NEWS IS IT LEGAL?

SCHOOLS
Augusta, Maine

Should it be against the law for teachers to assign materials that some parents might consider "obscene"? A bill that would criminalize the act of assigning violent or sexually explicit learning materials (in the form of literature, art, or film) to students in Maine classrooms has been introduced in the Maine legislature.

LD 94, proposed by Representative Amy Arata (R-New Gloucester) seeks to make it a felony for teachers and school administrators to knowingly allow students to be exposed such material without student or parental consent. This was to be considered a Class C crime—a felony that could have potentially brought a fine and jail time.

In an initial vote, the bill was unanimously rejected by members of a legislative committee on February 11. Rep. Arata said she intended to amend her bill to remove the felony portion. Lawmakers discussed further options and have agreed to take a new vote.

While Republicans on the committee spoke in favor of Arata's intent, they shared Democrats' concerns about the criminal component.

Rather than change the criminal code to bring punitive charges against teachers, committee members urged Arata to reach out to the state Board of Education with her concerns.

She plans to draft a new bill removing the criminal aspect, but requiring teachers get "informed consent" from a parent or guardian and the student before distributing "obscene" material.

"It was never my intent to have anybody go to jail," Arata said. Instead, she wants to raise awareness around the issue so parents will know to "pay more attention and ask questions." Reported in: *Bangor Daily News,* February 11, 2019.

COLLEGES AND UNIVERSITIES
Washington, D.C.

Would a presidential executive order regulating free speech on college campuses result in more free speech or more censorship?

Speaking at the Conservative Political Action Conference (CPAC) on March 2, President Trump said he wants universities' federal funding to be at risk if they fail to protect conservatives' right to express their viewpoints. Details of his proposed executive order still had not been released by mid-March.

As an example of why he feels such federal intervention is needed, the president cited conservative activist Hayden Williams of the Leadership Institute, who was physically assaulted in February at the University of California's Berkeley campus.

But some professors are disputing the president's argument that the incident justifies an executive order. Neither Williams nor his attacker, Zachary Greenberg, are students or employees of the university. A UC Berkeley spokesperson said that Williams "had every right to be on campus, and every right to express his view."

Many educators are concerned that Trump's executive order will regulate free speech on college campuses. Following the president's announcement at CPAC, University of Chicago president Robert Zimmer wrote a letter calling the declaration "a grave error for the short and the long run."

Zimmer warned, "It makes the government, with all its power and authority, a party to defining the very nature of discussion on campus. A committee in Washington passing judgment on the speech policies and activities of educational institutions, judgments that may change according to who is in power and what policies they wish to promulgate, would be a profound threat to open discourse on campus." Reported in: *The Observer,* March 2, March 6, 2019.

Minneapolis, Minnesota

Can a university professor be disciplined for using the n-word in class? What if he is reading a literary passage to his students that includes the n-word? Or does his academic freedom allow him to expose his students to the offensive word?

The American Association of University Professors' (AAUP) Department of Academic Freedom, Tenure, and Governance has sent a letter to the president of Augsburg University after the university suspended Phillip Adamo over his use of a quoted passage from a book by James Baldwin which used the n-word.

AAUP raised the concern that Adamo's suspension was a violation of his academic freedom, as it appears to have been primarily based on classroom speech that was clearly protected by principles of academic freedom. AAUP also raised concerns that his suspension violates Association-supported procedural standards that are explicitly incorporated into Augsburg University's faculty handbook.

Adamo contacted the AAUP after receiving a letter from Dr. Karen Kaivola, Augsburg's provost and chief academic officer, informing him of his temporary suspension from teaching in the current spring semester pending a "formal resolution process" concerning potential misconduct.

AAUP's letter, signed by Hans-Joerg Tiede, AAUP's associate secretary, said, "To the extent that the administration's actions against Professor Adamo are based on his reading from *The Fire Next Time* in

his class, they violate his freedom in the classroom under principles of academic freedom long recognized by this Association and in Augsburg University's faculty handbook." Tiede added that "Professor Adamo's public suspension raises concerns about its impact on the climate for academic freedom at Augsburg University generally" and "is likely to have a chilling effect on others who teach at the institution." Reported in: aaup.org, February 1, 2019.

PRIVACY

Orange County, California; Eden Prairie, Minneapolis, Rochester, and St. Paul, Minnesota; Raleigh, North Carolina; Henrico, Virginia

How often are local police and federal investigators using "reverse location" search warrants? How many innocent cell phone users are being investigated simply because they were somewhere near the scene of a crime within a certain time frame?

Slate, Forbes, WRAL-TV in Raleigh, North Carolina, and Minnesota Public Radio (MPR) all have recently reported on police departments using search warrants that allow them to sweep up the coordinates and movements of every cellphone in a broad area, to see if any of the phones came close to the site of their investigation.

Police departments across the country have been knocking at Google's door for at least the last two years with warrants to tap into the company's extensive stores of cellphone location data, according to *Slate.*

Captain John Sherwin of the Rochester Police Department in Minnesota told *Forbes* it wasn't just Google that could furnish cops with a startling mount of detailed location data. Facebook and Snapchat also had proven useful, he said.

MPR described a warrant "so expansive in time and geography that it had the potential to gather data on tens of thousands of Minnesotans."

With such warrants, according to *Slate,* "the police can end up not only fishing for a suspect, but also gathering the location data of potentially hundreds (or thousands) of innocent people. There have only been anecdotal reports of reverse-location searches, so it's unclear how widespread the practice is, but privacy advocates worry that Google's data will eventually allow more and more departments to conduct indiscriminate searches."

Cases where reverse-location search warrants were used include:

- A suspicious fire, a murder, and sexual battery in Raleigh, North Carolina;
- Home invasions, theft, and a shooting in Minnesota;
- Unspecified searches by the State Bureau of Investigation in Orange County, California;
- An FBI investigation into a string of robberies in Virginia.

Law enforcement at all levels of government for years have used warrants to collect information on every phone connected to a cell tower at a certain time. But Google's location tracking is more precise, and Google tracks phones that aren't connected to cell towers, such as those using GPS satellites or Wi-Fi. Follow-up warrants involving devices using Google may ask for more personal information, such browsing history and past purchases.

Google issued a statement: "We have an established process for managing requests for data about our users, and in these particular instances, require a search warrant. We always push back on overly broad requests, to protect our users' privacy."

Many privacy advocates argue that reverse-location search warrants are prohibited under the Fourth Amendment, which generally dictates that searches by law enforcement need to be specific and limited only to what's necessary.

Law enforcement "needs to suspect a particular person or criminal activity, not just go, for example, search every home in a given area," said Jennifer Lynch, who serves as the surveillance-litigation director for the Electronic Frontier Foundation.

One of the main concerns with these generalized searches is that the data of unsuspecting innocent people inevitably falls into the hands of police. Even though these people might not be breaking any laws, the information that such methods dredge up could still be revealing and sensitive. "What if this type of location-based collection is occurring in our red light district and you're finding out everyone who was there, or some sort of shady establishment? Or what if you're targeting at a medical facility or religious house of worship?" says Jake Laperruque, who serves as senior counsel at the Constitution Project. "It gets really bad really fast."

Privacy advocates are encouraging judges to be more discerning in approving warrant applications. Because this is a relatively new technique, some worry that the courts do not understand the true invasiveness of what police departments are requesting or how much precise location data Google has stored. Reported in: WRAL-TV, March 15, 2018 and July 13, 2018; *Forbes,* October 23, 2018; MPR, February 7, 2019; *Slate,* February 19, 2019.

Albany, New York

How much personal information is Facebook collecting? New York Governor Andrew Cuomo on February 22 ordered two state agencies to investigate a media report that Facebook Inc. may be accessing far more personal information from smartphone users than previously known, including health and other sensitive data.

The directive to New York's Department of Financial Services (DFS) came after the *Wall Street Journal* (WSJ) said testing showed that Facebook collected personal information within seconds of users entering it into other apps on their smartphones.

The WSJ reported that several apps share sensitive user data, including weight, blood pressure, and ovulation status with Facebook. The report said the company can access data in some cases even when the user is not signed into Facebook or does not have a Facebook account.

In a statement, Cuomo called the practice an "outrageous abuse of privacy." He also called on the relevant federal regulators to become involved.

Facebook said in a statement it would assist New York officials in their probe, but noted that the WSJ's report focused on how other apps use people's data to create ads.

"As (the WSJ) reported, we require the other app developers to be clear with their users about the information they are sharing with us, and we prohibit app developers from sending us sensitive data. We also take steps to detect and remove data that should not be shared with us," the company said.

In late January, Cuomo and New York Attorney General Letitia James announced an investigation into Apple Inc. about its failure to warn consumers about a FaceTime bug that had let iPhones users listen to conversations of others who have not yet accepted a video call.

In March, New York's financial services department is slated to implement the country's first cybersecurity rules governing state-regulated financial institutions such as banks, insurers, and credit monitors.

In January, DFS said life insurers could use social media posts in underwriting policies, so long as they did not discriminate based on race, color, national origin, sexual orientation, or other protected classes. Reported in: Reuters, February 25, 2019.

INTERNATIONAL

New Delhi, India

Should a national government censor online communications to limit the spread of "fake news"? In India, the government has proposed new rules that could have a profoundly chilling effect on free speech and privacy online.

Under the new rules, internet and social media platforms would be required to deploy automated tools to ensure that information or content deemed "unlawful" by government standards never appears online. The Indian government has yet to define what it considers unlawful, but critics warn that it could create incentives for internet companies to flag, and potentially remove, more content than necessary, to avoid publishing something illegal. The definition of "unlawful" likely would encompass everything prohibited under Indian law, which includes hate speech against certain protected groups, defamation, child abuse, depictions of rape, and many other types of communication.

Efforts to automatically flag content that could potentially fall under any of these categories will likely identify a lot of legal, and unobjectionable, material, *Wired* suggested.

The newly proposed rules also require secure messaging services like WhatsApp to decrypt encrypted data for government use, which could affect the security of users around the globe. The rules also would require internet companies to notify users of their privacy policies monthly.

The proposed changes involve Section 79 of the IT Act, a safe harbor protection for internet "intermediaries" that's akin to Section 230 of the Communications Decency Act in the United States. Current Indian law protects intermediaries such as internet service providers and social media platforms from liability for the actions of their users until they are made aware of a particular post; without the new rules intermediaries currently are only required to censor content when directed by a court.

Even before the rules go into effect, internet companies have begun self-censoring content in response to the proposed change. On January 17, Netflix and eight other streaming services voluntarily agreed to ban unlawful content from their platforms. According to BuzzFeed News, Netflix's decision to self-regulate was "an attempt to avoid official government censorship."

In a statement, India's Internet Freedom Foundation described the proposal as "a tremendous expansion in the power of the government over ordinary citizens eerily reminiscent of China's blocking and breaking of user encryption to surveil its citizens."

Mozilla policy adviser Amba Kak said much of the same in a January 2 post. The proposal "calls into play numerous fundamental rights and freedoms guaranteed by the Indian constitution," Kak wrote. "Whittling down intermediary liability protections and undermining end-to-end encryption are blunt and

disproportionate tools that fail to strike the right balance."

According to reports by India's *Economic Times*, government officials say the push to weaken encryption services is in response to recent criticism of secure messaging app WhatsApp, which is owned by Facebook. Misinformation ran rampant across the massively popular platform last year, exacerbating tensions between castes and fanning violence.

Government officials elsewhere have used similar arguments to justify encryption-busting tactics. Most recently, Australia's Parliament passed sweeping legislation giving authorities the ability to demand companies create backdoors in secure messaging services. Reported in: *Wired,* January 18, 2019.