THE
BRECHNER REPORT

Volume 40, Number 5 ■ A monthly report of mass media law in Florida
Published by The Brechner Center for Freedom of Information ■ College of Journalism and Communications ■ University of Florida
May 2016

Supreme Court rules First Amendment protects police officer demoted for perceived speech

WASHINGTON – The First Amendment generally prohibits government employers from dismissing or demoting a public employee for engaging in constitutionally-protected speech. Now, the U.S. Supreme Court has ruled it unconstitutional to demote a police officer based on the mistaken belief that the officer had engaged in political activity.

Jeffrey Heffernan, the petitioner in the case, was a police officer in Paterson, New Jersey. Heffernan was demoted after other officers saw him with a sign for a mayoral candidate, leaving the impression that he supported the candidate. In fact, Heffernan was merely picking up the sign at the request of his bedridden mother.

The case had been appealed up from the 3rd Circuit Court of Appeals, which ruled Heffernan's constitutional rights had not been violated because he had not actually exercised his First Amendment rights.

FIRST AMENDMENT

However, the Supreme Court disagreed. "When an employer demotes an employee out of a desire to prevent the employee from engaging in political activity that the First Amendment protects, the employee is entitled to challenge that unlawful action under the First Amendment," Justice Stephen G. Breyer wrote for the Court's majority. That is "even if, as here, the employer makes a factual mistake about the employee's behavior," he added.

Source: Heffernan v. City of Paterson, *No. 14–1280*

Court rules on FOIA fee reduction for students

WASHINGTON – The U.S. Court of Appeals for the District of Columbia ruled that students who make Freedom of Information Act requests are eligible for reduced fees because they are part of an "educational institution."

FOIA

FOIA requesters fall under one of three categories, which determine the fees an agency may charge to fulfill the request. One of the categories includes noncommercial requests made by educational institutions, scientific institutions, and the news media. Those who fall within this category qualify for reduced fees and may only be charged for document duplication, but not for costs related to document search or review.

Courts have agreed that teachers qualify for a fee reduction under the definition of "educational institution," but students had not previously been held to the same standard.

Writing for the court, Judge Brett Kavanaugh explained, "Students who make FOIA requests to further their coursework or other school-sponsored activities are eligible for reduced fees under FOIA because students, like teachers, are part of an educational institution."

The University of Virginia student involved in this case, Kathryn Sack, submitted her FOIA requests to the Department of Defense while researching for her Ph.D. dissertation on polygraph bias. The lawsuit arose after the Department refused to categorize Sack as an educational-institution requester and handed Sack a bill of $900 for the request.

Source: Sack v. United States Department of Defense*, No. 14-5039*

FOIA lawsuit seeks FISC orders for encrypted data

SAN FRANCISCO – The Electronic Frontier Foundation has filed a Freedom of Information lawsuit against the U.S. Department of Justice in an attempt to disclose whether the government has used secret court orders to force technology companies to decrypt their customers' private information, according to an EFF press release.

The lawsuit specifically seeks information about whether the government has ever sought or obtained an order from the Foreign Intelligence Surveillance Court requiring third-party technology companies to assist in surveillance efforts, the press release states.

EFF filed its FOIA requests in October and March in response to increasing government pressure on companies to provide access to the encrypted data on their customers' devices, including the FBI's attempt to have Apple create a "backdoor" to the San Bernadino shooter's iPhone, according to the press release.

FOIA

EFF Senior Staff Attorney Nate Cardozo stated in the press release, "If the government is obtaining FISC orders to force a company to build backdoors or decrypt their users' communications, the public has a right to know about those secret demands to compromise people's phones and computers." Such practices compromise the safety and security of people whose devices contain deeply personal and private information, Cardozo added.

Source: Electronic Frontier Foundation

FOIA official resigns from office

WASHINGTON – The director of the Office of Government Information Services, which is tasked with overseeing the operation of the Freedom of Information Act across the Obama Administration, is resigning after only 9 months on the job, Politico reported.

James Holzer took over his role as a transparency official last August at OGIS, which conducts audits of agencies' FOIA operations and proposes methods of streamlining those operations, according to the website.

Holzer is returning to his previously-held position at the Department of Homeland Security, the website reported.

Lawmakers have attempted to give OGIS more independence and effectiveness in FOIA oversight through proposed legislation this year, but the measure awaits referral to a conference committee or a decision on the final drafting of the bill, the website reported.

Source: POLITICO

Court upholds order denying drone records

WASHINGTON – The U.S. Circuit Court of Appeals for the District of Columbia upheld a lower court's order denying the American Civil Liberty Union's Freedom of Information Request for information about the government's use of drones in "targeted killings."

The ACLU sought legal memoranda related to the government's use of drones in premeditated killings as well as records from the CIA that include the identities and location of the targeted individuals, the number of people killed, and the agencies involved.

The CIA refused to release any records, claiming the information fell under FOIA exemptions. The District Court granted the agency summary judgement, and the D.C. Circuit agreed that the information was exempt under FOIA Exemption 1 (pertaining to classified records).

Source: American Civil Liberties Union v. United States Department of Justice*, 15-5217*

Commodity promotions programs want FOIA exemption

WASHINGTON – The House Appropriations Committee has asked the U.S. Department of Agriculture to exempt the American Egg Board and other similar research and promotions boards from FOIA requests, NPR reported.

The commodity promotions programs that seek FOIA exemptions have often been controversial because they use government authority to collect money for private commercial goals, such as advertising campaigns, NPR reported.

Parke Wilde, a food policy expert at Tufts University, criticizes the food industry groups that "very much want to have it both ways," according to NPR. Wilde points out that industry groups argued in 2005 before the Supreme Court that the programs entailed "government speech," but now the programs are emphasizing their private nature in order to circumvent FOIA requirements, NPR reported.

Source: NPR

Bill to force tech companies to unencrypt data

PRIVACY

WASHINGTON – Lawmakers have introduced a bill that would require technology companies to comply with court orders demanding access to their encrypted services or devices, Yahoo News reported.

Senators Richard Burr, R-North Carolina, and Dianne Feinstein, D-California, introduced the bill, dubbed the "Compliance with Court Orders Act of 2016," to help law enforcement access information related to criminal investigations on encrypted services and devices, according to the website.

The bill presents conflicting ideas by stating technology companies must do whatever it takes to unencrypt data and fulfill court orders, but on the other hand states the government is not asking the companies to change the design of their services or devices, the website reported.

Additionally, the bill includes a provision that requires the government to pay for reasonable costs associated with such requests. However, the bill does not discuss what would happen if a company refused to comply with a court order for encrypted data, which leaves the courts to decide penalties on a case-by-case basis, according to the website.

Source: Yahoo News

County won't refund commissioner's legal fees

ACCESS MEETINGS

MANATEE COUNTY – The Manatee County Commission rejected Commissioner Robin DiSabatino's request for reimbursement of her legal bills arising out of a case accusing her of violating the state's Public Records Law, the Sarasota Herald-Tribune reported.

DiSabatino defended herself in a three-yearlong legal battle against Michael Barfield, a paralegal with Citizens For Sunshine, the paper reported. Her legal fees exceeded $30,000, including $6,500 she paid to settle the lawsuit, according to the paper. County attorneys did not defend her because the records at issue had been stored on DiSabatino's personal computer, the paper reported.

County Attorney Mickey Palmer advised the county commissioners not to authorize the requested reimbursement because state law says that she must have prevailed in the lawsuit to qualify for reimbursement, according to the paper.

DiSabatino's attorney, Ralf Brookes, claims DiSabatino did prevail in the case and says he intends to file a lawsuit against the county to seek reimbursement of the legal fees, the paper reported.

Source: Sarasota Herald-Tribune

City Hall raid

DEBARY – State law enforcement agents raided DeBary City Hall, taking more than 37,000 emails sent and received by the city manager, who has been accused of violating the state's Sunshine Law, The Daytona Beach News-Journal reported.

The warrant asked for emails related to controversial dealings between the city and the St. Johns River Water Management District for a development project in conservation land near the city's SunRail station, the paper reported.

ACCESS MEETINGS

DeBary City Manager Dan Parrott may have violated the Sunshine Law when he sent an email to four out of five council members, seeking feedback on a letter drafted to the water district's executive director, Ann Shortelle, according to the paper.

President of the First Amendment Foundation, Barbara Petersen, warns that asking council members' opinions on a letter is basically polling the members, which should only take place in an open and public meeting, the paper reported. Even in situations in which a state official needs a quick response, the proper way to address the issue is at an emergency meeting, Petersen suggested.

Source: The Daytona Beach News-Journal

THE BRECHNER REPORT

Brechner Center for Freedom of Information
3208 Weimer Hall, P.O. Box 118400
College of Journalism and Communications
University of Florida, Gainesville, FL 32611-8400
http://www.brechner.org
e-mail: brechnerreport@jou.ufl.edu

Sandra F. Chance, J.D., Exec. Director/Exec. Editor
Linda Riedemann Norbut, Editor
Sarah Silberman, Production Coordinator

The Brechner Report is published 12 times a year under the auspices of the University of Florida Foundation. *The Brechner Report* is a joint effort of The Brechner Center for Freedom of Information, the University of Florida College of Journalism and Communications, the Florida Press Association, the Florida Association of Broadcasters, the Florida Society of Newspaper Editors and the Joseph L. Brechner Endowment.

Once-public data is trade secret

TALLAHASSEE – Florida's 2nd Circuit Court for Leon County ruled that State Farm Insurance may keep hidden trade secrets that have otherwise been public for years, The Palm Beach Post reported.

The ruling could impact other property insurers by allowing them to quash public access to information submitted to the state's Quarterly and Supplemental Reporting System, the paper reported. The system keeps a quarterly tally on how many policies a company has statewide or in a particular county and how many policies have been cancelled, according to the paper.

State Farm argued that this information should be considered a trade secret to avoid other companies from being tipped off by their own marketing strategies, the paper reported.

This information had been available for public use since 2009, according to the paper.

However, the ruling itself does not discuss the implications the decision to declare this information a trade secret may have on the Public Records Law.

Florida's new insurance commissioner, David Altmaier, will appeal the decision to the 1st District Court of Appeal.

Source: The Palm Beach Post, State Farm Fla. Ins. Co. v. Fla. Office of Ins. Regs*., No. 2014-CA-1267*

FWC stops gun data collection

TALLAHASSEE – The Florida Fish and Wildlife Conservation Commission will stop requiring a form waiver, which range patrons had to complete before being allowed access to any of the commission's public shooting ranges, the Sarasota Herald-Tribune reported.

Florida statute makes it a third-degree felony for any agency to create a gun registry, the paper reported. The problem with such a list is that it could become a tool for harassing or abusing law-abiding citizens based on their choice to exercise their Second Amendment right to bear arms, according to the paper. The law also aims to protect firearm owners from falling victim to theft, the paper reported.

However, the FWC's waiver required gun range patrons to provide their name, address, phone number, email address, driver's license number and primary weapon, according to the paper. These forms are public records and came close to creating a gun registry in violation of state law, the paper reported.

FWC Executive Director Nick Wiley said the agency would scale back the waivers due to concerns from the public, according to the paper.

"I'm glad people brought it to our attention. I'm glad we had a chance to look at it, and I'm glad our staff found a way to fix it," he said.

FWC will still require patrons to sign a waiver of liability, which only requires someone to print and sign their name, the paper reported.

Source: Sarasota Herald-Tribune

Police to use 1,000 body cameras

MIAMI – The Miami-Dade Police Department, the largest in the state, will equip its officers with 1,000 body cameras, ABC News reported.

The $5.5 million initiative is set to be fulfilled by the end of September, the network reported. About $1 million of that will come from a $75 million federal grant program signed by President Obama in 2014, according to the network.

The implementation of body cameras is expected to reduce the number of use-of-force incidents and curb frivolous lawsuits against police officers, the network reported.

Miami-Dade Police Director Juan Perez says the officers will have some discretion to turn off the cameras in particularly sensitive situations, but the general policy will be to have the cameras running as soon as an encounter begins, according to the network.

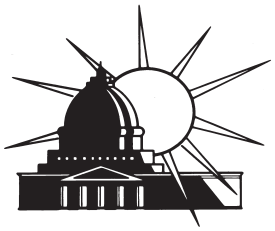
ACCESS

Camera footage will be subject to the state's Public Records Law. Florida's law requiring all parties in a conversation to consent to audio recordings was recently changed by the legislature to exempt police-worn camera footage from the law, the network reported.

Source: ABC News

THE
BRECHNER
REPORT
University of Florida
Brechner Center for Freedom of Information
3208 Weimer Hall, P.O. Box 118400
Gainesville, FL 32611

May 2016



UF UNIVERSITY of FLORIDA

Non-Profit Organization
U.S. POSTAGE
PAID
Permit No. 94
Gainesville, FL

Time to Kill Another Dangerous CFAA Bill

The Computer Fraud and Abuse Act (CFAA), the federal "anti-hacking" statute, is long overdue for reform. The 1986 law—which was prompted in part by fear generated by the 1983 technothriller WarGames—is vague, draconian, and notoriously out of touch with how we use computers today. Unfortunately, Sens. Sheldon Whitehouse and Lindsey Graham are on a mission to make things worse. They've proposed (for the second time) legislation that fails to address any of the CFAA's problems while simply creating more confusion. And they may try to sneak their proposal through as an amendment to the Email Privacy Act—the very same sneaky tactic they tried last year.

Their latest proposal is ostensibly directed at stopping botnets. It's even named it the "Botnet Prevention Act of 2016." But the bill includes various provisions that go far beyond protecting against attacks by zombie computers:

The Back Page
By Jamie Williams

First, the bill would expand the CFAA's existing prohibition against selling passwords to trafficking in any "means of access." The broadening is unnecessary and misguided, as other statutes—like the U.S. code section concerned fraud in connection with access devices—already cover what the authors seem to be targeting. The bill also doesn't define "means of access," another sign of its poor drafting. With no guidance, it's unclear how broadly prosecutors or courts will apply this provision. The provision could make criminals of paid researchers who test access in order to identify, disclose, and fix vulnerabilities.

Second, the bill empowers government officials to obtain court orders to force companies to hack computer users for a wide range of activity completely unrelated to botnets. What's worse is that the bill allows the government to do this without any requirement of notice to non-suspect or innocent customers or companies, including botnet victims. It's understandable that the government does not want to tip off potential suspects, but those not suspected of committing any crime should be notified when their computers are part of a criminal investigation.

Third, the bill would create a new felony offense of damaging "critical infrastructure." But this conduct, too, is already captured under the CFAA's existing provisions. The section is yet another classic example of overcriminalization and redundancy—especially at a time when Congress is debating a significant decriminalization bill. And although "critical infrastructure" may sound limited, the definition in the bill tracks the Department of Homeland Security's definition, which includes software companies and ISPs. Plus, given the provision's steep penalties and limits on judges' discretion to reduce sentences or allow sentences to run concurrently (rather than back-to-back), it will simply give prosecutors even more leverage to force defendants into plea deals.

These changes would only increase—not alleviate—the CFAA's harshness, overbreadth, and confusion.

As noted, this isn't the senators' first attempt to take the CFAA in the wrong direction. Last year, they tried to slip similarly terrible measures through Congress via an amendment to the notorious Cybersecurity Information Sharing Act of 2015 (CISA). Sens. Whitehouse and Graham's proposal was ultimately not included in CISA, which Whitehouse blamed on the "pro-botnet" caucus, but in reality, it's because a lot of people—including a lot of EFF supporters—spoke out against the egregious CFAA amendment.

The senators' proposal has no grounding in what would actually keep us—or our computers—safe. Rather, it seems motived by the same vague fears of a hypothetical computer takeover that overtook Congress (after watching a clip from WarGames) back in 1986. In that way, Whitehouse and Graham may be keeping true to the CFAA's roots. But now it's time to focus on reality.

Just as last year, EFF will oppose the senators' proposal—in whatever form it takes. What we need is reform that reigns in the CFAA, not a measure that makes things worse.

This article first appeared on www.EFF.org on May 26, 2016.