus to capture potential security threats, such as car robberies or student protests. "So we mapped out some CCTV in that area and a path of travel to our main administration building, which is sometimes where people will walk to make their concerns known and they like to stand outside that building," Glavin said. "Not that we're a big protest campus, we're certainly not a Berkeley, but it made sense to start to build the exterior camera system there." Reported in: *The Intercept*, September 6.

Sacramento, California

Will technology companies that use people's personal data be able to defang a California law that was designed to protect Californians' privacy?

In June, privacy advocates celebrated the passage of a bill in California that gave residents of that state unprecedented control over how companies use their data. Lobbying groups

and trade associations, including several representing the tech industry, immediately started pushing for a litany of deep changes that they say would make the law easier to implement before it goes into effect in January 2020. Privacy advocates worry that pressure from powerful businesses could end up gutting the law completely.

"This is their job: to try to make this thing absolutely meaningless. Our job is to say no," said Alastair MacTaggart, chair of the group Californians for Consumer Privacy, which sponsored a ballot initiative that would have circumvented the legislature and put the California Consumer Privacy Act to a vote in November. Big Tech and other industries lobbied fiercely against the initiative. In June, MacTaggart withdrew it once the bill, known as AB 375, passed.

At the most basic level, the law allows California residents to see what data companies collect on them, request that it be deleted, know what companies their data has been sold to, and direct businesses to stop selling that information to third parties. But the task of shaping the specifics is now in the hands of lawmakers—and the special interests they cater to.

"The new sheriffs showed up and drew a gun. Then they put it down and walked away," Kevin Baker, legislative director of the American Civil Liberties Union in California, says, referring to MacTaggart's initiative. "Now that they've done that, and the initiative threat has gone away, we're back to politics as usual."

In early August, a coalition of nearly 40 organizations, ranging from the banking industry to the film industry to the tech industry's leading lobbying groups, sent a 20-page letter to lawmakers, effectively a wish list of changes—a clear sign of the battle in store for 2019.

Among the most significant proposed changes was a reframing of who the law considers a "consumer." The bill as written applies to all California residents, a provision that industry groups wrote would be "unworkable and have numerous unintended consequences." Instead, trade groups want the law only to apply to people whose data was collected because they made a purchase from a business or used that business's service. They also propose making it so that only businesses had the right to identify people as consumers, and not the other way around.

Such a change might seem small, but it would substantially narrow the law's scope, says Mary Stone Ross, who helped draft the ballot initiative as the former president of Californians for Consumer Privacy. "This is significant because it [would] not apply to information that a business does not obtain directly from the consumer," Ross says, like data sold by data brokers or other third parties.

Another major change sought to tweak disclosure requirements. Whereas the original bill requires companies to share specific pieces of data, the industry groups prefer to draw the line at "categories of personal information."

There are other, subtler suggested changes, too, that Ross says would have sweeping implications. The law includes language that would prevent a business from discriminating against people by, say, charging them inordinate fees if they opt out of data collection. But prohibiting blanket discrimination is too broad for the business groups, who want to add a caveat specifying that they may not "unreasonably" discriminate. In another section, which discusses offering consumers incentives for the sale of their data, the industry groups also proposed striking the words "unjust" and "unreasonable" from a line that reads, "A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature."

On August 28, during an Assembly hearing on the bill, the final sticking point, particularly for the tech giants, was the law's handling of data collected for the purposes of advertising. While the law prohibits users from opting out of advertising altogether, it does allow them to opt out of the sale of their personal information to a third party. But the industry wanted to create an exception for information that's sold for the purposes of targeted advertising, where the users' identities aren't disclosed to that third party. Privacy groups including the ACLU and Electronic Freedom Frontier vehemently opposed the proposal, as did MacTaggart. They argued that such a carve-out would create too big of a loophole for businesses and undermine consumers' right to truly know everything businesses had collected on them.

As of August 28, the industry groups failed to get that amendment into the bill. But MacTaggart and others expect to fight this battle all over again next year.

It's not that the privacy bill is perfect. The ACLU, for one, criticized the bill's exclusion of a provision in the ballot initiative that would have given people the right to sue companies for violating their data privacy rights. It instead leaves enforcement up to the attorney general, except in the case of a data breach.

As the bill was being finalized, all sides did agree to some tweaks, like clarifying language that would protect data collected through clinical trials and other health-related information. Another change ensures that information collected by journalists remains safeguarded.

"One of the reasons why AB 375 passed unanimously is everyone knew there'd be a cleanup bill, and they had plenty of time to lobby to get their changes through," said Ross, who opposed pulling the ballot initiative in June.

Some engaged citizen, of course, could always mount another bid for a ballot initiative, but with the 2018 deadline already passed, that couldn't happen until at least 2020, and it would take millions more dollars to put up another fight. That has left activists like Ross and MacTaggart relatively powerless in the very battle they began. Reported in: wired.com, August 29.

Washington, DC

How much personal information does the US Department of Homeland Security (DHS) really collect? DHS is quietly building what will likely become the largest database of biometric and biographic data on citizens and foreigners in the United States.

The agency's new Homeland Advanced Recognition Technology (HART) database will include multiple forms of biometrics—from facial recognition to DNA, and could sweep in data from questionable sources and highly personal data on innocent people. It will be shared with federal agencies outside of DHS as well as state and local law enforcement and foreign governments. Yet, the public still knows very little about it.

Privacy advocates warn that the records DHS plans to include in HART can chill and deter people from exercising their First Amendment protected rights to speak, assemble, and associate. Face recognition makes it possible to identify and track people in real time, including at lawful political protests and other gatherings. Other data DHS is planning to collect—including information about people's "relationship patterns" and from officer "encounters" with the public—can be used to identify political affiliations, religious activities, and familial and friendly relationships. Such data points can be colored by conjecture and bias.

In late May, Electronic Frontier Foundation (EFF) filed comments criticizing DHS's plans to collect, store, and share biometric and biographic records it receives from external agencies and to exempt this information from the federal Privacy Act. These newly-designated "External Biometric Records" (EBRs) will be integral to DHS's bigger plans to build out HART. EFF told the agency in its comments that DHS must do more to minimize the threats to privacy and civil liberties posed by this vast new trove of highly sensitive personal data.

DHS currently collects a lot of data. Its legacy IDENT fingerprint database contains information on 220 million unique individuals and processes 350,000 fingerprint transactions every day. This is an exponential increase from 20 years ago when IDENT only contained information on 1.8 million people. Between IDENT and other DHS-managed databases, the agency manages over 10 billion biographic records and adds 10-15 million more each week.

DHS's new HART database will allow the agency to vastly expand the types of records it can collect and store. HART will support at least seven types of biometric identifiers, including face and voice data, DNA, scars and tattoos, and a blanket category for "other modalities." It will also include biographic information, such as name, date of birth, physical descriptors, country of origin, and government ID numbers. And it will include data we know to be highly subjective, including information collected from officer "encounters" with the public and information about people's "relationship patterns."

EFF warns that DHS's face recognition roll-out is especially likely to chill speech and deter people from associating with others. The agency uses mobile biometric devices that can identify faces and capture face data in the field, allowing its ICE (immigration) and CBP (customs) officers to scan everyone with whom they come into contact, whether or not those people are suspected of any criminal activity or an immigration violation. DHS is also partnering with airlines and other third parties to collect face images from travelers entering and leaving the United States. When combined with data from other government agencies, EFF said, these "troubling" collection practices will allow DHS to build a database large enough to identify and track all people in public places, without their knowledge—not just in places the agency oversees, like airports, but anywhere there are cameras.

Police abuse of facial recognition technology is not a theoretical issue: it's happening today. Law enforcement has already used face recognition on public streets and at political protests. During the protests surrounding the death of Freddie Gray in 2015, Baltimore Police ran social media photos against a face recognition database to identify protesters and arrest them. Recent Amazon promotional videos encourage police agencies to acquire that company's face "Rekognition" capabilities and use them with body cameras and smart cameras to track people throughout cities. At least two US localities (Orlando, Florida, and Washington County in Oregon) are already using Rekognition, according to records obtained by the American Civil Liberties Union of Northern California.

EFF charges that DHS is not taking necessary steps with its new HART database to determine whether its own data and the data collected from its external partners are sufficiently accurate to prevent innocent people from being identified as criminal suspects, immigration law violators, or terrorists. Face recognition, in particular, frequently is an inaccurate and unreliable biometric identifier. DHS's tests of its own systems found significantly high levels of inaccuracy—the systems falsely rejected as many as 1 in 25 travelers.

People of color and immigrants will shoulder much more of the burden of these misidentifications. For example, people of color are disproportionately represented in criminal and immigration databases, due to the unfair legacy of discrimination in our criminal justice and immigration systems. Moreover, FBI and MIT research has shown that current face recognition systems misidentify people of color and women at higher rates than whites and men, and the number of mistaken IDs increases for people with darker skin tones. False positives represent real people who may erroneously become suspects in a law enforcement or immigration investigation.

DHS believes it's legally authorized to collect and retain face data from millions of US citizens traveling internationally. However, as Georgetown's Center on Privacy and Technology notes, Congress has never authorized face scans of American citizens. Reported in: aclunc.org, May 22; eff.org. June 7.

Washington, DC

For travelers, is the convenience boarding a plane quickly—with no boarding pass, paper ticket, or airline phone app—worth the loss of privacy that comes with facial recognition technology on international flights?

With the new Traveler Verification Service, passengers get their photo taken, and their face becomes their boarding pass.

"I would find it super convenient if I could use my face at the gate," said Jonathan Frankle, an artificial intelligence researcher at Massachusetts Institute of Technology studying facial recognition technology. But "the concern is, what else could that data be used for?"

The problem confronting Frankle, as well as thousands of travelers, is that few companies participating in the program give explicit guarantees that passengers' facial recognition data will be protected.

And even though the program is run by the Department of Homeland Security, federal officials say they have placed no limits on how participating companies—mostly airlines but also cruise lines—can use that data or store it, opening up travelers' most personal information to potential misuse and abuse such as being sold or used to track passengers' whereabouts.

The data the airlines collect is used to verify the identity of passengers leaving the country, an attempt by the department to better track foreigners who overstay their visas. After passengers' faces are scanned at the gate, the scan is sent to Customs and Border Protection (CBP) and linked with other personally identifying data, such as date of birth and passport and flight information.

For its part, Customs and Border Protection has said it will retain facial scans of American citizens for no longer than 14 days. But the agency has said it cannot control how the companies use the data because they "are not collecting photographs on CBP's behalf."

John Wagner, the deputy executive assistant commissioner for the agency's Office of Field Operations, said he believed that commercial carriers had "no interest in keeping or retaining" the biometric data they collect, and the airlines have said they are not doing so. But if they did, he said, "that would really be up to them."

But, Wagner added, "there are still some discussions to be had," and federal officials are considering whether they should write in protections.

Privacy advocates have criticized the agency for allowing airlines to act as unregulated arbiters of the data.

"CBP is a federal agency. It has a responsibility to protect Americans' data, and by encouraging airlines to collect this data, instead they are essentially abdicating their own responsibility," said Jennifer Lynch, a senior staff attorney with the Electronic Frontier Foundation, a digital rights nonprofit. Reported in: *New York Times*, August 6.

Chicago, Illinois

Should the 2020 US Census—required by the US Constitution to count all residents of the United States—ask whether residents are US citizens? Is the question an intrusion on residents' privacy?

The American Library Association (ALA) has joined 144 groups in opposing the addition of a citizenship question to the 2020 Census form. ALA is a signee of a letter submitted August 1 by the Leadership Conference on Civil and Human Rights to the Department of Commerce, which oversees the US Census Bureau.

The comments submitted by the coalition elaborate on the harm that would result from adding such a question to the 2020 Census, including diminished data accuracy, an increased burden of information collection, and an added cost to taxpayers. The submission also points to the US Census Bureau's own January 19 technical review, in which Associate

Director for Research and Methodology John Abowd concluded that adding a citizenship question would have an "adverse impact on self-response and, as a result, on the accuracy and quality of the 2020 Census."

The technical review also stated that using existing administrative records instead of asking a citizenship question would provide more accurate citizenship data at lower cost to the federal government.

"Adding a citizenship question to the 2020 Census would suppress Census response, distorting the statistics and making them less informative," said ALA President Loida Garcia-Febo.

ALA has participated in previous coalition efforts to prevent the Trump administration's addition of a citizenship question to the 2020 Census, including a January 10 letter opposing the proposal. The Association is engaging with the US Census Bureau and other stakeholders to keep libraries informed of and represented in the 2020 Census policy discussions and planning process, with the goal that libraries may be better able to support their communities.

The US Census is a count of all US residents, required once every ten years by the Constitution, to determine Congressional representation; district boundaries for federal, state, and local offices; and allocation of billions of dollars in federal funding to states and localities, such as grants under the Library Services and Technology Act. Libraries across the US provide access to the wealth of statistical data published by the US Census Bureau and help businesses, government agencies, community organizations, and researchers find and use the information. Reported in: *American Libraries*, August 9.

Fort Meade, Maryland

Will technical difficulties keep the US federal government from storing the records of millions of calls made since 2015?

The National Security Agency (NSA) has announced a startling failure in the implementation of the USA Freedom Act of 2015. According to a public statement released by NSA on June 28, the call detail records (CDR) that NSA has been receiving from telephone companies under the Act are infected with errors, NSA cannot isolate and correct those errors, and so it has decided to purge from its data repositories all of the CDRs ever received under the Act. As the public statement explains, "on May 23, 2018, NSA began deleting all call detail records (CDRs) acquired since 2015 under Title V of the Foreign Intelligence Surveillance Act (FISA) . . . because several months ago NSA analysts noted technical irregularities in some data received from telecommunications service providers. These irregularities also resulted in the production to NSA of some CDRs that NSA was not authorized to receive. Because it was infeasible to identify and isolate properly produced data, NSA concluded that it should not use any of the CDRs."

Writing in the Lawfare blog, David Kris, a lawyer specializing in national security issues, explained that the problem arose after the USA Freedom Act changed the rules for the NSA's surveillance of phone calls: "The USA Freedom Act ended the bulk collection of telephony metadata and replaced it with a new procedure under which NSA sent queries to the telephone companies and received from them the responsive information. . . . This was the key privacy-enhancing feature of the USA Freedom Act—it radically reduced the raw amount of metadata held by the government."

After giving details about the NSA's new process, Kris concluded, "Somewhere in there, we now know, something went wrong. All of the data obtained by NSA under the Act are useless and will be destroyed. There is some problem that apparently infects at least some of the data—presumably in the form of inaccurate connections between telephone numbers—as well as some overproduction of data, and NSA cannot distinguish the good data from the bad."

Kris then asks, "What are the lessons here?" His answer:

> The obvious one is probably that Murphy's Law remains in force. And that law is particularly powerful as applied to large, complex systems. Sometimes, these systems generate mistakes that threaten privacy. Sometimes they generate mistakes that threaten security. The more complex the system—legally or technologically—the more likely that it will yield errors of both types.
>
> The USA Freedom Act created a more complex legal system requiring a more complex technological system governing collection of telephony metadata. This system failed. The failure has been discovered and apparently remediated. But I am left wondering whether another error could arise, whether the system is too complex to be sustainable, and therefore whether the juice is worth the squeeze. . . . We should know the answer to that question soon: under Section 705 of the USA Freedom Act, the CDR process is scheduled to sunset, unless renewed, at the end of 2019, and it will be very interesting to see whether the executive branch even seeks renewal.

Reported in: Lawfare, July 2.

Columbus, Ohio

Do parents have a right to know when their children question their sexual identity, or should children be able to keep such concerns private?

Ohio House Bill 658 would require government entities, including schools, courts, and hospitals, to "immediately" notify parents if a child displays signs of gender dysphoria or "demonstrates a desire to be treated in a manner opposite of the child's biological sex," according to the proposal.

Introduced by Republican Representatives Tom Brinkman and Paul Zeltwanger, the bill also gives parents the right to "withhold consent for gender dysphoria treatment or activities that are designed and intended to form a child's conception of sex and gender."

Opponents say that if it becomes law, the initiative could endanger children's lives.

"In targeting transgender children, the bill authors create ridiculous and unenforceable requirements––requirements that out transgender students and create a significant threat of bullying and reduced access to social support systems," LGBTQ advocacy group Equality Ohio said in a statement. "This unnecessary and discriminatory bill does nothing to support youth and families. In fact, it puts the livelihoods of some of our most vulnerable youth—transgender youth—further at risk with bullying and discrimination by potentially forcing teachers to out them."

If House Bill 658 were to become law, Ohio would have to "deputize its state employees to be gender cops," the organization said, calling the provision "dangerous for Ohio families."

Other transgender advocacy groups have also pushed back against the bill, including some who said it could be harmful to transgender children who don't feel safe at home. Nearly 37 percent of transgender people attempt suicide before the age of 24 and those who feel rejected at home or school are even more likely, according to data from the National Center for Transgender Equality.

House Bill 658 received its first hearing from the House's Community and Family Advancement committee on June 20, pushing it one step closer to a possible vote in the state's general assembly. Reported in: ABC News, June 28.

3-D PRINTING

Seattle, Washington

Now that three-dimensional printers can produce working guns, should publication of the 3-D printing instructions for guns be banned as a threat to public safety? Or is such publication protected as form of free speech?

Amazon has removed a book that reproduced code for 3-D printed guns from its bookstore, saying the content violated its guidelines. A legal battle continues over whether the programming code for printed guns will be permitted or banned. *[See "From the Bench," page 66.]*

Amazon reprinted the code for Defense Distributed's plastic gun, called the Liberator, in a 584-page book, called *The Liberator Code Book: An Exercise in Freedom of Speech*. Defense Distributed is an Austin, Texas-based non-profit that researches and designs 3-D-printable weapons.

"This is a printed copy of step files for the Liberator, and not much else," wrote someone named "CJ Awelow," who claimed to be the author, in a brief description on Amazon before the book was removed. "Code is speech," Awelow wrote, echoing the legal argument made by Defense Distributed. "Proceeds will be used to fight for free speech and the right to bear arms."

In an email, Amazon confirmed it had removed the book for "violating our content guidelines." Amazon declined to comment on how many copies of the book had been sold.

Blueprints for 3-D-printed guns have stirred controversy this summer after the government settled with Defense Distributed, allowing the non-profit to distribute its plans online for free. The distribution was halted, however, after 19 state attorneys general filed a lawsuit that prompted a Seattle judge to issue a temporary restraining order in July.

Defense Distributed used Amazon's removal of the book to champion its cause, tweeting: "Sadly the book has been taken off of Amazons webstore. This is one [*sic*] again a huge blow to our first amendment. If you want change, act now.—Defense Distributed (@DefDist) 7:40 pm, August 22."

Someone claiming to be Awelow posted to Reddit's r/Firearms channel and said the book had been a bestseller in Amazon's Computer and Technology Education section since its publication.

The post also included the address of a website that hosts the 3-D-printed gun plans. CNET downloaded files from the site which appeared to be authentic.

In court, more than a dozen states argue the publication of code to produce downloadable, 3-D-printable weapons is a public safety risk. The states argue the plastic guns, which are without serial numbers and therefore untraceable, would skirt various gun regulations. But Defense Distributed and its supporters argue that blocking the computer code for the weapons amounts to a First Amendment violation—whether that code

is published on the internet or, for example, in a book on Amazon.

The states are seeking a permanent injunction. Reported in: cnet.com, August 23; *Washington Post*, August 23.

INTERNATIONAL

Strasbourg, France

Will the flow of information on the internet be stifled by new copyright legislation in Europe?

The European Parliament on September 12 approved a package of dramatic changes to copyright law, with big implications for the future of the internet. *[In a related article, European "Right to be Forgotten" legislation can also affect the international flow of information on the internet, and is under review by the European Court of Justice—see "From the Bench," page 69.]*

The European Union's new copyright directive is an update to a 2001 directive on copyright, and is aimed at modernizing rules for the digital age. It is part of the EU's "digital single market," a strategy aimed at setting a common standard for online services and businesses.

If it goes into effect, the legislation would make online platforms such as Google and Facebook directly liable for content uploaded by their users, and would mandate greater "cooperation" with copyright holders to police the uploading of infringing works. It would also give news publishers a new, special right to restrict how their stories are featured by news aggregators such as Google News. And it would create a new right for sports teams that could limit the ability of fans to share images and videos online.

The vote is not the end of Europe's copyright fight. Under the European Union's convoluted process for approving legislation, the proposal will now become the subject of a three-way negotiation involving the European Parliament, the Council of the Europe Union (representing national governments), and the European Commission (the EU's executive branch). If those three bodies agree to a final directive, then it will be sent to each of the 28 EU member countries (or likely 27 after Brexit) for implementation in national laws.

"We're enormously disappointed that MEPs [Members of European Parliament] failed to listen to the concerns of their constituents and the wider internet," said Danny O'Brien, an analyst at the Electronic Frontier Foundation.

One concern is that online providers will become so worried about liability for infringement that they will start taking down a lot of legitimate content—for example, content that parodies a copyrighted work or otherwise exercises the European equivalents of fair use rights. To deal with this danger, the directive mandates that online platforms provide "effective and expeditious complaints and redress mechanisms."

The challenge is that there is an inherent tension between the interests of copyright holders and users. From the perspective of big content owners, an "effective and expeditious" takedown regime is one that takes down content first and asks questions later. Content owners argue that giving users too much due process allows them to abuse the system, repeatedly uploading copies of infringing files. But critics say that YouTube's efforts to appease rights holders has created a system where it is too burdensome for users to pursue legitimate appeals.

Balancing fairness to content creators against fairness to users is inherently tricky. Rather than trying to address the issue directly, the European Parliament is simply pushing the issue down to the national level, letting governments in Germany, France, Poland, and other European governments figure out the messy details.

The other big concern is that these new regulations will be overly burdensome for smaller online services. YouTube spent $60 million developing the Content ID system; obviously, a startup trying to compete with YouTube is unlikely to have $60 million available to spend on a competing system. So there is a danger that shifting responsibility onto online platforms will have the practical effect of cementing the dominance of today's major platforms.

The legislation approved by the European Parliament attempts to deal with this by including a carve-out for small businesses. The new rules only apply to "online content sharing services," and the definition of that category excludes "microenterprises and small sized enterprises," which are defined as having fewer than 50 employees. Of course, that means that a would-be YouTube competitor could suddenly be hit with a bunch of new legal obligations on the day it hires its 51st employee.

The legislation requires a new copyright for news publishers to restrict how people summarize and link to their articles. The goal is to get Google, Facebook, and other technology giants to pay news publishers licensing fees for permission to link to their articles.

Critics have derided this as a "link tax." The legislation remains vague about how this will work in practice. It doesn't make clear what kinds of links or summaries will be allowed and which will require a license.

Wikimedia—which hosts the popular online encyclopedia—is one of a number of opponents of the law, slamming it as a "threat to our

fundamental right to freely share information."

Mozilla, the firm behind the internet browser Firefox, is also opposed, and argues the law could "make filtering and blocking online content far more routine."

Tim Berners-Lee, an inventor of the World Wide Web, and Jimmy Wales, the founder of Wikipedia, were among a number of high-profile industry figures to co-sign an open letter last month lambasting the proposed law as an "imminent threat" to the future of the internet.

Activists are concerned that the law could stop people from posting everything from an internet meme to a news article. Memes, a central part of internet culture, often rely on the use of copyrighted images, usually for a comedic effect.

In addition to approving new rights for news publishers, the legislation also narrowly approved a new copyright for the organizers of sports teams. Copyright law already gives teams the ability to sell television rights for their games, but fans have traditionally been free to take pictures or personal videos and share them online. The new legislation could give sports teams ownership of all images and video from their games, regardless of who took them and how they are shared. Reported in: cnbc, July 5; ars technica.com, September 12.