THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | SUMMER 2021

U.S. Department of Justice Limits Seizure of Journalists' Records and Information

On July 19, 2021, several media outlets reported that U.S. Attorney General Merrick Garland has formally prohibited the U.S. Department of Justice (DOJ) from seizing journalists' phone and email records in connection with government leak investigations. Observers praised the move as an important step in protecting freedom of the press in the United States after revelations in the first half of 2021 that President Donald Trump's administration secretly seized journalists' records on at least three occasions.

The Trump administration continued the trend started by President Barack Obama's administration of prosecuting individuals for leaking classified government information under the Espionage Act, 18 U.S.C. § 793, including to members of the press. The first such case for the Trump administration came to an end on Aug. 23, 2018 when former National Security Agency (NSA) contractor Reality Winner was sentenced to 63 months in prison and three years of probation, as well as 100 hours of community service upon her release. Winner was released from federal prison on June 2, 2021. (For more information on the cases against Winner and others, see "Investigations, Prosecutions, and Sentencing Continue in Government Leak Cases" in the Fall 2018 issue of the Silha *Bulletin* and "Trump Administration Targets Journalist, Leaker of Government Information, and Former Government Employees Who Took Classified Documents" in the Summer 2018 issue.)

Additionally, on May 23, 2019, the DOJ released an indictment alleging 18 charges against WikiLeaks founder Julian Assange, 17 of which were under the Espionage Act, prompting significant concern from journalists and press advocates that the indictment was the next step in prosecuting traditional journalists under the statute. (For more information on the charges against Assange, see "Federal Prosecutors Charge Julian Assange With Seventeen Counts Under the Espionage Act, Prompting Renewed Concern for Journalists" in the Summer 2019 issue of the Silha *Bulletin*.)

On July 27, 2021, several media outlets reported that former U.S. Air Force intelligence analyst Daniel Everette Hale was sentenced to 45 months in prison for retention and transmission of national defense information under the Espionage Act. Previously, on March 31, 2021, Hale pleaded guilty after he leaked classified documents revealing the government's use of drone strikes for "targeted killings" overseas, among other revelations. (For more information on Hale's leak and the prosecution against him, see *Former Government Intelligence Analyst Charged with Leaking Classified Information to* The Intercept in "Trump Administration Targets Two More Leakers of Government Information" in the Fall 2019 issue of the Silha *Bulletin*.)

In an *amicus* brief filed in July 2021 ahead of Hale's sentencing hearing, 17 media law professors and scholars, including Silha Professor of Media Ethics and Law and Director of the Silha Center Jane E. Kirtley and University of Minnesota Law School Robins Kaplan Professor Heidi Kitrosser, argued that the prosecution of Hale and other government whistleblowers under the Espionage Act "raises substantial First Amendment concerns," including that "the government will abuse its censorial powers to target speech that it dislikes or that threatens its interests or credibility. Prosecutions that target leaks to the [news] media directly raise these concerns." They also risk chilling speech and reporting about important topics and information of public interest.

Espionage Act prosecutions, according to the brief, also conflict with two First Amendment principles: "(1) speech about the actions of our government receives the highest level of constitutional protection, and (2) heightened scrutiny is necessary when the government seeks to shield particular information about itself from public view." The brief therefore called for a "just sentence" that would "necessarily take into account the First Amendment interests at stage when the Executive uses the [Espionage] Act in this unanticipated way — weighing any harm caused by disclosure of the classified information at issue against the importance of the disclosure to informed public disclosure and democratic accountability." The full brief is available online at: https://drive.google.com/file/d/1Y_yDOFXazv71XwlUJAX1X2QGQCO5qcI1/view.

Additionally, on June 3, 2021, former U.S. Department of the Treasury official Natalie Mayflower Sours Edwards was sentenced to six months in prison after she pled guilty to one count of conspiracy to make unauthorized disclosures of suspicious activity reports (SARs) in January 2021, as reported by *BuzzFeed News*. (For more information on Edwards' leak and the prosecution against her, see *Senior Treasury Department Employee Charged with Leaking Confidential*

DOJ Limits, *continued on page 3*

Inside This Issue

Summer 2021: Volume 26, No. 3

Silha Center Staff

DOJ Limits, *continued from page 1*

Documents to BuzzFeed News in "Investigations, Prosecutions, and Sentencing Continue in Government Leak Cases" in the Fall 2018 issue of the Silha *Bulletin*.)

In some cases, leak investigations and prosecutions have implicated members of the press. For example, in 2018, *The New York Times* reported that during an FBI investigation into alleged classified leaks by former U.S. Senate Select Committee on Intelligence (SSCI) director of security James A. Wolfe, who was charged and arrested on three counts of lying to federal authorities, prosecutors secretly seized phone and email records of *Times* reporter Ali Watkins. (For more information on the confiscating of Watkins' records, see *Federal Prosecutors Seize Phone and Email Records of* New York Times *Reporter in Leak Investigation* in "Trump Administration Targets Journalist, Leaker of Government Information, and Former Government Employees Who Took Classified Documents" in the Summer 2018 issue of the Silha *Bulletin*. For more information on the lawsuit, see "First Amendment Coalition Sues Department of Justice Over Secret Collection of Journalist's Telephone and Email Records" in the Fall 2018 issue of the Silha *Bulletin*.)

COVER STORY

Another example is James Risen, a Pulitzer Prize winning journalist and author. In 2010, federal prosecutors indicted Jeffrey Sterling, a former Central Intelligence Agency (CIA) officer, alleging that Sterling provided classified information for Risen's book, *State of War*. In 2011, then-Attorney General Eric Holder authorized a subpoena ordering Risen to testify at Sterling's trial, to which Risen refused. In 2013, a U.S. Court of Appeals for the Fourth Circuit three-judge panel overturned a district court order, which had prevented prosecutors from asking Risen the name of his source. After the U.S. Supreme Court declined to hear Risen's case in June 2014, he faced potential jail time for contempt. However, the DOJ ultimately did not seek Risen's testimony. (Risen and his attorney Joel Kurtzberg were the 2015 Silha lecturers. For more information about the lecture, see "30th Annual Silha Lecture Addresses Challenges to Reporting on National Security Matters" in the Fall 2015 issue of the Silha *Bulletin* and "30th Annual Silha Lecture to Feature *New York Times* Investigative Reporter James Risen and Attorney Joel Kurtzberg" in the Summer 2015 issue. For more information on the background to Risen's case, see "Espionage Conviction Ends Lengthy Struggle to Compel Journalist's Testimony" in the Winter/Spring 2015 issue of the Silha *Bulletin*, "Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberties" in the Fall 2014 issue, "Update: Supreme Court Declines to Hear Reporter's Privilege Cases" in the Summer 2014 issue, "Reporters Struggle to Claim Privilege to Avoid Testifying About Confidential Sources" in the Fall 2013 issue, and "Judges Rebuke Government on Leak Prosecutions" in the Summer 2011 issue.)

The DOJ's guidelines regarding obtaining journalists' records, 28 CFR § 50.10, date back to 1970 when Attorney General John Mitchell instituted them in response to press concerns about the growing number of subpoenas seeking to compel journalists to reveal confidential news sources. In 2013, the DOJ amended the guidelines following growing criticism after the department obtained Associated Press (AP) telephone records. The same year, the DOJ named Fox News reporter James Rosen as a co-conspirator during a leak investigation of a State Department official in order to obtain Rosen's emails. (For more information on the secret subpoenas of the AP, see "Justice Department Secretly Subpoenas Associated Press Phone Records" in the Winter/Spring 2013 issue of the Silha *Bulletin* and "Department of Justice Revises Guidelines for Investigating Journalists" in the Summer 2013 issue. For more information on the targeting of Rosen, see "Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberty" in the Fall 2014 issue of the Silha *Bulletin*. For more on the Obama administration's prosecution of individuals under the Espionage Act, see "President Barack Obama Leaves Mixed Legacy on Government Transparency" in the Fall 2016 issue of the Silha *Bulletin*, "Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberties" in the Fall 2014 issue, "Manning, Kiriakou Face Punishment for Blowing the Whistle on the War on Terror" in the Winter/Spring 2013 issue, "Leaks: New Policies Emerge; Congress Gets Involved" in the Summer 2012 issue, "The Obama Administration Takes on Government Leakers; Transparency May be a Casualty" in the Winter/Spring 2012 issue, "Judge Rebukes Government on Leak Prosecutions" in the Summer 2011 issue, "Open Government Advocates Criticize Obama's Prosecution of Leakers" in the Winter/Spring 2011 issue, and "The Media and the Military: Guantanamo Access Rules Loosened; Other Guidelines Set to Limit Leaks" in the Fall 2010 issue.)

In 2014 and 2015, the DOJ further revised the guidelines, strengthening protections for reporters. However, in 2019, *The Hill* opinion contributor John Solomon reported that then-Deputy Attorney General Rod Rosenstein's office had been overseeing for several months the revision of U.S. Department of Justice (DOJ) guidelines regarding the obtaining of journalists' records by law enforcement. (For more information on Rosenstein's actions, see *DOJ Reviews Guidelines Regarding Issuing Subpoenas, Court Orders, and Search Warrants Against Journalists* in "Department of Justice Continues Mulling Policies Regarding Jailing, Subpoenaing, and Searching U.S. Journalists" in the Winter/Spring 2019 issue of the Silha *Bulletin*.)

The guidelines, titled "Policy regarding obtaining information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media," previously provided that the "use of certain law enforcement tools, including subpoenas, court orders, . . . and search warrants to seek information from, or records of, non-consenting members of the news media [are] extraordinary measures, not standard investigatory practices." Therefore, according to the guidelines, these measures may only be used 1) after the Attorney General has authorized the use, 2) when the information sought is "essential to a successful investigation, prosecution, or litigation," and 3) after "all reasonable alternative attempts have been made to obtain the information from alternative sources." The full guidelines are available online at: https://www.law.cornell.edu/cfr/text/28/50.10. (For more information about the previous DOJ guidelines, see *DOJ Reviews Guidelines Regarding Issuing Subpoenas, Court Orders, and Search Warrants Against Journalists* in "Department of Justice Continues Mulling Policies Regarding Jailing, Subpoenaing, and Searching U.S. Journalists" in the Winter/Spring 2019 issue of the Silha *Bulletin*.)

In 2021, at least three instances of the DOJ under President Trump seizing journalists' records came to light, prompting

DOJ Limits, *continued on page 4*

DOJ Limits, *continued from page 3*

concern and criticism from members of the news media and press advocates. First, on May 7, 2021, *The Washington Post* reported that the DOJ secretly obtained *Post* journalists' phone records and attempted to obtain their email records in connection to their reporting on Russian interference in the 2016 presidential election. One story was based on classified U.S. intelligence intercepts indicating that then-Sen. Jeff Sessions (R-Ala.) had discussed the Trump campaign with Russia's ambassador to the United States, Sergey Kislyak. The full story is available online at: https://www.washingtonpost.com/world/national-security/sessions-discussed-trump-campaign-related-matters-with-russian-ambassador-us-intelligence-intercepts-show/2017/07/21/3e704692-6e44-11e7-9c15-177740635e83_story.html?itid=lk_inline_manual_18.

According to the *Post*, the DOJ sent "three separate letters dated May 3 . . . to Post reporters Ellen Nakashima and Greg Miller, and former Post reporter Adam Entous," writing that the journalists were "hereby notified that pursuant to legal process the United States Department of Justice received toll records associated with the following telephone numbers for the period from April 15, 2017 to July 31, 2017. The letters listed work, home or cellphone numbers covering that three-and-a-half-month period." Federal prosecutors also "got a court order to obtain 'non content communication records' for the reporters' work email accounts, but did not obtain such records," according to the *Post*.

The *Post*'s full reporting on the seizure of the phone records is available online at: https://www.washingtonpost.com/national-security/trump-justice-dept-seized-post-reporters-phone-records/2021/05/07/933cdfc6-af5b-11eb-b476-c3b287e52a01_story.html.

Second, on May 20, 2021, CNN reported that the Trump administration seized phone records and email records of CNN Pentagon correspondent Barbara Starr. The DOJ informed Starr about the seizures in a May 3 letter, explaining that federal prosecutors obtained her phone and email records from June 1, 2017 to July 31, 2017. According to CNN, prosecutors targeted "Starr's Pentagon extension, the CNN Pentagon booth phone number and her home and cell phones, as well as Starr's work and personal email accounts."

CNN's full reporting on the seizure of the phone and email records is available online at: https://www.cnn.com/2021/05/20/politics/trump-secretly-obtained-cnn-reporter-records/index.html.

Finally, on June 2, 2021, *The New York Times* reported that the DOJ secretly seized the phone records of four *Times* reporters — Matt Apuzzo, Adam Goldman, Eric Lichtblau and Michael S. Schmidt — over the course of four months in 2017. In a letter to the *Times*, the DOJ stated that it also obtained a court order to seize email logs, but that "no records were obtained." The *Times* reported that although the DOJ did not specify which article was being probed as part of an undisclosed leak investigation, the "lineup of reporters and the timing suggested that the leak investigation related to classified information reported in an April 22, 2017, article the four reporters wrote about how James Comey, then the FBI director, handled politically charged investigations during the 2016 presidential election."

> "The attorney general has taken a necessary and momentous step to protect press freedom at a critical time.. . . This historic new policy will ensure that journalists can do their job of informing the public without fear of federal government intrusion into their relationships with confidential sources."
>
> **— Bruce D. Brown, Reporters Committee for Freedom of the Press executive director**

The *Times*' full reporting on the seizure of the phone records is available online at: https://www.nytimes.com/2021/06/02/us/trump-administration-phone-records-times-reporters.html.

On May 21, 2021, several media outlets reported that President Joe Biden had said that he would not allow the DOJ to seize journalists' phone records and emails, calling it "simply, simply wrong." On June 5, Garland announced that the DOJ would cease seizing journalists' materials in order to expose confidential sources.

Five days later, *The New York Times* reported that the DOJ had also targeted Democratic legislators' communication data. The *Times* revealed that Apple informed U.S. House of Representatives Intelligence Committee Chairman Adam Schiff (D-Calif.) and Rep. Eric Swalwell (D-Calif.) in May 2021 that their metadata had been subpoenaed and turned over to the DOJ in 2017 and 2018. The move came as the committee was investigating President Trump's ties to Russia. The subpoenas also targeted other members of the committee, as well as staff and family members. The *Times*' full report is available online at: https://www.nytimes.com/2021/06/10/us/politics/justice-department-leaks-trump-administration.html.

On June 11, the Associated Press (AP) reported that DOJ Inspector General Michael Horowitz had announced that his office, the department's internal watchdog, was probing the DOJ's efforts. On June 17, CBS News reported that the House Judiciary Committee was also investigating the secret subpoenas, including those targeting members of the press.

In a July 19 memo to DOJ leadership and federal prosecutors, Garland formalized the commitment he made in June, according to the AP on the same day. The memo first emphasized that "a free and independent press is vital to the functioning of our democracy." The memo next noted that the DOJ previously used "a balancing test to restrict the use of compulsory process to obtain information from or records of members of the news media." The memo also stated that "[t]he United States has, of course, an important national interest in protecting national security information against unauthorized disclosure." However, the memo contended that "a balancing test may fail to properly weigh the important national interest in protecting journalists from compelled disclosure of information revealing their sources, sources they need to apprise the American people of the workings of their government."

The memo therefore prohibited several actions, including that "[t]he Department of Justice will no longer use compulsory legal process for the purpose of gathering information

from or records of members of the news media acting within the scope of newsgathering activities." The records and information enumerated in the memo include compelled testimony, physical documents, telephone records, metadata, and digital content. The "new prohibition applies to compulsory legal process issued to reporters directly, to their publishers and employers, and to third-party service providers for any of the foregoing." The prohibition applies to "subpoenas, warrants, court orders[,] . . . [and] civil investigative demands."

The new policy included some exceptions, including if "a member of the news media is under investigation for a violation of criminal law, such as insider trading" or if a journalist "used criminal methods, such as breaking and entering, to obtain government information." According to *The Washington Post* on July 19, the DOJ "may seek reporters' records only if the reporter is the subject or target of an investigation outside their journalistic work or is suspected of working as an agent of a foreign power or with a foreign terrorist group, or if there is an imminent risk of bodily harm or death."

The memo clarified that the "prohibition *does* apply when a member of the news media has, in the course of newsgathering, only possessed or published government information, including classified information" (emphasis added). However, the prohibition does not affect the DOJ's ability to target government employees who leaked government information.

The full memo is available online at: https://www.washingtonpost.com/context/u-s-sharply-limits-when-prosecutors-can-seek-reporter-phone-email-records-to-investigate-leaks/9b41fc3b-ad5d-406f-b061-39ebabccfaea/?itid=lk_inline_manual_3.

The Hill reported on July 19 that Garland said that the DOJ would "support congressional legislation" seeking to put the new standards into a statute. As the *Bulletin* went to press, Congress had not passed any legislation to this effect.

In a July 19 statement following the memo, Reporters Committee for Freedom of the Press (RCFP) executive director Bruce D. Brown praised the move. "The attorney general has taken a necessary and momentous step to protect press freedom at a critical time," he wrote. "This historic new policy will ensure that journalists can do their job of informing the public without fear of federal government intrusion into their relationships with confidential sources."

National Press Club president Lisa Nicole Matthews and National Press Club Journalism Institute president Angela Greiling Keane also praised the memo in a July 19 statement. "We are grateful the attorney general has at long last squared Justice Department policy with the First Amendment," they wrote. "Too often in recent years, reporters' communications records have been subpoenaed in the name of fighting leaks. The government has a right to try to protect legitimate secrets. But the public benefits in incalculable ways from an unfettered press exposing facts that government officials sometimes would prefer to keep quiet. The broad and ongoing benefit of that sunshine outweighs the government's interest in clamping down on any particular leak. The new policy gets it right."

— Scott Memmel
Postdoctoral Associate
Silha *Bulletin* Co-editor

The Summer 2021 issue of the Silha *Bulletin* includes several articles adapted from "Privacy and Data Protection," a chapter published in the course handbook for the Practising Law Institute's Communications Law in the Digital Age conference, which will take place in November 2021.

Professor Kirtley gratefully acknowledges the contributions of Silha research assistants Scott Memmel, Jonathan Anderson, Samantha Brunn, and Claire Colby.

Jane E. Kirtley
Silha Center Director and
Silha Professor of Media Ethics and Law

Chauvin Trial Marks Key Moment in Minnesota Media Access to Court Proceedings During Pandemic

On Nov. 4, 2020, Hennepin County District Judge Peter Cahill issued an order allowing limited audio and video recording, broadcasting, and live streaming of the trial of former Minneapolis police officer Derek Chauvin. Cahill cited the "quite unique" circumstances of the trial: the case drew international attention and the COVID-19 pandemic limited public attendance. According to Cahill, "the only way to vindicate the Defendants' constitutional right to a public trial and the media and public's constitutional right of access to criminal trials is to allow audio and video coverage of the trial, including broadcast by the media."

ACCESS

Chauvin was charged with second-degree murder, third-degree murder, and second-degree manslaughter in the death of George Floyd. On May 25, 2020, Chauvin, who was joined by three other police officers, apprehended Floyd for suspicion of using a counterfeit $20 bill. Chauvin knelt on Floyd's neck for 8 minutes and 46 seconds, even after Floyd said he could not breathe and became nonresponsive, according to the initial criminal complaint. A copy of the criminal complaint is available online at: https://z.umn.edu/6z8r. On April 20, 2021, a jury found Chauvin guilty on all charges. (For more information on Floyd's death, protests that followed, incidents between the press and police, incidents between the press and demonstrators, and subsequent litigation, see "Ongoing Protests and Confrontations Between the Press and Police Prompt Legal Action, Ethical Debates, and Media Advocacy" in the Fall 2020 Silha *Bulletin*; "Journalists Covering Fallout from George Floyd Death Take Legal Action; Misinformation Underscores Lessons from 2020 Silha Spring Ethics Forum" in the Summer 2020 issue; and "Special Report: Journalists Face Arrests, Attacks, and Threats by Police Amidst Protests Over the Death of George Floyd" in the Winter/Spring 2020 issue.)

According to Cahill's order, a single pool producer was allowed to record the trial and share the feed to other media outlets. The order set out some limitations: no jurors were to appear on the recording, and no witnesses under the age of 18 could appear without express parental consent. No members of George Floyd's family were to be filmed without consent. According to Nielsen, at least 23.2 million Americans watched on television as Chauvin was convicted April 20 in the death of George Floyd. The trial represented Minnesota's first livestreamed criminal trial. After a successful experience with cameras in the courtroom, some media attorneys are hoping that the trial prompt the Minnesota Supreme Court to change the rules in the future. Cahill's full order is available online at: https://z.umn.edu/6z8q.

On June 18, the Minnesota Supreme Court issued an order to the Advisory Committee for the Rules of Criminal Procedure to re-evaluate the current rules about coverage of criminal proceedings and "consider whether the requirements set forth in that rule for audio and video coverage of criminal proceedings should be modified or expanded." A copy of the Minnesota Supreme Court's order is available online at: https://z.umn.edu/6z8s.

Background

Rule 4 of the Minnesota General Rules of Practice allows media cameras to record most criminal proceedings only when the defense, prosecution, and judge agree. Minn. Gen. R. Prac. 4.01 *et seq*. The Minnesota Supreme Court enacted the rule in 2018. (For more information about the evolution of cameras in Minnesota courtrooms, see "Minnesota Supreme Court Allows Audio and Video Recordings in Some Portions of Criminal Cases" in the Summer 2018 issue of the Silha *Bulletin*.) Neighboring states like Iowa and Wisconsin have televised trials previously, but the U.S. Supreme Court has not articulated a national standard, according to the St. Paul *Pioneer Press* on May 1.

In this case, Chauvin initially agreed to cameras, but the prosecution opposed them. In his Nov. 4, 2020 order, Cahill invoked both the defendant's Sixth Amendment right to a public trial and the First Amendment right of the public and the press to access the trial. Cahill specifically addressed Rule 4 in his order. "Normally, this rule can be applied without concern that it will impinge on the right to a public trial or the right of access held by the public and press," Cahill wrote. "Spectators may freely attend trials, and the usual trial receives little attention, except from family and friends of the victim or the defendant and the Court can easily accommodate those wishing to attend the trial in person. On occasion, members of the media attend and report on the proceedings." But due to the COVID-19 pandemic, Cahill wrote, televising the trial could allow for meaningful public access while respecting social distancing guidelines. A copy of Cahill's order is available online at: https://z.umn.edu/6z8t.

After Cahill's initial order allowing recording, Minnesota Assistant Attorney General Matthew Frank filed a motion to reconsider. "The risks of broadcasting witness testimony are particularly acute, where, as here, live video and audio coverage may be intimidating to some witnesses and make it less likely that they will testify, potentially interfering with a fair trial," Frank wrote in his November 25 filing. A copy of the state's filing is available online at: https://z.umn.edu/6z8u.

On December 14, a coalition of media organizations represented by Ballard Spahr attorneys filed a memorandum opposing the prosecution's motion to reconsider. The Silha Center for the Study of Media Ethics and Law was part of the coalition. "The Court rightly held that, given the enormous public interest in this trial, the limitations imposed by the pandemic, and the options created by modern technology, meaningful access equates to remote access," the filing read. A copy of the media coalition's filing is available online at: https://z.umn.edu/6z8v.

On December 18, Cahill issued an order denying the State's motion to reconsider and amend the initial media plan. A copy of that order is available online at: https://z.umn.edu/6z8w.

Positive Results Build Momentum for Increased Press Access

Court TV — which provided gavel-to-gavel coverage of the O.J. Simpson trial — was the designated pool camera starting three weeks before the trial, according to a memo from Minnesota's Fourth Judicial District on Feb. 16, 2021. A full copy of the memo

is available at: https://www.mncourts.gov/mncourtsgov/media/High-Profile-Cases/27-CR-20-12646/MediaUpdate.pdf. Data from Nielsen show that more than 23 million Americans watched the trial on television, and even more people watched on their laptops or cellphones.

The broadcast feed gave the public insight into the often-mundane happenings of the justice system.

"For me, it's an affirmation of how ordinary this is," Jane E. Kirtley, Silha Professor of Media Ethics and Law and Director of the Silha Center told the Minneapolis *Star Tribune* on March 19. "The cameras are having no impact on what's happening in the courtroom."

The fact that the cameras did not significantly affect the trial could be important. "I think it will eliminate the argument that cameras are inherently disruptive," Kirtley told the *Star Tribune*. "There will be a great deal of pressure on government entities to continue this level of access."

Hennepin County District Chief Judge Toddrick Barnette told Minnesota Public Radio (MPR) on April 29 that he was initially skeptical about allowing cameras in the courtroom but was reassured through working with journalists. "Over time, I felt more comfortable that they were really interested in the integrity of the process and worked very hard to make sure there were no violations of Judge Cahill's order," Barnette said.

Retired Hennepin County District Judge Kevin Burke told KSTP-TV, the Twin Cities' ABC affiliate, on April 22 that the process of allowing cameras in the courtroom "went perfect" and "gave the public the right to be there, to see what happened and to make judgments themselves about the ultimate verdict."

On June 24, Burke published an op-ed with reporter-turned-lawyer Elizabeth Stawicki in the *Pioneer Press* arguing for increased camera access to future criminal trials. "Opponents have long argued that cameras would taint the legal process and deny defendants fair trials: jurors would be reluctant to serve; judges and attorneys would grandstand; and witnesses would be afraid to testify. That didn't happen in the Chauvin trial — jury selection wrapped up early; the judge controlled the courtroom; and witnesses testified," the op-ed read.

After the conviction, Minnesota Attorney General Keith Ellison told KMSP-TV, the Twin Cities' Fox affiliate, that he had reconsidered his initial stance. "Look, you know, we all watch reality TV shows, that was one thing I was really worried about," he told the station April 28. "I didn't want this trial to be a reality show. I wanted this trial to be a pursuit of the truth and I was worried cameras might interfere with that goal. But it turned out, it worked better than I thought, so I'll say, I can be wrong, I guess I was a little bit."

> "The cameras are having no impact on what's happening in the courtroom.. . . There will be a great deal of pressure on government entities to continue this level of access."
>
> **— Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law**

In an interview with Silha Research Assistant Claire Colby on June 16, attorney Leita Walker said that the media coalition she represented was generally "really, really happy" with the level of access granted. "The camera access itself was all they could have ever asked for — it was not only gavel to gavel, every second of open court, but it was livestreamed as opposed to some sort of delayed, televised rebroadcast," Walker said.

As stipulated in Cahill's order, cameras were turned off for jury selection and for testimony of minor witnesses.

"I think the media probably always wants the cameras on for everything, but there was generally an understanding of why the court was limiting video, but not audio coverage of those portions," Walker said.

Allowing cameras in court was an overall positive experience, she said. "I think this was an example of where the court really collaborated closely with the press and in a way that allowed the public to see justice unfold in a very, very important case," Walker said. "There were no moments where I think anyone regretted camera access. It wasn't disruptive, it didn't create the so-called media circus."

Though the pandemic was cited as a major reason for televising this trial, Walker said she hopes the success of this trial will influence future cases. "We have to get the rule changed, and we're working on that with the Supreme Court," Walker said. "And I think you'll see a movement to ask the court to change Rule 4 because without that change, any prosecutor, any defense attorney can keep cameras out of courts."

On August 4, Walker filed a motion on behalf of the Media Coalition asking the court to unseal juror identities and "other juror information, including the prospective juror list, juror profiles, juror questionnaires and the original verdict forms." A full copy of the motion is available online at: https://mncourts.gov/mncourtsgov/media/High-Profile-Cases/27-CR-20-12646/Memorandum08042021.pdf.

Mitchell Hamline law professor Kate Kruse told the *Pioneer Press* on May 1 that the livestreaming of Chauvin's trial could make it difficult to find impartial jurors for the March 2022 trial of the three other former police officers. The federal civil rights case against Chauvin and his co-defendants "apparently will not be televised or livestreamed," because of strict federal court bans on audio or video presence in federal trial courts, according to *MinnPost* on May 18.

For more information on camera access in the Chauvin trial, see *Judge Allows Audio-Video Recording, Livestreaming of Trial* in "Court Access and Medical Privacy Issues Arise in Wake of George Floyd Killing" in the Fall 2020 issue of the Silha *Bulletin*.

— Claire Colby
Silha Research Assistant

Associated Press, *ProPublica*, and Well-Known Journalists Raise Ethical Questions and Considerations

ETHICS

In the spring and early summer of 2021, questions were raised about the ethics of several news reports and decisions by journalists and news organizations. The Associated Press (AP) fired a reporter for her tweets on the Israel-Palestine conflict after she faced a deluge of right-wing harassment online; *New York Times* op-ed columnist David Brooks' financial ties to Facebook were unveiled; CNN anchor Chris Cuomo was discovered to have advised his elder brother, Andrew Cuomo, as the Governor of New York, who faced sexual assault allegations earlier this year; and *ProPublica* published the tax information of some of the wealthiest Americans after an anonymous source leaked the verified documents to the outlet.

Associated Press Fires Reporter Emily Wilder

On May 19, 2021, the Associated Press (AP) fired one of its reporters, Emily Wilder, after her pro-Palestine college activism at Stanford University and tweets critical of Israel became the target of a right-wing social media take-down. Wilder had started working as an AP Associate in Phoenix, Ariz., just three weeks prior. The dismissal occurred in the context of escalating conflict between Israel and Palestine. The AP claimed Wilder had violated its social media policies, but some commentators alleged that the news outlet had succumbed to what they characterized as a disinformation campaign helmed by college students.

The controversy began on May 17, when the Stanford College Republicans student group alleged on Twitter that Wilder, who is Jewish, is an "anti-Israel agitator" and highlighted her college activism. Two days later, the AP fired Wilder.

The AP alleged that Wilder violated its social media policy during the three weeks of her employment, but the company did not elaborate on which of Wilder's tweets actually violated it. "Emily Wilder was let go because she had a series of social media posts that showed a clear bias toward one side and against another in one of the most divisive and difficult stories we cover," Brian Carovillano, the AP's managing editor, told CNN on May 30, 2021. Wilder was not in a reporting position at the AP, Carovillano added, and her position did not involve covering international news.

The AP further alleged Wilder put other AP journalists in danger because her tweets could suggest that the AP takes sides and its reporters in war zones would be targets. "It's really important that we maintain our credibility on these stories," Carovillano told CNN. "Journalists' safety is at stake and the AP's credibility is at stake. Our credibility is constantly under attack. Our social media guidelines exist to protect that credibility, because protecting our credibility is the same as protecting journalists."

> "Particularly in an era when operations like Project Veritas exist in part to try to discredit the mainstream media and as hack-and-leak operations become more common, it is especially urgent that news organizations prove they understand the threat and develop a plan to cope with it."
>
> **— Janine Zacharia, Stanford University Department of Communication Carlos Kelly McClatchy lecturer**

Wilder, however, said in a statement on May 22, 2021, that she feels she is "one victim to the asymmetrical enforcement of rules around objectivity and social media that has censored so many journalists — particularly Palestinian journalists and other journalists of color — before me." Wilder's statement is available online at: https://z.umn.edu/70ev.

More than 100 AP employees signed an open letter criticizing Wilder's firing. "Wilder was a young journalist, unnecessarily harmed by the AP's handling and announcement of its firing of her," the employees wrote. "We need to know that the AP would stand behind and provide resources to journalists who are the subject of smear campaigns and online harassment. As journalists who cover contentious subjects, we are often the target of people unhappy with scrutiny. What happens when they orchestrate a smear campaign targeting another one of us? Interest groups are celebrating their victory and turning their sights on more AP journalists. They have routinely made journalists' identities subject to attack. Once we decide to play this game on the terms of those acting in bad faith, we can't win." A copy of the letter is available online at: https://z.umn.edu/70ew.

Margaret Sullivan, writing for *The Washington Post* on May 27, 2021, opined that Wilder's firing is a cautionary tale of what happens when bad-faith attacks are taken at face value. "News organizations need to do much more," Sullivan wrote. "They might start by revisiting the Gamergate controversy in 2014, the nightmarish campaign of misogynistic stalking and grievance-driven harassment against female video game journalists and other women in that industry. The journalists who have been targeted by these kinds of attacks — especially women and people of color — best understand the insidious techniques, vile motivations and health-threatening repercussions."

Janine Zacharia, writing for *Politico* on May 26, 2021, argued that the AP "essentially caved" to a disinformation campaign against one of its journalists. "Wilder's dismissal has emboldened those who aim to harm our most important journalistic institutions at a time when restoring respect for fact-based news is paramount for sustaining democracy," Zacharia contended.

Zacharia further elaborated that she personally spent two years as part of a Stanford working group studying the way actors use information warfare for political purposes. The working group, Zacharia wrote, looked to the AP's practices in developing a playbook on how to handle situations involving propaganda. And yet, Zacharia contended, "the AP's firing of Wilder demonstrates that managers there have not yet digested the threat of disingenuous campaigns even against their own employees. Particularly in an era when operations like Project

Veritas exist in part to try to discredit the mainstream media and as hack-and-leak operations become more common, it is especially urgent that news organizations prove they understand the threat and develop a plan to cope with it."

David Brooks Failed to Disclose Facebook Monetary Ties

On March 3, 2021, *Buzzfeed News* reported that David Brooks, a *New York Times* columnist, had been earning a second salary through a nonprofit partly funded by Facebook, yet Brooks had not disclosed this affiliation in any of his columns, including those that promoted the nonprofit's work.

Multiple news organizations reported that Brooks' work on an initiative called Weave, which is affiliated with the Aspen Institute, aims to combat social isolation and build communities of "weavers" who are supposed to bring together disparate groups in the social fabric of society. Brooks has written about Weave on numerous occasions in the *Times*, even going so far as to promote one of its events and then reporting on it later after attending it himself.

The *Times* refused to confirm whether it knew Brooks was on the Aspen Institute's payroll, or whether it knew the Weave project was ultimately funded by Facebook. A *Times* spokesperson, Eileen Murphy, told *Buzzfeed* after it broke the story that the *Times* would evaluate Brooks' ties and whether they should be disclosed in future columns.

On March 5, Brooks appeared on "PBS NewsHour." When asked if he was rethinking his decision not to disclose this funding relationship, Brooks refuted the allegation that he failed to disclose his relationship with Facebook. Brooks said, "We did totally disclose it. Everything has been public. First, the Times completely was informed when I started Weave [as to] what it was going to be and how I was going to get compensated by Aspen. Second, the Aspen Institute is completely transparent about who the donors are, and so we released the donors. Third, since I started Weave in 2018, I have not meaningfully written about any organization or individual who has supported us, including Facebook.. . . Fourth, I do understand the concerns, and . . . I want to be beyond question, and so we're going to make some changes."

Ultimately, Brooks resigned from his paid role at the Aspen Institute, and disclosures were added to all past stories he had written about the project, according to a *New York Times* statement from March 6, 2021. The statement went on to explain that Brooks' previous editors were aware of his ties to Facebook, but after a managerial transition on the editorial staff his current editors were not. After *Buzzfeed*'s reporting, the editorial team concluded that the setup presented conflicts of interest. Though he did resign from the paid role, the statement said Brooks would maintain his volunteer position at the institute.

Commentators said they were surprised by Brooks' apparent disregard for such a basic tenet of professional journalism. In *The Washington Post* on March 4, 2021, Patrick Lee Plaisance, the editor of the *Journal of Media Ethics* and a communications professor at Pennsylvania State University, said Brooks' "failure to disclose [his compensation] undermines a reader's ability to assess his claims" and it also damages the overall credibility of the *Times*, which readers expect to act transparently.

Jan Schaffer, executive director of J-Lab: The Institute for Interactive Journalism and former ombudsman of the Corporation for Public Broadcasting (CPB), wrote on March 8, 2021 that the trend of celebrity journalists holding multiple paid gigs is "disturbing." "And it's mystifying how journalists — in this era of 24/7 news developments — can manage to report and produce breaking news while also being a regular talking head on various news programs," Schaffer wrote.

Chris Cuomo Advises Andrew Cuomo on How to Respond to Sexual Assault Allegations

In the first half of 2021, CNN anchor Chris Cuomo joined numerous strategy calls with his older brother, New York Gov. Andrew Cuomo, as the elder Cuomo faced multiple sexual assault allegations, according to *The Washington Post* on May 21, 2021. Reportedly, Chris Cuomo advised Andrew Cuomo not to resign from office and instead to take a defiant stance. Chris Cuomo also invoked "cancel culture" as a reason to hold firm against the allegations.

According to the *Post*, CNN later acknowledged in a statement that Chris Cuomo's involvement in the strategy sessions was a mistake. "Chris has not been involved in CNN's extensive coverage of the allegations against Governor Cuomo — on air or behind the scenes," the network said. "In part because, as he has said on his show, he could never be objective. But also because he often serves as a sounding board for his brother.. . . However, it was inappropriate to engage in conversations that included members of the Governor's staff, which Chris acknowledges. He will not participate in such conversations going forward." CNN said it would not discipline Chris for his actions.

Chris Cuomo offered an on-air apology to viewers on May 20, 2021, saying he has a unique obligation to journalistic integrity and to his family. "It was a mistake because I put my colleagues here, who I believe are the best in the business, in a bad spot," Cuomo said. But he went further to say he is still going to prioritize his family, and that he knows where the ethical line is. The video recording of the on-air apology is available online at: https://z.umn.edu/74b7.

Erik Wemple, writing for *The Washington Post* on May 20, 2021, was skeptical of Chris Cuomo's apology. "The reason that Chris Cuomo 'acknowledges' that it was inappropriate to advise his brother in strategy sessions is because, well, he got caught violating one of journalism's clearest ethical red lines," Wemple wrote. "He gets no credit for acknowledging the transgression, and how are we to trust the pledge not to backslide?"

Tom Jones, writing for *Poynter* on May 20, 2021, emphasized the egregiousness of Cuomo's actions. "The host of a primetime show on one of the country's biggest and most influential cable news networks is advising one of the most powerful and influential politicians in this country on how to handle serious sexual misconduct allegations," Jones wrote. And when Chris Cuomo hosted Andrew Cuomo on CNN's primetime evening slot throughout the COVID-19 pandemic, Jones asserted, the network could have predicted the lines would get blurry. "CNN should've seen all this coming, and now it has to live with the consequences — which is some viewers not being able to trust a major personality on its network," he wrote.

Heidi Stevens, writing for the *Chicago Tribune* on May 26, 2021, said that "CNN is walking an uncomfortable line here. By choosing not to discipline Chris Cuomo, they're making it hard for viewers to trust that the network's reports and analysis are uncompromised by employees'

Ethical Questions, *continued on page 10*

Ethical Questions, *continued from page 9*

personal connections." And when that trust erodes either by inaction or choice, Stevens wrote, "once it's gone, [it] is incredibly difficult to win back."

On Aug. 8, 2021, CNN Chief Media Correspondent Brian Stelter commented on the scandal and appeared to defend Chris Cuomo. During a monologue on his program, "Reliable Sources," Stelter said, "This has been a conundrum for CNN that has no perfect answer, no perfect solution. Some think CNN made it worse by letting Chris interview his brother when COVID-19 was ravaging New York. But that was an unprecedented time period. And so is this one: A famous family in the news, a governor who soared to the highest heights last year now falling to the lowest lows — self-inflicted wounds — and a brother who just wants to do his job, just wants to anchor his show."

On Aug. 10, 2021, Andrew Cuomo announced that he would resign as New York's governor. The decision came after the New York State Attorney General issued a report concluding that Cuomo "sexually harassed nearly a dozen women, including current and former government workers, by engaging in unwanted touching and making inappropriate comments," and that both he and his aides "unlawfully retaliated against at least one of the women for making her complaints public and fostered a toxic work environment," *The New York Times* reported on Aug. 11, 2021.

ProPublica Publishes Taxes of the Wealthiest in America

On June 8, 2021, *ProPublica* published a series of articles on how much the wealthiest Americans pay in taxes each year. The outlet expected people to question the ethics of such a move, and its lead editors published an explainer, writing, "Many will ask about the ethics of publishing such private data. We are doing so — quite selectively and carefully — because we believe it serves the public interest in fundamental ways, allowing readers to see patterns that were until now hidden." *ProPublica*'s explainer is available online at: https://z.umn.edu/70et.

ProPublica aimed to reveal just how inequitable the tax code is, and where it can be changed to better reflect Americans' priorities as the Biden Administration looks to levy funds for social programs in the next three years. "The secret tax files offer new, factual evidence for lawmakers considering such changes: Should the biggest winners in America's epochal concentration of wealth over the last 40 years be permitted to pay levies of considerably less than 37%?" *ProPublica*'s editors wrote.

The outlet acknowledged that whoever leaked the trove of information to it may have had bad motives for doing so. "We do not know the identity of our source," the editors wrote. "We did not solicit the information they sent us. The source says they were motivated by our previous coverage of issues surrounding the IRS and tax enforcement, but we do not know for certain that is true. We have considered the possibility that information we have received could have come from a state actor hostile to American interests."

ProPublica acknowledged publication of the tax information may have violated federal law. The news outlet wrote, "A federal law ostensibly makes it a criminal offense to disclose tax return information. But we do not believe that law would be constitutional if applied to bar or sanction publication of a story in the public interest when the news organization did not itself remove the information from the control of the IRS or solicit anyone else to do so — as we did not. And this is not our first experience with this law." *ProPublica* did not reference the particular law at issue, but the outlet may have been referring to 26 U.S.C. § 7213(a)(3), which states, in relevant part: "It shall be unlawful for any person to whom any return or return information . . . is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information." Violation of this provision is a felony and may be punished by a fine of up to $5,000, up to 5 years in prison, or both.

However, legal experts believe this publication prohibition is unconstitutional as a violation of the First Amendment when a news outlet has obtained the information lawfully and the information is a matter of public concern. Writing about the statute on March 3, 2017, *New York Times* Supreme Court Correspondent Adam Liptak said the publication prohibition "is almost certainly unconstitutional." That is because the Supreme Court has found that "journalists are free to publish truthful information on matters of public concern notwithstanding laws to the contrary as long as they did nothing illegal in obtaining the information," Liptak wrote. One such case is *Bartnicki v. Vopper*, 532 U.S. 514 (2001), in which the Court found that the First Amendment allowed a Pennsylvania radio station to air a surreptitious recording of a phone call. The call participants were officials involved in collective-bargaining negotiations at a Pennsylvania school district, and the radio station had received the recording unsolicited. A federal law — 18 U.S.C. § 2511(1)(c) — makes it illegal for any person to "intentionally disclose[], or endeavor[] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." The Court held in *Bartnicki* that the First Amendment protected the radio station's airing of the recording because the radio station did not take part in the illegal interception of the phone call and the content of the recording was a matter of public concern. Further, the *Bartnicki* Court reasoned, enforcement of the federal statute at issue "implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern." (For more information on the *Bartnicki* case, see "Silha Lecture 2001 To Focus on *Bartnicki v. Vopper*" in the Spring 2001 Silha *Bulletin*; "U.S. Supreme Court Rules In Historic *Bartnicki* Case" in the Summer 2001 issue; and "*Bartnicki v. Vopper* Topic of Sixteenth Annual Silha Lecture" in the Fall 2001 issue.)

Tom Jones, writing for *Poynter* on June 9, 2021, argued the journalistic value outweighed the risk. "ProPublica does show, in detail, why we should at least examine how taxes work for the rich," Jones wrote. "And that gives its investigation journalistic value."

Jeremy Barr, writing for *The Washington Post* on June 8, 2021, observed that media organizations generally "prefer to know who is sending source material to have a better grasp of the authenticity of the material, the way in which it was obtained and the motivations of the sender. But, in this case, some journalists praised ProPublica for focusing on the veracity of the documents as the primary factor in deciding to publish, not the identity of the source."

— Samantha Brunn
Silha Research Assistant

Special Report: U.S. Supreme Court Rulings and Opinions Raise Numerous Freedom of Speech and Press, Privacy Issues and Questions

In 2021, the U.S. Supreme Court issued several important opinions implicating freedom of speech and press, as well as data privacy and security.

- On June 23, 2021, the Court, in *Mahanoy Area School District v. B.L.*, ruled in favor of a Pennsylvania student after she was suspended from her high school junior varsity cheerleading squad for two vulgar Snapchat posts, holding that the suspension violated her First Amendment rights.

SPECIAL REPORT

- On July 2, 2021, Justices Clarence Thomas and Neil Gorsuch wrote separate dissenting opinions from the Court's denial of *certiorari* in *Berisha v. Lawson*, in which they called for the reevaluation of the actual malice standard originating in the Court's landmark ruling in *New York Times v. Sullivan*, 376 U.S. 254 (1964).
- On March 4, 2021, the Supreme Court held in *United States Fish and Wildlife v. Sierra Club, Inc.* that a federal administrative agency's predecisional, deliberative draft biological opinions are protected from disclosure under Exemption 5 of the Freedom of Information Act (FOIA) even if the relevant records reflect the agency's final views on a proposal.
- On April 1, 2021, the Supreme Court held in *Facebook, Inc. v. Duguid* that the Telephone Consumer Protection Act of 1991's (TCPA) definition of an "automatic telephone dialing system" (ATDS) does not apply to devices that only have the capacity to store numbers and dial them automatically, resolving a federal circuit court split. The ruling resolved a circuit court split regarding the ATDS definition, raising implications for future litigation and enforcement.
- On April 22, 2021, in *AMG Capital Management, LLC v. Federal Trade Commission*, the Supreme Court ruled that the Federal Trade Commission Act, specifically the section authorizing the Federal Trade Commission (FTC) to seek injunctive relief in unfair and deceptive trade practice cases, does not authorize the agency to impose monetary relief or order courts to collect it.
- On June 25, 2021, the Supreme Court held in *TransUnion v. Ramirez* that a "risk of future harm" was insufficient to grant standing under Article III of the U.S. Constitution for class action lawsuits, providing at least some clarity to its previous ruling in *Spokeo v. Robins*, 578 U.S. 330 (2016).
- On June 3, 2021, the U.S. Supreme Court held in *Van Buren v. United States* that an individual who uses valid access and log-in credentials to obtain information from a computer system does not violate the Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030(a)(2) (2017), even if the individual accessed the information for a prohibited purpose.

Supreme Court Rules in Favor of Student in Latest Student Speech Case

On June 23, 2021, the U.S. Supreme Court held that the Mahanoy Area School District in Pennsylvania violated student Brandi Levy's First Amendment rights by suspending her from an extracurricular team after she posted vulgar language and gestures criticizing her high school and extracurricular activities on social media. *Mahanoy Area School District v. B.L.*, 141 S.Ct. 2038 (2021). Following the ruling, those involved in the case and observers expressed mixed emotions about the ruling, calling it an important First Amendment victory, especially for Levy, but one that did not preclude the possibility of restricting students' off-campus speech in the future.

The case arose when Levy, a student at Mahanoy Area High School, tried out for her school's varsity cheerleading squad and a private softball team. Levy did not make the varsity cheerleading team and also did not get her preferred softball position, instead being named to the junior varsity cheerleading team. Levy summarily posted two photos on Snapchat, a social media application. The first photo depicted Levy and one of her friends with their middle fingers raised with the caption, "Fuck school fuck softball fuck cheer fuck everything." The second photo was blank, but had the caption, "Love how me and [another student] get told we need a year of jv before we make varsity but tha[t] doesn't matter to anyone else?"

Several students at Mahanoy Area High School saw the photos, which quickly spread to other members of the cheerleading squad, some of whom shared them with the cheerleading coaches after being "visibly upset" about the posts. The photos were the topic of at least one class taught by one of the cheerleading coaches.

The coaches, after discussing the matter with the school principal, concluded that the posts contained profanity in connection with an extracurricular activity, therefore violating team and school rules. The coaches summarily suspended Levy from the junior varsity team for the upcoming year, despite apologies from Levy. The school's athletic director, principal, superintendent, and school board all affirmed the suspension.

The U.S. District Court for the Middle District of Pennsylvania ruled in Levy's favor, finding that the social media posts had not caused "substantial disruption" at the school. *B.L. v. Mahanoy Area School District*, 289 F.Supp.3d 607 (M.D. Penn. 2017). In reaching this finding, the court applied *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969), in which the Supreme Court held that students do not "shed their constitutional rights to freedom of speech or expression," even "at the schoolhouse gate." However, the Court also held in *Tinker* that schools have a special interest in regulating speech that "materially disrupts classwork or involves substantial disorder or invasion of the rights of others."

The U.S. Court of Appeals for the Third Circuit affirmed the district court, holding that *Tinker* established that a public school cannot constitutionally prohibit peaceful student political demonstration consisting of "pure speech" on school property during the school day. *B.L. v. Mahanoy Area School District*, 964 F.3d 170 (3rd Cir.

SCOTUS Rulings, *continued on page 12*

SCOTUS Rulings, *continued from page 11*
2020). The court emphasized that there was no evidence that the protest would "substantially interfere with the work of the school or impinge upon the rights of other students." However, the court also noted that "conduct by [a] student, in class or out of it, which for any reason—whether it stems from time, place, or type of behavior—materially disrupts classwork or involves substantial disorder or invasion of the rights of others is . . . not immunized by the constitutional guarantee of freedom of speech."

In his majority opinion for the 8-1 Supreme Court, Justice Stephen Breyer first noted that "[m]any courts have taken this statement as setting a standard — a standard that allows schools considerable freedom on campus to discipline students for conduct that the First Amendment might otherwise protect." However, he noted that the Third Circuit "held that this additional freedom did 'not apply to off-campus speech,' which it defined as 'speech that is outside school-owned, -operated, or -supervised channels and that is not reasonably interpreted as bearing the school's imprimatur.'" The Third Circuit therefore used this reasoning to conclude that the school consequently could not discipline Levy for her speech.

Second, Justice Breyer detailed "three specific categories of student speech that schools may regulate in certain circumstances: (1) "indecent," "lewd," or "vulgar" speech uttered during a school assembly on school grounds; (2) speech, uttered during a class trip, that promotes "illegal drug use"; and (3) speech that others may reasonably perceive as "bear[ing] the imprimatur of the school," such as that appearing in a school-sponsored newspaper[.]" Justice Breyer cited *Bethel School District No. 403 v. Fraser*, 478 U.S. 675, 684 (1986); *Morse v. Frederick*, 551 U.S. 393, 409 (2007); and *Hazelwood School District v. Kuhlmeier*, 484 U.S. 260, 266 (1988), respectively. (For more information on *Morse*, see "In *Morse v. Frederick*, Court Places Limits on Student Expression" in the Summer 2007 issue of the Silha *Bulletin*.)

Third, Justice Breyer held that "the special characteristics that give schools additional license to regulate student speech always disappear when a school regulates speech that takes place off campus." He added, "The school's regulatory interests remain significant in some off-campus circumstances." Justice Breyer included several examples, including "serious or severe bullying or harassment targeting particular individuals; threats aimed at teachers or other students; the failure to follow rules concerning lessons, the writing of papers, the use of computers, or participation in other online school activities; and breaches of school security devices, including material maintained within school computers."

> "It might be tempting to dismiss B.L.'s words as unworthy of the robust First Amendment protections discussed herein. But sometimes it is necessary to protect the superfluous in order to preserve the necessary."
>
> **— U.S. Supreme Court Justice Stephen Breyer**

Justice Breyer declined to "set forth a broad, highly general First Amendment rule stating just what counts as 'off campus' speech and whether or how ordinary First Amendment standards must give way off campus to a school's special need to prevent, e.g., substantial disruption of learning-related activities or the protection of those who make up a school community." He therefore rejected the Third Circuit's standard, finding that the court's ruling "basically, if not entirely, would deny the off-campus applicability of *Tinker*'s highly general statement about the nature of a school's special interests."

Justice Breyer added that the Supreme Court was "uncertain as to the length or content of any such list of appropriate exceptions or carveouts to the Third Circuit majority's rule" and that the Court "hesitate[d] to determine precisely which of many school-related off-campus activities belong on such a list." He continued, "Neither do we now know how such a list might vary, depending upon a student's age, the nature of the school's off-campus activity, or the impact upon the school itself."

Instead, Justice Breyer named "three features of off-campus speech that often, even if not always, distinguish schools' efforts to regulate that speech from their efforts to regulate on-campus speech." The first feature is that "a school, in relation to off-campus speech, will rarely stand *in loco parentis*," meaning "off-campus speech will normally fall within the zone of parental, rather than school-related, responsibility."

The second feature was that "from the student speaker's perspective, regulations of off-campus speech, when coupled with regulations of on-campus speech, include all the speech a student utters during the full 24-hour day." Justice Breyer noted that the result was that "courts must be more skeptical of a school's efforts to regulate off-campus speech, for doing so may mean the student cannot engage in that kind of speech at all," including protected political and religious speech.

The final feature was that a "school itself has an interest in protecting a student's unpopular expression, especially when the expression takes place off campus." Here, Justice Breyer wrote that "America's public schools are the nurseries of democracy." He continued, "Our representative democracy only works if we protect the 'marketplace of ideas.' This free exchange facilitates an informed public opinion, which, when transmitted to lawmakers, helps produce laws that reflect the People's will. That protection must include the protection of unpopular ideas, for popular ideas have less need for protection. Thus, schools have a strong interest in ensuring that future generations understand the workings in practice of the well-known aphorism, 'I disapprove of what you say, but I will defend to the death your right to say it.'"

Finally, Justice Breyer turned to Levy's speech. He concluded that Levy's posts amounted to criticism "of the team, the team's coaches, and the school — in a word or two, criticism of the rules of a community of which [Levy] forms a part." It therefore "did not involve features that would place it outside the First Amendment's ordinary protection," including fighting words or obscenity. Instead, her posts amounted to "the kind of pure speech to which, were she an adult, the First Amendment would provide strong protection."

Justice Breyer also emphasized "when, where, and how [Levy] spoke," namely "outside of school hours from a location outside the school." He continued, "She did not identify the school in her posts or target any member of the school community with vulgar or abusive language. [Levy] also transmitted her speech through a personal cellphone, to an audience consisting of her private circle of Snapchat friends." Justice Breyer concluded that "[t]hese features of her speech, while risking transmission to the school itself, nonetheless . . . diminish the school's interest in punishing [Levy's] utterance."

Justice Breyer turned to the school's interests in punishing Levy's speech, which he broke into three parts. The first part was "the school's interest in teaching good manners and consequently in punishing the use of vulgar language aimed at part of the school community." Justice Breyer added that "the school has presented no evidence of any general effort to prevent students from using vulgarity outside the classroom." He further found that "[t]he strength of this anti-vulgarity interest is weakened considerably by the fact that [Levy] spoke outside the school on her own time." He further found that the school "did not stand *in loco parentis*" because there was "no reason to believe [Levy's] parents had delegated to school officials their own control of [her] behavior [in posting the Snapchat photos]."

The second part of the school's interests was "trying to prevent disruption, if not within the classroom, then within the bounds of a school-sponsored extracurricular activity." Justice Breyer dismissed this argument, writing that the Court found "no evidence in the record of the sort of 'substantial disruption' of a school activity or a threatened harm to the rights of others that might justify the school's action," citing *Tinker*. Instead, Justice Breyer noted that "the record shows that discussion of the matter took, at most, 5 to 10 minutes of an Algebra class 'for just a couple of days' and that some members of the cheerleading team were 'upset' about the content of [Levy's] Snapchats."

The third and final part of the school's interests was "a concern for team morale." Once again, Justice Breyer concluded that there was insufficient evidence to support this claim, writing that there was little that demonstrated "any serious decline in team morale — to the point where it could create a substantial interference in, or disruption of, the school's efforts to maintain team cohesion."

Justice Breyer concluded by writing, "It might be tempting to dismiss B. L.'s words as unworthy of the robust First Amendment protections discussed herein. But sometimes it is necessary to protect the superfluous in order to preserve the necessary." He therefore affirmed the Third Circuit's ruling, though he noted that the Supreme Court did "not agree with the reasoning of the Third Circuit's panel majority."

> "Protecting young people's free speech rights when they are outside of school is vital, and this is a huge victory for the free speech rights of millions of students who attend our nation's public schools."
>
> **— David Cole, American Civil Liberties Union legal director**

In a concurring opinion, Justice Samuel Alito, joined by Justice Neil Gorsuch, wrote that because "[t]his is the first case in which we have considered the constitutionality of a public school's attempt to regulate true off-premises student speech," it was therefore "important that our opinion not be misunderstood." Justice Alito agreed with the majority on several grounds, including that:

- "the First Amendment permits public schools to regulate some student speech that does not occur on school premises during the regular school day;
- this authority is more limited than the authority that schools exercise with respect to on-premises speech;
- courts should be 'skeptical' about the constitutionality of the regulation of off-premises speech;
- the doctrine of *in loco parentis* 'rarely' applies to off-premises speech;
- public school students, like all other Americans, have the right to express 'unpopular' ideas on public issues, even when those ideas are expressed in language that some find 'inappropriate' or 'hurtful';
- public schools have the duty to teach students that freedom of speech, including unpopular speech, is essential to our form of self-government;
- the Mahanoy Area High School violated B. L.'s First Amendment rights when it punished her for the messages she posted on her own time while away from school premises;
- and the judgment of the Third Circuit must therefore be affirmed."

Justice Alito also agreed "that it is not prudent for us to attempt at this time to 'set forth a broad, highly general First Amendment rule' governing all off-premises speech." However, his lengthy opinion detailed "the framework within which efforts to regulate off-premises speech should be analyzed," including discussing *Tinker*, *Fraser*, *Hazelwood*, *Morse*, and other cases.

Ultimately, Justice Alito concluded, "If today's decision teaches any lesson, it must be that the regulation of many types of off-premises student speech raises serious First Amendment concerns, and school officials should proceed cautiously before venturing into this territory."

In a dissenting opinion, Justice Clarence Thomas contended that "schools historically could discipline students in circumstances like those presented here. Because the majority does not attempt to explain why we should not apply this historical rule and does not attempt to tether its approach to anything stable, I respectfully dissent."

Justice Thomas first provided court precedent establishing that "although schools had less authority after a student returned home, it was well settled that they still could discipline students for off-campus speech or conduct that had a proximate tendency to harm the school environment."

Second, Justice Thomas wrote that "[i]f there is a good constitutional reason to depart from this historical rule, the majority and the parties fail to identify it." He therefore applied a new "rule": "Assuming that [Levy's] speech occurred off campus, the purpose and effect of [Levy's] speech was 'to degrade the [program and cheerleading staff]' in front of 'other pupils,' thus having 'a direct and immediate tendency to . . . subvert the [cheerleading coach's] authority.'" Justice Thomas therefore reasoned that "the coach had authority to discipline [Levy]."

SCOTUS Rulings, *continued on page 14*

SCOTUS Rulings, *continued from page 13*

Finally, Justice Thomas concluded that "[t]he larger problem facing us today is that our student-speech cases are untethered from any textual or historical foundation," including that "[t]he Court's failure to explain itself in *Tinker* needlessly makes this case more difficult."

The Supreme Court's full ruling is available online at: https://www.supremecourt.gov/opinions/20pdf/20-255_g3bi.pdf.

Following the ruling, those involved in the case, as well as observers, expressed mixed opinions about who ultimately won. Levy said in a statement that her school "went too far, and I'm glad that the Supreme Court agrees." She added, "I was frustrated, I was 14 years old, and I expressed my frustration the way teenagers do today. Young people need to have the ability to express themselves without worrying about being punished when they get to school."

In a separate statement, David Cole, legal director for the American Civil Liberties Union (ACLU), which represented Levy called the decision "a huge victory for students' speech rights.. . . It means that when students leave school every day, they don't have to carry the schoolhouse on their backs." He added, "Protecting young people's free speech rights when they are outside of school is vital, and this is a huge victory for the free speech rights of millions of students who attend our nation's public schools."

Attorney Michael Levin, who represented the Mahanoy Area School District, argued that the Supreme Court "clearly [ruled] that school districts had the right under the Constitution to regulate off-campus speech in a wide variety of situations." The school district added in a separate statement that the ruling marked an important vindication of schools' authority to protect students and staff and to fulfill schools' educational missions." Conversely, the Mahanoy Area School District superintendent asked, "Where is the line drawn?" in terms of schools being able to discipline students who break rules detailed in contracts they signed.

In a June 30, 2021 email to *Courthouse News*, Frank LoMonte, director of the Brechner Center for Freedom of Information at the University of Florida, called the ruling "enormously important for the safety and welfare of young people everywhere." He continued, "For years, schools have been claiming near-total authority over students' speech no matter when and where it happens, even off-campus on personal time, and the Third Circuit has now clearly said that there is a meaningful legal distinction between in-school speech and off-campus speech.. . . This is the only rule that can possibly make sense in today's world, where students are taking on leadership in social-justice movements and need the full force of the First Amendment to keep them safe from school punishment, even if they stir up controversy or provoke dissent."

In a June 23 interview with National Public Radio (NPR), Gregory Garre, the former solicitor general who represented the National School Boards Association in the case, called the decision a win for both sides, contending that although Levy won on the facts of the case, the high court rejected the notion that schools can never punish off-campus speech. "The court took a common-sense approach here," Garre said. "Just because speech originates off campus, particularly in a special context of social media, doesn't mean that it can't substantially disrupt the campus and the classroom."

Yale law professor Justin Driver called the decision "significant" in an interview with NPR, stating, "It's the first time in more than 50 years that a public school student has prevailed in a free speech case at the Supreme Court.. . . Public school students should be dancing in the streets." However, he also noted that the ruling "left many significant questions unanswered. And this suggests that the court is going to have another off-campus student speech case somewhere down the line."

Justices Thomas and Gorsuch Call for Reevaluation of *New York Times v. Sullivan* Standard

On July 2, 2021, Justices Clarence Thomas and Neil Gorsuch wrote separate dissenting opinions from the Court's denial of *certiorari* in *Berisha v. Lawson*, a defamation case dismissed on a summary judgment motion by the U.S. District Court for the Southern District of Florida, which was affirmed by the U.S. Court of Appeals for the Eleventh Circuit. *Berisha v. Lawson*, 973 F.3d 1304 (11th Cir. 2020), *cert. denied*, 141 S.Ct. 2424 (July 2, 2021).

Justices Gorsuch and Thomas called for the reevaluation of the actual malice standard, which was created in *New York Times v. Sullivan* in 1964 and requires proof that defendants knowingly made false statements or made statements with reckless disregard for their truth or falsity. 376 U.S. 254 (1964).

Justice Thomas previously called on the Supreme Court to revisit the actual malice standard in a concurring opinion filed in *McKee v. Cosby*, 139 S. Ct. 675 (2019) (Thomas, J., concurring in denial of certiorari) on Feb. 19, 2019. Justice Thomas wrote that he agreed with the Court's decision to deny *certiorari* in the case, but also contended that *Sullivan* and subsequent decisions extending the standard were "policy-driven decisions masquerading as constitutional law." Justice Thomas added, "There appears to be little historical evidence suggesting that the *New York Times* actual-malice rule flows from the original understanding of the First or Fourteenth Amendment." (For more information on *McKee* and Justice Thomas' concurring opinion, see "Justice Thomas Calls for Supreme Court to Reconsider the Actual Malice Standard" in the Winter/Spring 2019 issue of the Silha *Bulletin*.)

Berisha v. Lawson arose in 2015 when journalist and author published his book *War Dogs: The True Story of How Three Stoners from Miami Beach Became the Most Unlikely Gunrunners in History*. The story detailed how three Miami residents became international arms dealers, which led them to have run-ins with the "Albania mafia." The book named Shkelzen Berisha as a key figure in the mafia. Berisha later sued Lawson for defamation under Florida law, alleging that he was not associated with the mafia and that Lawson relied on poor sources to make that contention.

The U.S. District Court for the Southern District of Florida granted summary judgement in favor of Lawson, finding that Berisha was a public figure and that he had not satisfied the actual malice standard. *Berisha v. Lawson*, 378 F.Supp.3d 1145 (S.D. Fla. 2018). The Eleventh Circuit affirmed the district court ruling. *Berisha v. Lawson*, 973 F.3d 1304 (11th Cir. 2020).

The Supreme Court ultimately denied *certiorari* in the case. However, Justice Thomas filed a dissenting opinion in which he argued that the Court should

reconsider the actual malice standard. He initially argued that the Court's "pronouncement that the First Amendment requires public figures to establish actual malice bears 'no relation to the text, history, or structure of the Constitution."

Justice Thomas further wrote that the Court had "provided scant explanation for the decision to erect a new hurdle for public-figure plaintiffs so long after the First Amendment's ratification." He cited *Gertz v. Robert Welch, Inc.*, 418 U. S. 323, 334-335, 342 (1974), in which the Court reasoned that public figures must prove actual malice because "they invite attention and comment" and have "voluntarily exposed themselves to increased risk of injury from defamatory falsehood." Justice Thomas contended that "it is unclear why exposing oneself to an increased risk of becoming a victim necessarily means forfeiting the remedies legislatures put in place for such victims. And, even assuming that it is sometimes fair to blame the victim, it is less clear why the rule still applies when the public figure 'has not voluntarily sought attention.'"

Second, Justice Thomas asserted that reevaluation of the actual malice standard is "all the more needed because of the doctrine's real-world effects," including that "lies impose real harm." He continued, "The proliferation of falsehoods is, and always has been, a serious matter. Instead of continuing to insulate those who perpetrate lies from traditional remedies like libel suits, we should give them only the protection the First Amendment requires. I would grant *certiorari*."

In a separate dissenting opinion, Justice Gorsuch first acknowledged that "[t]he Bill of Rights protects the freedom of the press not as a favor to a particular industry, but because democracy cannot function without the free exchange of ideas. To govern themselves wisely, the framers knew, people must be able to speak and write, question old assumptions, and offer new insights." However, he wrote that "[l]ike most rights, this one comes with corresponding duties." In particular, Justice Gorsuch contended that "those exercising the freedom of the press had a responsibility to try to get the facts right — or, like anyone else, answer in tort for the injuries they caused," such as for defamation.

Justice Gorsuch asserted that despite a long history of this being the accepted view in the United States, it "changed only in 1964" with *Sullivan*. He noted that the Court "viewed these innovations 'overturning 200 years of libel law' as 'necessary to implement the First Amendment interest in 'uninhibited, robust, and wide-open' debate on public issues,'" citing *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U. S. 749, 766 (1985) (White, J., concurring in judgment).

Justice Gorsuch then provided several ways in which the legal and societal landscapes have changed since 1964, including first that the "media landscape has shifted in ways few could have foreseen," including that "thanks to revolutions in technology, today virtually anyone in this country can publish virtually anything for immediate consumption virtually anywhere in the world." Justice Gorsuch found that the "effect of these technological changes on our Nation's media may be hard to overstate," including the closures of numerous newspapers, decreased viewership of network news, and more. He also contended that the result of the changing media landscape was that "the old economic model that supported reporters, fact-checking, and editorial oversight is disappearing."

> "*Sullivan* provides crucial protection of the independence of news outlets, whose reporting might otherwise be chilled, even for accurate stories, if it were easier to sue them for defamation.. . . The more justices who look poised to potentially revisit that precedent in the coming years, the more alarming Justice Thomas's previously idiosyncratic critiques become."
>
> **— Steve Vladeck, University of Texas School of Law professor**

Second, Justice Gorsuch noted that although the Court in *Sullivan* "may have seen the actual malice standard as necessary 'to ensure that dissenting or critical voices are not crowded out of public debate,'" that justification has perhaps less "force . . . in a world in which everyone carries a soapbox in their hands."

Third, he contended that the Supreme Court "in 1964 may have thought the actual malice standard justified in part because other safeguards existed to deter the dissemination of defamatory falsehoods and misinformation.. . . Less clear is what sway these justifications hold in a new era where the old economic model that supported reporters, fact-checking, and editorial oversight is disappearing."

Fourth, Justice Gorsuch pointed out that when the "Court originally adopted the actual malice standard, it took the view that tolerating the publication of *some* false information was a necessary and acceptable cost to pay to ensure truthful statements vital to democratic self-government were not inadvertently suppressed." However, he asserted that "over time the actual malice standard has evolved from a high bar to recovery into an effective immunity from liability." Justice Gorsuch added, "If ensuring an informed democratic debate is the goal, how well do we serve that interest with rules that no longer merely tolerate but encourage falsehoods in quantities no one could have envisioned almost 60 years ago?"

Fifth, Justice Gorsuch suggested that the Court in 1964 "may have thought the actual malice standard would apply only to a small number of prominent governmental officials whose names were always in the news and whose actions involved the administration of public affairs." However, he asserted that "today's world casts a new light on these judgments as well,' including because "private citizens can become 'public figures' on social media overnight."

Justice Gorsuch therefore concluded that it is "unclear how well these modern developments serve *Sullivan*'s original purposes. Not only has the doctrine evolved into a subsidy for published falsehoods on a scale no one could have foreseen, it has come to leave far more people without redress than anyone could have predicted." He continued, "Rules intended to ensure a robust debate over actions taken by high public officials carrying out the

SCOTUS Rulings, *continued on page 16*

SCOTUS Rulings, *continued from page 15*

public's business increasingly seem to leave even ordinary Americans without recourse for grievous defamation. At least as they are applied today, it's far from obvious whether *Sullivan*'s rules do more to encourage people of goodwill to engage in democratic self-governance or discourage them from risking even the slightest step toward public life."

Justice Gorsuch added, "I do not profess any sure answers. I am not even certain of all the questions we should be asking. But given the momentous changes in the Nation's media landscape since 1964, I cannot help but think the Court would profit from returning its attention, whether in this case or another, to a field so vital to the 'safe deposit' of our liberties."

The full ruling denying *certiorari*, including Justices Thomas' and Gorsuch's dissenting opinions, is available online at: https://scholar.google.com/scholar_case?case=12214066669315353884&hl=en&as_sdt=6&as_vis=1&oi=scholarr.

Following the release of the dissenting opinions, several observers expressed concern about the implications of revisiting *Sullivan* for journalism. CNN Supreme Court analyst and University of Texas School of Law professor Steve Vladeck told CNN on July 2, 2021, "*Sullivan* provides crucial protection of the independence of news outlets, whose reporting might otherwise be chilled, even for accurate stories, if it were easier to sue them for defamation.. . . The more justices who look poised to potentially revisit that precedent in the coming years, the more alarming Justice Thomas's previously idiosyncratic critiques become."

In a July 7 opinion piece for *The Washington Post*, media critic Erik Wemple wrote, "[I]t's hard to see how a reassessment of *Sullivan* would combat the brand of Internet disinformation mentioned by Thomas and Gorsuch. The viral lies that thrive on message boards and percolate up to unhinged quasi-news sites often spread at the fingertips of anonymous malefactors." University of Florida professor Clay Calvert told Wemple, "Individual libel suits are an incredibly ineffective, time consuming and expensive mechanism for policing the massive problems of disinformation on the Internet."

Wemple also argued that Justices Thomas and Gorsuch failed to mention "one key dimension of the *Sullivan* file," namely that the case arose from "the efforts of Montgomery, Ala., city commissioner L.B. Sullivan to seek damages for inaccuracies in an advertisement — not a news article — that ran in the New York Times seeking contributions for the defense of the Rev. Martin Luther King Jr." Wemple cited former *New York Times* columnist Anthony Lewis' book *Make No Law* in noting that "[t]he jury in the case was all White, the judge a believer in 'white man's justice.' The award in the case was for $500,000, the largest libel judgment in the state's history." Furthermore, "various Alabama officials had filed 11 libel suits against the Times seeking $5.6 million in damages. It turned out that the supporters of a racially oppressive regime didn't like having a northern paper mucking around in their business. The campaign was effective, too, as the Times withdrew its reporters from Alabama for a year over legal concerns." (Lewis delivered the 17th Annual. Silha Lecture, "Terrorism and Freedom: A Discussion on How to Preserve Constitutional Values in a Time of National Crisis," on Oct. 8, 2002. For more on the lecture, see "Silha Lecturer Anthony Lewis Speaks to a Packed House" in the Fall 2002 issue of the Silha *Bulletin*.)

The result, Wemple contended, was that "the pre-*Sullivan* legal landscape posed a threat to the paper's reporting and perhaps to its very existence" and without the actual malice standard, "political actors in contemporary America [c]ould seize on the abandonment of *Sullivan* to replicate those media-suppression activities of Alabama officials during the civil rights era."

Gibson, Dunn & Crutcher LLP attorney Theodore J. Boutrous contended in an interview with Wemple that *Sullivan* marked an important moment in protecting journalists so they can do their jobs. "If anything, we now know [efforts at suppressing the news media would be worse [without *Sullivan*].. . . [I]t would be times a thousand — because we've seen that campaigns by public officials to use defamation lawsuits and the threats of lawsuits to try to punish and deter truthful news reporting has only increased in modern times." (Boutrous delivered the 33rd Annual Silha Lecture, titled "The First Amendment and #MeToo" on Oct. 17, 2018. For more on the lecture, see "33rd Annual Silha Lecture Addresses the Free Speech Implications of the #MeToo Movement" in the Fall 2018 issue of the Silha *Bulletin*.)

U.S. Supreme Court Holds Deliberative Process Exemption Protects Some Administrative Agency Documents from Disclosure Under FOIA

On March 4, 2021, the U.S. Supreme Court ruled that an administrative agency's predecisional, deliberative draft biological opinions are protected from disclosure under the Freedom of Information Act's (FOIA) deliberative process privilege exemption, even if the records reflect the agency's final views on a proposal. *United States Fish and Wildlife v. Sierra Club, Inc.*, 141 S.Ct. 777 (2021). The decision reversed the U.S. Circuit Court of Appeals for the Ninth Circuit, which had affirmed a ruling from the U.S. District Court for the Northern District of California that draft opinions are not privileged under FOIA. The 7-2 decision, which was Justice Amy Coney Barrett's first majority opinion on the Court, indicated that if an agency issues a finding of "jeopardy" in a biological opinion related to a government action, the finding need not be disclosed under FOIA unless the agency moves forward with the action without making a single change to it. Open government advocates were critical of the decision and called on Congress to amend FOIA in response.

The case involved two federal agencies — the Fish and Wildlife Service and the National Marine Fisheries Service (collectively, the Services) — and an environmental advocacy group, the Sierra Club. In April 2011, the U.S. Environmental Protection Agency (EPA) proposed a rule related to "cooling water intake structures" that are used to cool industrial equipment. The proposed rule had the potential to affect protected listed species under the Endangered Species Act, so the EPA was required to consult with the Services to obtain either a "jeopardy" or "no jeopardy" biological opinion before issuing the rule. If the Services issued a "jeopardy" finding, the EPA would be required to either implement a "reasonable and prudent alternative," terminate the action, or apply for an exemption.

In December 2013, Services staff issued draft biological opinions that found the proposed EPA rule would place protected species in "jeopardy"

and proposed other "reasonable and prudent alternatives" to the proposed rule. The draft opinions were circulated but were not approved by officials at either Service agencies. Instead, decisionmakers continued their conversations with the EPA, discussing what exactly the EPA's goal was with the rule and other elements of the rule. The Services did nothing with the draft opinions, but instead continued to hold conversations with the EPA about the rule.

In March 2014, the EPA sent the Services a proposed rule that was significantly different than the original 2013 proposed rule. After conducting a new review, the Services found the proposed rule unlikely to harm any listed species and issued a "no jeopardy" biological opinion. The EPA issued its final rule based on the March 2014 changes the same day.

The Sierra Club submitted a FOIA request for the 2013 proposed rule, seeking the Services' biological opinions and other documents related to the discussions between the EPA and the Services. The Services released thousands of documents under FOIA but withheld the draft biological opinions related to the 2013 proposed rule, citing the deliberative process privilege. The deliberative process privilege is incorporated within Exemption 5 — one of nine primary exemptions to disclosure under FOIA — which an agency may invoke to prevent disclosure of "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5) (2000). Specifically, the deliberative process privilege covers "documents reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and polices are formulated," the Court wrote, citing *NLRB v. Sears, Roebuck & Co.*, 421 U. S. 132, 150 (1975).

On Dec. 21, 2015, the Sierra Club filed suit in U.S. District Court for the Northern District of California, asserting that the draft opinions were not privileged. The District Court agreed with Sierra Club and the Ninth Circuit affirmed in part, holding that the draft opinions were not privileged because they concerned the Services' final opinion that the 2013 proposed rule was likely to "adversely affect" protected species. *Sierra Club v. U.S. Fish and Wildlife Service*, No. 3:15-cv-05872-EDL (N.D. Cal. 2021); *Sierra Club v. U.S. Fish and Wildlife Service*, 911 F.3d 967 (9th Cir. 2018). The Supreme Court granted a petition for a writ of *certiorari* filed by the Services.

The Court held that the Services' draft opinions regarding the 2013 proposed rule were not a final decision, but rather reflected a preliminary review of the proposed rule; therefore, they were protected under the deliberative process privilege. The Court reasoned that the privilege applies to "predecisional, deliberative documents" and not "documents reflecting a final agency decision and the reasons supporting it." The Court held that whether a document is predecisional is based on whether the agency treats the document as final, removing the agency's ability to freely change its mind on its implementation. A document is deliberative if it helped the agency formulate a position.

Further, the Court held that for documents to fall outside of the deliberative process privilege, the documents must have legal consequences, not merely practical consequences. The Court opined that final biological opinions have legal consequences because they alter "'the local regime to which the action agency is subject, authorizing it' to take action affecting an endangered species 'if (but only if) it complies with the prescribed conditions.'" Alternatively, although a draft opinion might have practical consequences — that is, the draft opinion might inspire an agency to change its proposed rule or adopt a different approach) — it falls short of creating legal consequences if the agency adopts an alternative approach.

In considering the steps the EPA took in adopting its final rule, the Court held that the Services did not treat the 2013 draft opinions as final, but more akin to a "draft of a draft." The decision makers at the Services did not approve the draft opinions, did not send them to the EPA, and resumed talks with the EPA to discuss a different approach that would not create a "jeopardy" finding related to protected species.

Although the Court warned that the decision did not create a blanket rule that all documents labeled as a draft would be protected under the deliberative process privilege and that a fact-based inquiry would need to be conducted to determine whether agencies were "hiding" final decisions in draft form, it also concluded that the Services did not engage in such a practice in this case. Therefore, the Court reversed the Ninth Circuit and remanded the case to the District Court to determine whether any portions of the documents could be separated from those portions protected by the deliberative process privilege.

Justice Stephen Breyer dissented, joined by Justice Sonia Sotomayor. Justice Breyer objected to allowing draft opinions to be withheld under the deliberative process privilege because he disagreed with the majority's finding that the 2013 draft opinions were not final decisions.

Justice Breyer first opined that whether a decision can be changed should not define whether a document is final. In the past, the Services have issued a final biological opinion that they have then withdrawn and replaced with a new final opinion. He concluded that a draft biological opinion is final as it relates to the content within, not as it relates to its ability to be changed. "The mere possibility of a future change does not alter the finality, or the final effect, of the original document," Justice Breyer wrote.

Second, Justice Breyer wrote that both a final biological opinion and a draft biological opinion function in the same way during the administrative process: They both propose "reasonable and prudent modifications or alternatives." A draft opinion and a final opinion provide the agency with the same options for response; the agency can drop the action, accept proposed modifications, take the action and accept potential penalties, or seek an exemption. The only difference between the two is that the draft opinion must be issued before the final opinion.

Third, Justice Breyer emphasized that it is the draft opinion — and not the final opinion — that "informs the EPA of the Services' conclusions about jeopardy and alternatives and triggers within the EPA the process of deciding what to do about those conclusions." It very rarely happens that the Services issue a "jeopardy" finding in a final biological opinion. If a final opinion is disclosable under FOIA, Justice Breyer questioned why a draft opinion "embodying the same Services conclusions" and which leaves the EPA with the same choices would not be disclosable.

SCOTUS Rulings, *continued on page 18*

SCOTUS Rulings, *continued from page 17*

Fourth, Justice Breyer reasoned that permitting discovery of draft opinions would not have a chilling effect on frank internal agency discussions because there are draft opinions that are discoverable and yet agencies still conduct deliberations related to these "releasable" documents. Draft biological opinions are commonly released to the public when they relate to actions by a private party. For example, when a private party seeks an EPA permit and the Services draft their biological opinion related to the permit, the draft opinion is exempt from the deliberative process privilege. Justice Breyer described the discoverability of opinions related to private parties but not government agencies as "anomalous," writing: "To hold that Draft Biological Opinions are discoverable when a private party seeks an EPA permit but not when, as here, the EPA seeks to write a generally applicable rule that governs private party conduct seems highly anomalous."

Finally, Justice Breyer argued against the majority's holding that a draft biological opinion does not impose legal consequences. Draft opinions, like final opinions, limit an agency's options by analyzing "reasonable and prudent alternatives." Justice Breyer reasoned that if both types of opinions require the agency to face the same potential legal consequences, both types should be viewed as imposing legal consequences.

"In sum, the likely finality of a Draft Biological Opinion, its similarity to a Final Biological Opinion, the similar purposes it serves, the agency's actual practice, the anomaly that would otherwise exist depending upon the presence or absence of a private party, and the presence of at least some regulation-based legal constraints — convince me that a Draft Biological Opinion would not normally enjoy a deliberative privilege from FOIA disclosure," Justice Breyer wrote.

Justice Breyer concluded his dissent by clarifying that although he believes draft biological opinions "do not normally enjoy" the deliberative process privilege, he would remand the case to the Ninth Circuit to conduct a factual analysis as to whether the 2013 biological opinions were in fact drafts, because some of them were heavily highlighted and edited while others were complete albeit absent a final signature.

A full copy of the ruling is available online at: https://z.umn.edu/742v.

In comment to *Bloomberg Law* on March 4, Andrew Rosenberg, Director of the Center for Science and Democracy at the Union of Concerned Scientists, said the Supreme Court's decision may result in agencies disclosing less information about how they ultimately arrived at decisions. "I think that the implications are that the public will have less information and ability to be involved in the process of consultation between agencies. Agencies will be doing much more behind closed doors," Rosenberg told the news outlet. Likewise, Lewis and Clark Law School professor Daniel Rohlf told *Bloomberg Law* that the ruling will have the effect of inhibiting government transparency. "Public disclosure of government documents and judicial review of federal agency's decisions help ensure that the government follows the law; this ruling puts up an unnecessary roadblock to both," Rohlf said.

> "Public disclosure of government documents and judicial review of federal agency's decisions help ensure that the government follows the law; this ruling puts up an unnecessary roadblock to both."
>
> **— Daniel Rohlf, Lewis and Clark Law School professor**

Melissa Wasser, Policy Counsel at the Project on Government Oversight, wrote in a blog post on March 18 that the decision "will exacerbate the application of Exemption 5 moving forward unless Congress steps in to reform FOIA." Specifically, Wasser called on Congress to create a balancing test for applying the deliberative process privilege that would "require agencies to release information where the public's interest in disclosure outweighs the government's interest in secrecy." Wasser also advocated for legislation that would require agencies to "identify a specific identifiable harm before being allowed to withhold records under a discretionary exemption." "These reforms will greatly reduce costs and resources on the government's end, both when initially going through documents and when going through litigation, which is costly for both parties," Wasser wrote. Wasser's blog post is available online at: https://z.umn.edu/748b.

Supreme Court Strikes Down TCPA Debt-Collection Exemption, Leaves Remainder of Statute Intact

On April 1, 2021, the U.S. Supreme Court unanimously ruled in *Facebook, Inc. v. Duguid*, 141 S.Ct. 1163, 1164 (2021), that the Telephone Consumer Protection Act's (TCPA), 47 U.S.C. § 227(a)(1) (2021), definition of an "automatic telephone dialing system" (ATDS) does not apply to devices that only have the capacity to store numbers and dial them automatically, which was the basis of a federal circuit court split. The Court held that "a necessary feature of an autodialer under § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called." The decision means that Facebook's database of phone numbers associated with Facebook accounts does not qualify as an ATDS. Following the ruling, some observers viewed the decision as an unbridled win for private companies who profit from the use of customer data and as a crushing loss for consumer privacy.

According to the law firm McGuire Woods LLP, the circuit split that brought about the *Duguid* case arose when the U.S. Courts of Appeals for the Second, Third, Sixth, Seventh, Eleventh, and D.C. Circuits interpreted the definition of an ATDS narrowly, whereas the Ninth Circuit in *Duguid* interpreted the definition more broadly to include any device that can automatically dial numbers from a list.

Congress passed the TCPA in 1991 with the goal of broad privacy protection in relation to illegal robocalls to consumers' telephones. An ATDS, which is also referred to as an "autodialer," is defined under the TCPA as "equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." Despite this legislation, however, spam calls and texts have proliferated. The TCPA includes a private right of action for individuals to combat such intrusions with class action litigation, much to the chagrin of

American companies. Thus, there have been multiple opportunities for courts to conclude that the TCPA inadequately outlines what kind of telemarketing behavior is and is not prohibited.

The case before the Supreme Court arose in January 2014 when Noah Duguid received automated text messages from Facebook about security features on his account, despite the fact he had never opened a Facebook account. Because he received the messages without consent and could not stop them for at least 10 months, he filed a lawsuit against Facebook in the U.S. District Court for the Northern District of California, alleging that Facebook had sent the text messages using an ATDS in violation of the TCPA.

In June 2019, the Ninth Circuit unanimously held that Duguid had plausibly alleged in an amended complaint that Facebook had used an ATDS as defined by the Ninth Circuit in *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1043 (9th Cir. 2018) (cert. dismissed 2019). The *Marks* court defined an ATDS as "equipment which has the capacity — (1) to store numbers to be called or (2) to produce numbers to be called, using a random or sequential number generator — and to dial such numbers automatically."

The Ninth Circuit's rulings in *Duguid* and *Marks* put it at odds with several other federal circuit courts that more narrowly interpreted the definition of an ATDS. Those narrower analyses focused primarily on the grammatical structure of the statute, including whether the words "store" and "produce" are modified by the phrase "using a random or sequential number generator."

In the most recent case using the narrower interpretation, the Seventh Circuit was asked in *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 461 (2020), to determine whether AT&T's "customer feedback tool," which "pulls and dials numbers from an existing database of customers rather than randomly generating them," constituted an ATDS under the TCPA. In the opinion by then-Judge Amy Coney Barrett, the Seventh Circuit panel explained that there were four ways to read the statutory definition:

- "First, the phrase 'using a random or sequential number generator' might modify both store and produce, which would mean that a device must be capable of performing at least one of those functions using a random or sequential number generator to qualify as an 'automatic telephone dialing system.' This is how the Third and Eleventh Circuits interpret the statute.
- Second, the phrase might describe the telephone numbers themselves, specifying that the definition captures only equipment that dials randomly or sequentially generated numbers. This is how the district court interpreted the provision.
- Third, the phrase might limit only the word produce, which would mean that the definition captures not only equipment that can produce numbers randomly or sequentially, but also any equipment that can simply store and dial numbers. This is the Ninth Circuit's interpretation.
- Finally, the phrase could describe the manner in which the telephone numbers are to be called, regardless of how they are stored, produced, or generated. Some courts — including the district court in this case — have alluded to this possibility, although none has adopted it."

The Seventh Circuit ultimately chose the first definition as the one that presented the least significant problems as compared to those presented by the other definitions.

This split led the Supreme Court to grant *certiorari* to answer a question posed by Duguid's case: "Whether the definition of an ATDS in the TCPA encompasses any device that can 'store' and 'automatically dial' telephone numbers, even if the device does not 'us[e] a random or sequential number generator.'" The full petition for writ of *certiorari* is available online at: https://www.supremecourt.gov/DocketPDF/19/19-511/119361/20191017155036139_2019-10-17%20Facebook%20v.%20Duguid%20Petition%20FINAL.pdf.

The Supreme Court's opinion, authored by Justice Sonia Sotomayor, analyzed the grammatical structure of the TCPA using the series qualifier canon. Justice Sotomayor explained that "[u]nder conventional rules of grammar, '[w]hen there is a straightforward, parallel construction that involves all nouns or verbs in a series,' a modifier at the end of the list 'normally applies to the entire series.' A. Scalia & B. Garner, Reading Law: The Interpretation of Legal Texts 147 (2012) (Scalia & Garner) (quotation modified)." Justice Sotomayor applied this to the case before the Court, writing, "Here, the series-qualifier canon recommends qualifying both antecedent verbs, 'store' and 'produce,' with the phrase 'using a random or sequential number generator.' That recommendation produces the most natural construction, as confirmed by other aspects of §227(a)(1)(A)'s text."

Reading the text otherwise, Justice Sotomayor argued, would expand the definition of an autodialer to be so broad as to encompass any modern cell phone that stores phone numbers and can be programmed to dial without human intervention. Justice Sotomayor held that this approach "would take a chainsaw to these nuanced problems when Congress meant to use a scalpel" and make ordinary citizens guilty parties in TCPA cases.

Justice Sotomayor acknowledged Duguid's argument that the term "random number generator" at the time it was written "invokes ways of producing numbers, not means of storing them." But ultimately, Justice Sotomayor concluded that Duguid made a valiant, if failed, effort to sway the court to find "using a random or sequential number generator" should only modify "produce" in the sequence. She wrote, "It is true that, as a matter of ordinary parlance, it is odd to say that a piece of equipment 'stores' numbers using a random number 'generator.' But it is less odd as a technical matter. Indeed, as early as 1988, the U. S. Patent and Trademark Office issued patents for devices that used a random number generator to store numbers to be called later (as opposed to using a number generator for immediate dialing)."

As to the "slippery slope" argument Duguid provided — that accepting the narrow definition of an ATDS will subject Americans to a "torrent of robocalls" — Justice Sotomayor wrote that the plaintiff "greatly overstates the effects of accepting [this] interpretation . . . In any event, Duguid's quarrel is with Congress, which did not define an autodialer as malleably as he would have liked."

Justice Sotomayor therefore held "that a necessary feature of an autodialer under § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called. The judgment of the Court of Appeals is reversed, and the case is remanded for further proceedings consistent with this opinion."

SCOTUS Rulings, *continued on page 20*

SCOTUS Rulings, *continued from page 19*

Justice Samuel Alito filed a concurring opinion, in which he wrote that he agreed "with the Court that an 'automatic telephone dialing system,' as defined in the Telephone Consumer Protection Act of 1991, must have the capacity to 'store ... telephone numbers' by 'using a random or sequential number generator.'" He added that he also agreed "with much of the Court's analysis and the analysis in several Court of Appeals decisions on this question."

However, Justice Alito wrote separately "to address the Court's heavy reliance on one of the canons of interpretation that have come to play a prominent role in our statutory interpretation cases. Cataloged in a treatise written by our former colleague Antonin Scalia and Bryan A. Garner, counsel for respondents in this case, these canons are useful tools, but it is important to keep their limitations in mind."

According to the law firm Gibson, Dunn & Crutcher LLP on April 1, 2021, the Supreme Court's opinion did not address the question of what type of mechanism or device counts as a random or sequential number generator, leaving the door open for the Federal Communications Commission to adopt further guidance limiting the TCPA's scope.

In an April 4, 2021 podcast from the Consumer Financial Services Group at Ballard Spahr LLP, partner Jenny Perkins contended that it is likely that litigation involving prerecorded messages, and questions over what qualifies as one, will next take center stage. "I think we're also going to see a new host of case law developed on prerecords," Perkins said. "Oftentimes, case law on prerecords have just been ignored. The hot issue has always been: What constitutes an ATDS? But for instance, the fifth circuit a couple years ago, they actually ruled that in order for a prerecord to be actionable under the TCPA, it actually must have played. So I think we're going to see a lot of litigation in developing case law on the prerecord space."

It is also likely that technology will change to meet the moment. In the aforementioned podcast, Ballard Spahr partner Mark Furletti said, "I think we will see more and better call blocking, call screening, absent technology. I know I have on my Gmail account — I have a primary mailbox, a promotion mailbox, and a social mailbox. I never look at the promotion mailbox almost ever. And so it won't surprise me if we see things on your cell phone that will . . . allow [you] to sort calls and texts in this exact same way."

Other commentators hailed the Court's decision as a win for corporations that rely on communicating with customers through telemarketing devices. Writing for *The National Law Review*, Brion Doyle and Jailah Emerson opined on June 5, 2021, "The Supreme Court's decision will likely quiet TCPA class action litigation in relation to the autodialer provision, which would be a welcome relief to businesses."

Mark Brennan, writing for *Bloomberg Law* on May 4, 2021, wrote, "It's about time . . . For more than a decade, compliance-minded American companies have been asking courts and the Federal Communications Commission to provide a clear answer to an issue driving some of the nation's most prolific and vexatious class action consumer protection litigation." Brennan went on to argue that these class action cases are not even necessarily accomplishing what the private right of action set out to do. "While these lawsuits enriched plaintiffs' lawyers and threatened many good U.S. call center jobs, they did very little for consumers. The suits don't go after the actual bad actors — scammers and fraudsters — but target credible, household-name companies. Consumers have received very little of the eye-popping settlement proceeds, and perhaps most importantly, they continue to receive millions of unlawful robocalls from bad actors."

Other observers, on the other hand, recognized the risks inherent in the Court handing corporations the win in this case. Jacob Finkel, writing for *Slate* on April 12, 2021, argued, "Progressives should take careful note of the unanimous victory the Supreme Court handed down for Facebook in early April. The tech giant's win gutted a 30-year-old federal law preventing junk calls, a boon to big corporations that now face less liability for annoying calls and texts. But even more importantly, it signaled the absolute supremacy of textualism — the conservative credo — as the universal language spoken not only by the newly emboldened majority but also by the Court's diminished liberal wing."

As textualism has flourished on the right, it has also influenced the few remaining left-leaning Supreme Court justices, Finkel explained, despite the fact that Sotomayor in particular has previously challenged textualist orthodoxy in the past. There may be many reasons for this — for instance, Sotomayor may have been using the language of the right to try to pave the way for a more moderate take on the TCPA. But ultimately, Finkel contended that "[t]he three liberal justices, and the progressive legal community more broadly, need to get to work on their own ideas. Otherwise, the only languages a future left-leaning Court will know how to speak will be different variations of conservative orthodoxy."

A Decision "In Favor of Scam Artists and Dishonest Corporations": Rethinking the FTC's Enforcement Agenda in the Wake of *AMG*

On April 22, 2021, in *AMG Capital Management., LLC v. Federal Trade Commission*, 141 S. Ct. 1341, 1344 (2021), the U.S. Supreme Court ruled that §13(b) of the Federal Trade Commission Act, 15 U.S.C. § 13(b) (2021), which authorizes the Federal Trade Commission (FTC) to seek injunctive relief in unfair and deceptive trade practice cases, does not authorize the commission to levy monetary relief or order courts to collect it. The Court did not entirely foreclose the FTC's ability to seek monetary remedies; it upheld the Commission's ability to obtain restitution after administrative proceedings and kept open the option of asking Congress to "grant it further remedial authority." The Court's decision reversed the U.S. Court of Appeals for the Ninth Circuit's affirmation of a $1.27 billion judgment entered against deceptive payday lenders. Consumer protection and privacy advocates predict the decision will change the way consumer redress actions play out. Meanwhile, a bill approved by the U.S. House of Representatives Committee on Energy and Commerce would grant the FTC full authority to assess monetary penalties without first undertaking administrative processes.

In 2012, the FTC sued Scott Tucker and his companies for "unfair or deceptive acts or practices in or affecting commerce" in violation of the FTCA. Tucker operated several online payday loan companies.

When explaining the loan terms, the companies "misled many customers" by including in the fine print a provision that the loan would automatically renew unless the customer took steps to opt out. The automatic renewal meant that customers who took out a $300 loan could be obligated to repay $975. Between 2008 and 2012, his businesses "made more than 5 million payday loans, amounting to more than $1.3 billion in deceptive charges."

The Commission did not use its statutory powers to take the defendant through its administrative process, but instead filed suit in the U.S. District Court for the District of Nevada. The Commission, under its §13(b) authority, asked the court to grant an injunction and order $1.27 billion in monetary relief. The litigation was split into two phases: a liability phase and a relief phase.

On Jan. 28, 2014, Magistrate Judge Cam Ferenbach granted summary judgment to the FTC for two of its claims and issued a Report and Recommendation analyzing the loan websites. The district court granted a permanent injunction against Scott Tucker and ordered him to pay the full $1.27 billion to the FTC. The amount, calculated by an FTC data analyst, represented consumer losses from 2008-2012.

Tucker appealed to a three-judge panel of the Ninth Circuit, arguing that the FTC was acting beyond its authority by ordering monetary damages under §13(b). Judge Diarmuid F. O'Scannlain wrote the opinion for the court. *Fed. Trade Comm'n v. AMG Capital Mgmt., LLC*, 910 F.3d 417 (9th Cir. 2018). O'Scannlain agreed that the loan documentation was deceptive because it "did not accurately disclose the loan's terms." In responding to Tucker's contention that the FTC was not explicitly granted the power to collect monetary damages, O'Scannlain acknowledged that Tucker's argument had "some force" but cited its own precedent to "squarely foreclose" his interpretation. In 2016, the Ninth Circuit had upheld the FTC's power to order restitution. *Fed. Trade Comm'n v. Commerce Planet, Inc.*, 815 F.3d 593, 598 (9th Cir. 2016). Tucker asked the court to reconsider its ruling in light of *Kokesh v. SEC*, 137 S. Ct. 1635 (2017), a Supreme Court case that classified disgorgement as a penalty instead of an equitable remedy. However, a three-judge panel can only overrule circuit precedent that is "clearly irreconcilable with the reasoning or theory of intervening higher authority." O'Scannlain ruled that *Kokesh* was not "clearly irreconcilable" with the court's precedent and therefore declined to overturn the previous case. The majority opinion concluded by finding that the $1.27 billion judgment appropriately represented Tucker's "ill-gotten" gains and that the lower court did not abuse its discretion in entering the judgment.

O'Scannlain and Judge Carlos Bea wrote a special concurrence, arguing that the Circuit's precedent was incompatible with the text and structure of the FTCA and requesting an *en banc* rehearing of the case. The Ninth Circuit denied a rehearing *en banc* on June 20, 2019.

The Supreme Court granted *certiorari* "in light of recent differences that have emerged among the Circuits as to the scope of §13(b)." Justice Stephen Breyer delivered the opinion for a unanimous Court, holding that §13(b)'s permanent injunction language did not authorize the FTC "directly to obtain court-ordered monetary relief."

Justice Stephen Breyer began with a plain language argument: nothing in §13(b) explicitly authorizes monetary judgments. Section 13(b) authorizes injunctions, which are "not the same as an award of equitable monetary relief." Justice Breyer then considered the whole structure of §13(b). The provision "focuses upon relief that is prospective, not retrospective." To understand the text as allowing for retroactive collection of monetary remedies is to "read the words as going well beyond the provision's subject matter."

Justice Breyer next examined the entire Act beyond §13(b). Other sections of the statute explicitly gave district courts power to impose monetary penalties and monetary relief after FTC administrative proceedings. He concluded that because Congress did not overtly insert the same language into §13(b), "it likely did not intend for §13(b)'s more cabined "permanent injunction" language to have similarly broad scope." According to Justice Breyer, a literal reading, which allows the Commission to obtain monetary relief only through administrative proceedings but obtain injunctions outside of these proceedings, "produces a coherent enforcement scheme."

Justice Breyer also refuted the FTC's argument that previous Supreme Court cases had interpreted statutory provisions allowing injunctive relief as authorizing equitable monetary relief. Previous cases could be distinguished, according to Justice Breyer, because they involved different statutes with different overall structures, and the Court did not "purport to set forth a universal rule of interpretation." Additionally, he concluded that a provision that grants authority to seek injunctions or other equitable powers "does not automatically authorize a court to provide monetary relief." He therefore held that the scope of equitable relief offered by a provision "remains a question of interpretation in each case," citing *Mertens v. Hewitt Associates*, 508 U.S. 248, 257 (1993).

Justice Breyer also rejected arguments that Congress "simply created two enforcement avenues" for the statute, one administrative and one judicial, because of the "interpretive difficulties" laid out early in the opinion. He rejected the argument that "Congress merely intended to enact a more onerous alternative to §13(b)" when it authorized monetary relief following administrative proceedings in a separate section of the statute.

The FTC also had argued that federal courts of appeal had, until recently, consistently accepted its interpretation of §13(b), and that Congress's inaction on the subject in subsequent amendments could be seen as a tacit endorsement. Justice Breyer rejected this argument as well, writing that "when 'Congress has not comprehensively revised a statutory scheme but has made only isolated amendments, it is impossible to assert with any degree of assurance that congressional failure to act represents affirmative congressional approval of [a court's] statutory interpretation."

Finally, Justice Breyer acknowledged the public policy argument for not allowing the Commission to use §13(b) to obtain monetary relief. The Court pointed out that the Commission still had the authority to pursue administrative procedures. Furthermore, he wrote that "[i]f the Commission believes that authority too cumbersome or otherwise inadequate, it is, of course, free to ask Congress to grant it further remedial authority."

Rebecca Slaughter, acting chair of the FTC, did just that. In a statement, she called the Supreme Court's decision a ruling "in favor of scam artists and

SCOTUS Rulings, *continued on page 22*

SCOTUS Rulings, *continued from page 21*
dishonest corporations," and urged "Congress to act swiftly to restore and strengthen the powers of the agency so we can make wronged consumers whole." The full statement is available online at: https://www.ftc.gov/news-events/press-releases/2021/04/statement-ftc-acting-chairwoman-rebecca-kelly-slaughter-us. On April 27, Slaughter testified before the House Committee on Energy and Commerce's Subcommittee on Consumer Protection and Commerce and asked that "Congress act quickly to provide clear authority to the Commission."

Following the ruling, observers contended that the FTC will be forced to rethink its enforcement agenda. This could lead to creative lawyering, according to an April 22, 2021 commentary by Morgan Lewis attorneys for the firm's website. "In consumer protection cases, the FTC may look to existing trade regulation rules, such as the Telemarketing Sales Rule, or statutory designations of 'deemed' trade regulation rules such as those in the Fair Debt Collection Practices Act, for an alternative basis for monetary relief in what would previously have been standalone Section 13(b) cases," the commentary read.

The FTC could look to other statutes as well, Greenberg Traurig attorneys Andrew G. Berg, Miriam G. Bahcall, Darren Abernethy and David S. Repking wrote in an April 23 commentary for the firm's website. The FTC still has power under additional statutes like the Restore Online Shopper's Confidence Act (ROSCA) to seek monetary relief.

Other authorities could fill the gap, Husch Blackwell attorneys Wendy K. Arends, Harvey M. Tettlebaum, Mark B. Tobey and Emily R. Lyons wrote in a May 3 commentary for the firm's website. The FTC could refer cases to agencies like the Consumer Finance Protection Bureau (CFPB), Federal Communications Commission (FCC), or Department of Justice (DOJ).

State attorneys general could also step in. The Commission plans to work with state attorneys general to seek monetary relief in consumer protection and privacy cases, Allison Grande wrote in a May 28 commentary for *Law360*. Absent powers to collect monetary relief, the FTC could also pursue non-traditional remedies in privacy and data security settlements, "including requirements to delete personal information that the agency alleges was wrongfully collected." The decision could also mean more rulemaking from the agency.

On March 25, 2021, Slaughter announced a new rulemaking group within the agency's Office of the General Counsel aimed at bolstering consumer protection. According to an FTC press release, the group "will allow the FTC to take a strategic and harmonized approach to rulemaking across its different authorities and mission areas. With this new group in place, the FTC is poised to strengthen existing rules and to undertake new rulemakings to prohibit unfair or deceptive practices and unfair methods of competition. Especially given the risk that the Supreme Court substantially curtails the FTC's ability to seek consumer redress under section 13(b), rulemaking is a critical part of the FTC's toolbox to stop widespread consumer harm and to promote robust competition." The full press release is available online at: https://www.ftc.gov/news-events/press-releases/2021/03/ftc-acting-chairwoman-slaughter-announces-new-rulemaking-group.

Meanwhile, days before the *AMG* decision was announced, 13 members of Congress introduced the Consumer Protection and Recovery Act, which was referred to the House Committee on Energy and Commerce. The bill would grant the FTC the ability to seek restitution and disgorgement under its §13(b) authority. On July 20, 2021, the bill passed the House in a 221-205 vote.

As the *Bulletin* went to press, the bill had not passed the Senate. The full text of the bill is available online at: https://energycommerce.house.gov/newsroom/press-releases/pallone-on-committee-passage-of-legislation-restoring-ftc-s-13b-consumer.

"No Concrete Harm, No Standing": TransUnion Implications for Data Privacy Suits

On June 25, 2021, the U.S. Supreme Court ruled in *TransUnion v. Ramirez*, 141 S. Ct. 2190, 2197 (2021), that a "risk of future harm" was insufficient to grant standing under Article III of the U.S. Constitution and that every member of a class action lawsuit must prove concrete harm beyond a mere statutory violation. The Court, in reversing the standing decision made by the U.S. Court of Appeals for the Ninth Circuit, clarified questions left unanswered by *Spokeo v. Robins*, 578 U.S. 330, 340 (2016), the Court's most recent precedent on Article III standing. Attorneys contended that the decision could have broad implications for data privacy suits. (For more information on *Spokeo*, see "Supreme Court Issues Long-Awaited *Spokeo* Ruling" in the Summer 2016 issue of the Silha *Bulletin*.)

TransUnion involved a class of 8,185 people whose names had been identified as "potential matches" for the U.S. Treasury Department's Office of Foreign Assets Control's (OFAC) list of "terrorists, drug traffickers, and other serious criminals." TransUnion offered an "OFAC Name Screen Alert" tool to compare consumers' first and last names to names on the list to help businesses avoid transacting with potential terrorists and criminals.

Of the class, 1,853 consumers had these misleading credit reports shared to third parties and 6,332 class members had the misleading "potential match" alert in their credit files but did not have their files shared with any third parties. The class action was brought under the Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681(e)(b) (2021), which requires credit reporting agencies to follow "reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."

Judge Mary H. Murguia, writing for the Ninth Circuit, held that each member of the class must establish Article III standing to recover monetary damages. *Ramirez v. TransUnion LLC*, 951 F.3d 1008 (9th Cir. 2020). TransUnion argued that to have sustained a concrete injury sufficient to confer Article III standing, each class member must show that TransUnion actually "disclosed his or her credit report to a third party." The Ninth Circuit held that TransUnion's failure to follow "reasonable procedures" to ensure accuracy caused all 8,185 class members to suffer a "material risk of harm" serious enough to constitute a concrete injury regardless of whether the misleading information was ultimately shared.

At the Supreme Court, Justice Brett Kavanaugh wrote the majority opinion in which he reversed the Ninth Circuit's characterization of risk of harm as a concrete injury. Justice Kavanaugh first summarized the basic requirements for Article III standing. The Constitution grants the federal judiciary

the power to handle "cases" and "controversies," and plaintiffs in a suit are further required to show a "personal stake" in the case. Justice Kavanaugh also explained that a plaintiff must also show "that he suffered an injury in fact that is concrete, particularized, and actual or imminent, that the injury was likely caused by the defendant and that the injury would likely be redressed by judicial relief," citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992).

The issue in this case, Justice Kavanaugh wrote, was whether the class members could meet the "concrete" harm requirement. Citing *Spokeo*, Justice Kavanaugh wrote that it was relevant in determining concrete harm to ask "whether the alleged injury has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." Congress's "creation of a statutory prohibition or obligation and a cause of action" does not supersede the Court's responsibility to independently confirm standing in each case.

Justice Kavanaugh reiterated the Court's holding in *Spokeo* that a plaintiff does not automatically satisfy the "injury in fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." In other words, even in the face of a statutory violation and cause of action, a plaintiff must still allege a concrete injury-in-fact.

In this case, the plaintiffs argued that TransUnion's alleged failure to follow reasonable procedures to ensure the accuracy of their credit reports had a "close relationship" to the traditionally recognized tort of defamation. Justice Kavanaugh agreed with this argument for the plaintiffs, who had their data shared with a third party, but held that the "mere existence" of a misleading OFAC alert without dissemination did not reach the bar necessary for a concrete injury. The plaintiffs who did not have their information shared with a third party argued that the existence of the misleading alert nonetheless put them at an increased risk of future harm. However, the Court found that the plaintiffs "did not demonstrate that the risk of future harm materialized" because the plaintiffs did not present additional evidence that they were "independently harmed by their exposure to the risk itself."

The plaintiffs had also brought forward a claim that TransUnion "breached its obligation to provide them with their complete credit files upon request" by failing to include the OFAC name alert information in an initial letter. The information was later sent via a second letter. Because the plaintiffs did not demonstrate that "the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."

Additionally, because the plaintiffs did not identify any "downstream consequences" of the format of this mailing, Justice Kavanaugh ruled that this was not enough to reach the level of a concrete injury. The court reversed the judgment from the Ninth Circuit and remanded the case for "further proceedings consistent with this opinion."

Justice Clarence Thomas — joined by Justices Stephen Breyer, Sonia Sotomayor, and Elena Kagan — dissented. Justice Thomas characterized the majority opinion as finding that "TransUnion's actions are so insignificant that the Constitution prohibits consumers from vindicating their rights in federal court." However, Justice Thomas wrote, "The Constitution does no such thing."

Justice Thomas pointed to similar complaints in the past against TransUnion and argued that the company made "surprisingly few changes" to its procedures as a result He went on to establish that "the principle that the violation of an individual right gives rise to an actionable harm was widespread at the founding, in early American history, and in many modern cases." Justice Thomas wrote that although the majority "discusses the supposed failure to show injury in fact," the dissent argues that this disturbs the precedent that "courts for centuries held that injury in law to a private right was enough to create a case or controversy." He found that each plaintiff in this case did establish a violation of their private rights.

According to Justice Thomas, "the majority holds that the mere violation of a personal legal right is *not* — and never can be — an injury sufficient to establish standing. What matters for the Court is only that the 'injury in fact be "concrete"'" (emphasis in original). Justice Thomas also pointed to the Court's previous opinion in *Spokeo*. In *Spokeo*, "the Court made clear that 'Congress is well positioned to identify intangible harms that meet minimum Article III requirements' and explained that 'the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact.'" Justice Thomas called this characterization of Article III standing "remarkable in both its novelty and effects." He continued, "Never before has this Court declared that legal injury is inherently insufficient to support standing. And never before has this Court declared that legislatures are constitutionally precluded from creating legal rights enforceable in federal court if those rights deviate too far from their common law roots."

Following the ruling, several observers contended that it would have massive implications for data privacy lawsuits, especially class actions. Law professors Daniel J. Solove and Danielle Keats Citron wrote in a *Boston University Law Review* article that the decision "significantly undermined the effectiveness of many privacy laws." Although the case nominally affects only federal courts, the professors wrote that "federal standing rules have a way of leaching into judicial thinking" so that "TransUnion may have reverberations beyond just the federal courts."

Dorsey attorneys wrote that the case will have a particular effect on large class action suits brought under established privacy statutes. For class action lawsuits brought under privacy statutes like Illinois' Biometric Information Privacy Act (BIPA) or the California Consumer Privacy Act (CCPA), the decision "severely curtails Federal court jurisdiction for CCPA and BIPA cases and will likely create procedural challenges for multi-state class actions that lack allegations of commonly suffered concrete harm."

Finally, Mayer Brown attorneys asserted in June 28, 2021 blog pst that the Supreme Court's ruling could make class certification itself more difficult, writing, "If proof of injury is individualized, which will be true in many cases, that reality frequently will make it impossible for the class to show that common issues predominate."

Supreme Court Narrows Scope of the Computer Fraud and Abuse Act in *Van Buren*

On June 3, 2021, in *Van Buren v. United States*, 141 S.Ct. 1648 (2021),

SCOTUS Rulings, *continued on page 24*

SCOTUS Rulings, *continued from page 23*

the U.S. Supreme Court held that an individual who uses valid access and log-in credentials to obtain information from a computer system does not violate the Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030(a)(2) (2017), even if they accessed the information for a prohibited purpose. Instead, the Court ruled that individuals violate the statute when they access "a computer with authorization but then obtain[s] information located in particular areas of the computer — such as files, folders, or databases — that are off-limits to [them]." Several observers praised the ruling for protecting research and news-gathering practices employed by researchers and journalists, though they also noted some concerns about the scope of the ruling and the possibility of future litigation.

The case arose when former police sergeant Nathan Van Buren formed what he thought was a close relationship with a man named Andrew Albo, despite warnings from the deputy chief of Van Buren's department that the man was "very volatile." At one point, Van Buren asked Albo for a personal loan, not realizing that Albo secretly recorded the request, took it to the local sheriff's office, and complained that Van Buren had tried to "shake him down" for money.

The Federal Bureau of Investigation (FBI) received the taped conversation and summarily "devised an operation to see how far Van Buren would go for money." The operation included several steps, ultimately leading Van Buren to use his patrol-car computer, with his valid credentials, to access the law enforcement database about a particular license plate number in exchange for about $5,000 from Albo. Van Buren's actions violated police department policy and training, which prohibited obtaining information for non-law enforcement purposes.

Federal prosecutors ultimately charged Van Buren with a one-count felony violation of the CFAA, which imposes criminal liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access," and thereby obtains computer information. The law defines "exceeds authorized access" as "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

The U.S. Court of Appeals for the Eleventh Circuit ultimately upheld the U.S. District Court for the Northern District of Georgia, which sentenced Van Buren to 18 months in prison after a jury convicted him for violating the CFAA. *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019). The Eleventh Circuit rejected Van Buren's claim that the "'exceeds authorized access' clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have." The court held that Van Buren violated the CFAA by accessing the database for an "inappropriate reason."

> "There will be questions to sort out about the exact scope of the [*Van Buren*] ruling, but the Supreme Court made clear that interpreting the CFAA to criminalize routine internet use — including routine journalism — is out of bounds."
>
> **— Grayson Clary,**
> **Reporters Committee for Freedom of the Press**
> **Stanton Foundation National Security**
> **and Free Press Fellow**

Justice Amy Coney Barrett wrote the majority opinion and first explained that although the parties agreed that Van Buren "access[ed] a computer with authorization" and "obtain[ed] . . . information in the computer," they disagreed about whether Van Buren was "entitled so to obtain" the information. Citing dictionary definitions, federal statutes, and other sources, Justice Barrett agreed with Van Buren's interpretation, namely that "[t]he phrase 'is entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."

Second, Justice Barrett rejected several counterarguments by the government, including that "any ordinary speaker of the English language would think that Van Buren 'exceed[ed] his authorized access' to the law enforcement database when he obtained license-plate information for personal purposes." However, Justice Barrett concluded that "the relevant question is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access *as the CFAA defines that phrase*. And as we have already explained, the statutory definition favors Van Buren's reading."

Justice Barrett further held that "Van Buren's account [of the 'without authorization' and 'exceeds authorized access' clauses of subsection (a)(2)] . . . makes sense of the statutory structure because it treats the . . . clauses consistently. Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry — one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." Justice Barrett added, "And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry."

Justice Barrett further explained that "the Government proposes to read the first phrase "without authorization" as a gates-up-or-down inquiry and the second phrase 'exceeds authorized access' as one that depends on the circumstances. The Government does not explain why the statute would prohibit accessing computer information, but not the computer itself, for an improper purpose." She also rejected the government's claim that precedent and statutory history support its interpretation of the clauses.

Finally, Justice Barrett observed that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity.. . . If the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." She continued, "Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the

CFAA. Or consider the Internet. Many websites, services, and databases . . . authorize a user's access only upon his agreement to follow specified terms of service. If the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers."

Justice Barrett therefore concluded that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer — such as files, folders, or databases — that are off limits to him." In the present case, "Van Buren accordingly did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose." She therefore reversed the Eleventh Circuit and remanded the case for further proceedings.

In a dissenting opinion, Justice Clarence Thomas, joined by Chief Justice John Roberts and Justice Samuel Alito, wrote that "common law and statutory law have long punished those who exceed the scope of consent when using property that belongs to others.. . . The [CFAA] extends that principle to computers and information."

Justice Thomas wrote that the majority's reading and interpretation of "exceeds authorized access" — namely that "[s]o long as a person is entitled to use a computer to obtain information in at least one circumstance, this statute does not apply even if the person obtains the data outside that circumstance — is "flawed for a number of reasons." First, Justice Thomas concluded that the majority's "interpretation is contrary to the plain meaning of the text," holding that "[b]ecause Van Buren lacked a law enforcement purpose, the 'proper grounds' did not exist. He was not *entitled* to obtain the data when he did so." He provided several examples, including an employee being entitled to pull a fire alarm in the event of a fire, but not for a different purpose, such as delaying a meeting.

Second, Justice Thomas held that "the majority's reading is at odds with basic principles of property law." He wrote, "Consider trespass. When a person is authorized to enter land and entitled to use that entry for one purpose but does so for another, he trespasses.. . . What is true for land is also true in the computer context; if a company grants permission to an employee to use a computer for a specific purpose, the employee has no authority to use it for other purposes."

Justice Thomas further held that "[t]he majority's interpretation — that criminality turns on whether there is a single exception to a prohibition — also leads to awkward results." He continued, "Under its reading, an employee at a credit-card company who is forbidden to obtain the purchasing history of clients violates the Act when he obtains that data about his ex-wife — unless his employer tells him he can obtain and transfer purchase history data when an account has been flagged for possible fraudulent activity. The same is true of the person who, minutes before resigning, deletes every file on a computer."

Finally, Justice Thomas concluded that statutory history also reinforces the dissenters' interpretation of the CFAA. He wrote that the "original text of this Act expressly prohibited accessing a computer with authorization and then 'us[ing] the opportunity such access provides for purposes to which such authorization does not extend.'" The result is that the CFAA "applied when persons used computers for improper reasons — just like Van Buren indisputably did here."

Justice Thomas concluded by rejecting the majority's claim that a contrary ruling would result in the criminalization of a broad scope of conduct. He wrote, "I would not give so much weight to the hypothetical concern that the Government *might* start charging innocuous conduct and that courts *might* interpret the statute to cover that conduct." Justice Thomas added, "In the end, the Act may or may not cover a wide array of conduct because of changes in technology that have occurred since 1984. But the text makes one thing clear: Using a police database to obtain information in circumstances where that use is expressly forbidden is a crime."

> "The Supreme Court's decision [in *Van Buren*] will allow researchers and journalists to use common investigative techniques online without fear of CFAA liability. It clears away a major barrier to online anti-discrimination testing and research, which is necessary to hold powerful companies and platforms accountable."
>
> **— Esha Bhandari, American Civil Liberties Union's Speech, Privacy, and Technology deputy director**

Following the rulings, several experts and advocacy organizations praised the ruling as protecting investigative techniques employed by journalists and researchers. On June 4, 2021, First Amendment Watch at New York University staff writer Soraya Ferdman explained that although "the lawsuit is not focused on how journalists go about their work, it nonetheless caught the attention of press freedom groups because its outcome could implicate First Amendment activities such as traditional newsgathering and newer data-journalism methods." In particular, the case would implicate "data scraping," meaning "using computer programs to quickly extract large amounts of data from websites." Ferdman continued, "Scraping has been used to report on such issues as doctors who continue to practice after having been caught sexually abusing their patients, inhumane prison conditions, and to match missing people with the unidentified dead."

Ferdman quoted Grayson Clary, the Stanton Foundation National Security and Free Press Fellow at the Reporters Committee for Freedom of the Press (RCFP), who also praised the ruling. He said, "There will be questions to sort out about the exact scope of the ruling, but the Supreme Court made clear that interpreting the CFAA to criminalize routine internet use — including routine journalism — is out of bounds. And we're grateful that the Court acknowl-

SCOTUS Rulings, *continued on page 26*

SCOTUS Rulings, *continued from page 25*
edged our brief highlighting the risks of the Government's interpretation for press freedom."

In a June 3, 2021 statement, Esha Bhandari, deputy director of the American Civil Liberties Union's (ACLU) Speech, Privacy, and Technology Project, wrote, "This is an important victory for civil liberties and civil rights enforcement in the digital age.. . . The Supreme Court's decision will allow researchers and journalists to use common investigative techniques online without fear of CFAA liability. It clears away a major barrier to online anti-discrimination testing and research, which is necessary to hold powerful companies and platforms accountable."

In a separate June 3 statement, Alex Abdo, the litigation director at the Knight First Amendment Institute at Columbia University, called the ruling "an important and welcome decision that will help protect digital research and journalism that is urgently necessary." However, Abdo also contended that Congress "should amend the [CFAA] to eliminate any remaining uncertainty about the scope of the statute. It should also create a safe harbor for researchers and journalists who are working to study disinformation and discrimination online. Major technology companies should not have a veto over research and journalism that are manifestly in the public interest."

Additionally, some observers raised a concern with footnote 8 in the majority opinion, contending it could lead to future litigation. The footnote reads, "For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." In a June 3, 2021 piece, Electronic Frontier Foundation (EFF) senior staff attorney Aaron Mackey and deputy executive director and general counsel Kurt Opsahl called the footnote "a bit odd, as the bulk of the majority opinion seems to point toward the law requiring someone to defeat technological limitations on access, and throwing shade at criminalizing TOS violations. In most cases, the scope of your access once on a computer *is* defined by technology, such as an access control list or a requirement to reenter a password." They cited Berkeley School of Law professor Orin Kerr, who speculated that the footnote may have been "a necessary limitation to build the six justice majority."

Mackey and Opsahl added that "leaving the question open means that we will have to litigate whether and under what circumstance a contract or written policy can amount to an access restriction in the years to come." Nevertheless, they still generally praised the ruling, writing that it was "a victory for all Internet users, as it affirmed that online services cannot use the CFAA's criminal provisions to enforce limitations on how or why you use their service, including for purposes such as collecting evidence of discrimination or identifying security vulnerabilities." They also called the ruling "especially good news for security researchers, whose work discovering security vulnerabilities is vital to the public interest but often requires accessing computers in ways that contravene terms of service."

— Scott Memmel
Postdoctoral Associate
Silha *Bulletin* Co-editor

— Jonathan Anderson
Silha *Bulletin* Co-editor

— Samantha Brunn
Silha Research Assistant

— Claire Colby
Silha Research Assistant

Special Report: European and U.S. Entities Interpret EU-U.S. Privacy Shield, GDPR, and Other Data Privacy Rules and Regulations

In the spring and summer of 2021, actions by courts and authorities in the European Union (EU) raised significant data privacy implications, including for personal data transfers between the EU and United States.

- On June 15, 2021, the Court of Justice of the European Union (CJEU), the EU's top court, ruled that the General Data Protection Regulation (GDPR) allowed privacy authorities in different EU countries to pursue legal actions against tech companies and others even when they are not the lead regulators of those companies (meaning that the company is not based in their country).
- On May 14, 2021, the High Court of Ireland dismissed a challenge by Facebook Ireland Ltd. (Facebook) against the Data Protection Commission of Ireland's (DPC) inquiry into Facebook's trans-Atlantic data flows.
- In a July 16, 2021 decision, the Luxembourg National Commission for Data Protection (Commission Nationale pour la Protection des Données or CNPD) imposed an approximately $886.6 million (€746 million) fine against Amazon.com, Inc. (Amazon) for violation of the GDPR, marking the largest fine ever under the GDPR.
- On Aug. 16, 2021, a federal judge dismissed a class action complaint brought by a United Kingdom (UK) citizen accusing a U.S.-based digital advertising technology company of violating the UK GDPR. U.S. District Court for the Northern District of California Judge Phyllis J. Hamilton dismissed the case on forum *non conveniens* grounds. Hamilton's ruling marked the first addressing whether an individual from the UK can file a complaint based on violation of the UK GDPR in U.S. courts.
- On June 4, 2021, the European Commission released the final version of its implementing decision adopting new standard contractual clauses (SCCs) — template data transfer agreements meant to ensure "appropriate data protection safeguards for international data transfers" to countries that otherwise do not have an adequate level of data protection by EU standards.
- In the summer of 2021, talks between the EU and United States continued regarding the replacement of the EU-U.S. Privacy Shield (Privacy Shield).
- On June 18, 2021, the European Data Protection Board (EDPB) adopted its final recommendations providing guidance on the timeline for allowing data flows to continue to the United States and other non-EU countries. The final recommendations generally followed two draft documents released in November 2020, but included some changes. The documents raised concerns from observers that the guidance amounted to "hard data localization," which would significantly limit the amount of personal data that can be transferred out of the EU.
- On April 21, 2021, the European Commission transmitted to the European Parliament a draft proposal regarding the EU's handling of artificial intelligence (AI).

Background

In 2015, the European Court of Justice (ECJ) invalidated the EU-U.S. Safe Harbor framework. Case C-362/14, *Schrems v. Data Prot. Comm'r.* (*Schrems I*), 2015 E.C.R. I-650 (Oct. 6, 2015). Less than a year later, the European Commission officially adopted an amended version of the EU-U.S. Privacy Shield (Privacy Shield) to replace the Safe Harbor framework.

Following *Schrems I*, Facebook switched to using Standard Contractual Clauses (SCCs) believing that they would provide adequate privacy protections for its users. On Dec. 1, 2015, Max Schrems, an Austrian privacy advocate, filed a renewed complaint with Data Protection Commissioner of Ireland Helen Dixon, asking her to halt data transfers under SCCs. Schrems argued, among other claims, that such clauses do not provide adequate legal protection necessary to permit personal data transfers, including between Facebook Ireland and Facebook's U.S. headquarters.

Around the same time that Schrems filed his complaint, the Irish High Court overturned Dixon's earlier decision not to investigate Facebook in light of Schrems' original complaint. Dixon launched an investigation, which focused on two issues: whether the United States provides adequate legal protection to EU users whose data is transferred, and, if not, whether SCCs used by Facebook provided the level of protection that previously existed under the Safe Harbor framework.

In May 2016, Dixon issued a Draft Decision, finding that Schrems' complaint was "well-founded." Dixon wrote that U.S. law failed to provide adequate legal remedies to EU citizens. The Draft Decision further found that SCCs could not fully address such concerns, making them invalid under EU law. However, Dixon concluded that she did not have the authority to declare the SCCs invalid under EU law.

In October 2017, Irish High Court Justice Caroline Costello filed an opinion addressing whether SCCs violate applicable law and court precedent in both the EU and the United States. *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, [2016] No. 4809 P. (Oct. 3, 2017) (IR.). Costello concluded that neither the three ECJ decisions regarding SCCs in 2001, 2004, and 2010, nor the introduction of the Privacy Shield Ombudsperson mechanism, "eliminate[d] the well-founded concerns raised by the DPC in relation to the adequacy of the protection afforded to EU data subjects whose personal date is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States." However, she also found that the Irish High Court "lack[ed] jurisdiction to pronounce upon the validity of the SCC decisions." Meanwhile, the GDPR took effect on May 25, 2018, establishing new rules and obligations related to EU citizens' personal data.

On July 16, 2020, the CJEU released its ruling in *Schrems II*, in which it struck down the EU-U.S. Privacy Shield, the framework adopted in 2016 to govern trans-Atlantic data flow. Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited* (*Schrems II*), ECLI:EU:C:2020:559

Privacy, *continued on page 28*

Privacy, *continued from page 27*

(July 16, 2020). However, the Court also confirmed the validity of SCCs, but required companies to ensure that third-party countries outside the EU meet the Union's privacy standards and requirements. The full ruling is available online at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11629969. (For more information on *Schrems I* and *II*, as well as the Privacy Shield, see "CJEU Strikes Down EU-U.S. Privacy Shield, Confirms Validity of Standard Contractual Clauses" in the Summer 2020 issue of the Silha *Bulletin* and "The United States, the European Union, and the Irish High Court Wrangle Data Privacy Concerns" in the Fall 2017 issue.)

CJEU Ruling Allows Privacy Authorities in Any EU Country to Enforce the GDPR Against Facebook, Other Tech Companies

On June 15, 2021, Facebook received another adverse ruling in the European Union (EU) concerning its data privacy practices. The Court of Justice of the European Union (CJEU) held that under the General Data Protection Regulation (GDPR), data protection agencies across the EU can bring legal actions against technology companies and others even if they are not the primary privacy regulator of those companies. Case C-645/19, *Facebook Ireland Limited v. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:483 (June 15, 2021). The result is that Facebook, although headquartered in Ireland, can face data privacy litigation in other EU countries. Although some observers praised the ruling as providing extra protections for data privacy, others raised concerns that tech companies would now face more litigation from a variety of EU authorities.

The case arose in 2015 when the Belgian Privacy Commission sought an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium (together "Facebook") "aiming to put an end to alleged infringements of data protection laws by Facebook," including "the collection and use of information on the browsing behaviour of Belgian internet users, whether or not they were Facebook account holders, by means of various technologies, such as cookies, social plug-ins 1 or pixels." The Belgian Privacy Commission was later replaced by the Data Protection Authority of Belgium (DPA).

In February 2018, the Dutch-language Court of First Instance (Nederlandstalige rechtbank van eerste aanleg Brussel) held that the "social network had not adequately informed Belgian internet users of the collection and use of the information concerned. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid." In March 2018, Facebook appealed the ruling to the Court of Appeal (Hof van beroep te Brussel), which held that "it solely has jurisdiction to give a ruling on the appeal brought by Facebook Belgium."

> "Given the existing bottlenecks in the GDPR cross-border enforcement system, all national authorities must be able, under certain conditions, to proactively take matters into their own hands and use their full powers when our rights are trampled on."
>
> **— Monique Goyens, European Consumer Organisation director-general**

Previously, the GDPR's "one-stop-shop" mechanism had provided the Data Protection Commission of Ireland (DPC) with special status to pursue GDPR actions against Facebook and other companies based in Ireland. The main issue before the CJEU was whether the Belgian DPA under the GDPR "may bring an action against Facebook Belgium, since it is Facebook Ireland which has been identified as the controller of the data concerned."

In its June 15, 2021 opinion, the CJEU first held that the GDPR "must be interpreted as meaning that a supervisory authority of a Member State which . . . has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross-border data processing." The Court held that this was the case "even though it is not the 'lead supervisory authority' . . . with respect to that data processing."

However, the Court emphasized that the use of that authority must be "exercised in one of the situations where that regulation confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation" and also "that the cooperation and consistency procedures laid down by that regulation are respected." The Court also noted that "close, sincere and effective" cooperation with the other national supervisory authorities is required under the GDPR.

The Court further concluded that "in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings[.]" However, the exercise of power must fall under the jurisdiction of the GDPR. The full ruling is available online at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=63E8DA34802E342F1B2F0C4EDAEB7E8E?text=&docid=242821&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=825670.

Following the ruling, several consumer advocates praised the decision. In a June 15, 2021 statement, Monique Goyens, director-general of the European Consumer Organisation (BEUC), a consumer rights group, said, "This is a positive development in the bid to have our privacy respected regardless of where the company is established in the EU.. . . Given the existing bottlenecks in the GDPR cross-border enforcement system, all national authorities must be able, under certain conditions, to proactively take matters into their own hands and use their full powers when our rights are trampled on."

Conversely, tech industry observers expressed concern about the potential ramifications of the decision. In a statement, Alex Roure, senior policy manager at the Computer & Communications Industry Association (CCIA), a major tech industry lobbyist, contended that the ruling "opened the back door for all national data protection enforcers to start multiple proceedings against

companies." The statement continued, "Data protection compliance in the EU risks becoming more inconsistent, fragmented, and uncertain. We urge national authorities to be cautious about launching multiple proceedings that would weaken legal certainty and further complicate data protection compliance in the EU."

A June 15 *Fortune* magazine piece similarly concluded that "Big Tech is likely to face more privacy enforcements — and more fines — in the European Union" following the CJEU ruling.

Irish High Court Dismisses Facebook's Challenge to Irish Data Protection Commission Procedures

On May 14, 2021, the High Court of Ireland rejected a challenge by Facebook Ireland Ltd. (Facebook) against a Data Protection Commission of Ireland (DPC) draft decision focusing on whether the social media company can continue to transfer European Union (EU) citizens' data between the EU and United States. *Facebook Ireland Ltd v. Data Protection Commission*, [2020] No. 617 JR., No. 126 COM. (May 14, 2021) (IR.). Following the ruling, observers noted the potential significance of the ruling for Facebook and other companies collecting EU citizens' personal data.

The case arose after the Court of Justice of the European Union's (CJEU) ruling in *Schrems II* when the DPC "commence[d] an 'own volition' inquiry . . . to consider whether the actions of Facebook Ireland Ltd . . . in making transfers of personal data relating to individuals in the European Union/ European Economic Area are lawful and whether any corrective power should be exercised by the DPC in that regard." On Aug. 28, 2020, the DPC issued a Preliminary Draft Decision (PDD) to Facebook. Among the provisions was that Standard Contractual Clauses (SCCs) may not be sufficient for Facebook to use given that U.S. law does not provide an equivalent level of protection for data privacy to that of the EU.

The social media company summarily "took issue, on several grounds, with the decision by the DPC to commence the inquiry by means of the PDD and with the procedures adopted by the DPC." Similarly, privacy advocate Max Schrems "also took issue with the DPC's decision and procedures on a number of grounds, some of which overlapped to an extent with the grounds advanced by [Facebook]." Although Facebook and Schrems initially "applied successfully to be joined as a notice party to the other's judicial review proceedings," Schrems ultimately reached a settlement in January 2021 with the DPC prior to a scheduled hearing set for the same month.

Facebook advanced several arguments why "the DPC's decision to issue the PDD and to adopt the procedure which it has adopted should be quashed," including that the DPC's decision violated the General Data Protection Regulation (GDPR). Facebook argued that the decision breached the GDPR "by virtue of[:]

- the DPC's failure to conduct any investigation before issuing the PDD;
- a breach of [Facebook]'s legitimate expectation that procedures published by the DPC in its 2018 Annual Report and on its website, and followed by the DPC in other inquiries, would be followed in respect of the DPC's inquiry;
- breaches of [Facebook's] right to fair procedures, including premature judgment of the issues by the DPC and a failure to afford sufficient time . . . to make submissions to the DPC;
- a failure by the DPC to take into account relevant considerations and, in particular, to await publication by the European Data Protection Board ("EDPB") of guidance/recommendations to assist controllers and processors as regards the use of what are called "supplementary measures" to ensure adequate protection for data subjects when transferring data to third countries;
- a breach of [Facebook's] right to equal treatment and non-discrimination;
- a breach of the DPC's obligation to act proportionately by subjecting [Facebook] to simultaneous inquiries[.]"

> "Data protection compliance in the EU risks becoming more inconsistent, fragmented, and uncertain. We urge national authorities to be cautious about launching multiple proceedings that would weaken legal certainty and further complicate data protection compliance in the EU."
>
> **— Alex Roure, Computer & Communications Industry Association senior policy manager**

In response, the DPC contended, among other claims, that Facebook was "fundamentally mistaken when it asserts that no investigation was carried out by the DPC before issuing the PDD and further maintains that [Facebook] was invited to make submissions on the facts and on the law and to provide such further information as it felt necessary in response to the preliminary views set out in the PDD." The DPC also "dispute[d] the allegations of breaches of fair procedures, and asserts that no extension of time was sought by [Facebook] to make a submission in response to the PDD and that no extension of time was refused by the DPC," among other claims.

Schrems "support[ed] the quashing of the PDD on the grounds that it infringes his legitimate expectation that his complaint would be determined by the DPC following the CJEU's judgment in *Schrems II*." However, Schrems also disagreed with Facebook on several grounds, including "the relief[] being sought by FBI on the grounds of an alleged departure by the DPC from its published procedures in issuing the PDD and commencing the own-volition inquiry."

On May 14, 2021, Irish High Court Justice David Barniville released his opinion, in which he "concluded that the decision of the DPC to issue the PDD and to adopt the procedures notified to [Facebook] and Mr. Schrems are amenable to judicial review" and that Facebook "must fail on [each of the grounds of challenge] and that it is, therefore, not entitled to any of the reliefs claimed in the proceedings."

Barniville concluded that the DPC did not breach "its obligations under the GDPR" and was not "otherwise in breach of EU law or contrary to the requirements or expectations of the CJEU in *Schrems II* in terms of the investigation or inquiry carried out by the DPC prior to issuing the PDD or in terms of the further investigation and inquiry envisaged by the terms of the PDD." Barniville provided several reasons for this conclusion, including

Privacy, *continued on page 30*

Privacy, *continued from page 29*

that he was "satisfied that at the time the inquiry was commenced by means of the PDD[,] the DPC was in possession of a vast amount of information by reason of its involvement and the involvement of its predecessor dating back to Mr. Schrems' original complaint in 2013." He also reasoned that "further investigations were conducted prior to the DPC's decision to commence the inquiry by issuing the PDD, that its investigations are continuing, that [Facebook] was and is entitled to make submissions on all relevant matters of fact and law and on any other matter it considers relevant, and that the Commissioner/DPC will consider those submissions before reaching her/its decision[.]" Barniville added, "I am satisfied that the DPC had not reached a decision or drawn conclusions in the inquiry at the time the PDD was issued."

Barniville then walked through each of the remaining challenges by Facebook, two of which the company "did not maintain." Barniville wrote, "Of the remaining grounds of challenge, I have concluded that those grounds must be rejected and that [Facebook] has not established any basis for impugning the DPC's decision or the PDD or the procedures for the inquiry adopted by the DPC." The full ruling is available online at: https://noyb.eu/sites/default/files/2021-05/High%20Court%20Judgement%202021-05-14.pdf.

In a May 14, 2021 article for *TechCrunch*, senior reporter Natasha Lomas wrote that Barniville's ruling "has huge potential operational significance for Facebook, which may be forced to store European users' data locally if it's ordered to stop taking their information to the U.S. for processing." She continued, "The last of the bungs which have been used to delay regulatory action in Ireland over Facebook's EU-U.S. data flows are finally being extracted — and the DPC must decide on the complaint. Or, to put it another way, the clock is ticking for Facebook's EU-U.S. data flows."

However, Lomas also noted that "[a]s ever in this complex legal saga — which has been going on in various forms since an original 2013 complaint made by European privacy campaigner Max Schrems — there's still some track left to run." She reasoned that "[w]hen Ireland (finally) decides it won't mark the end of the regulatory procedures[.]. . . A decision by the DPC on Facebook's transfers would need to go to the other EU [Data Protection Authorities (DPAs)] for review — and if there's disagreement there (as seems highly likely, given what's happened with draft DPC GDPR decisions) it will trigger a further delay (weeks to months) as the European Data Protection Board seeks consensus." Lomas added, "If a majority of EU DPAs can't agree the Board may itself have to cast a deciding vote. So that could extend the timeline around any suspension order. But an end to the process is, at long last, in sight."

In a May 20 interview with CNBC, Cillian Kieran, founder and CEO of data privacy software start-up Ethyca, asserted that requiring Facebook to process EU data within EU member states "could be a massive blow for the revenue model of Facebook." He added, "The recent ruling, and the potential suspension of Facebook's data flows, suggest serious challenges for other U.S. companies to conduct international business, especially those with fewer resources than Facebook to navigate legal procedures.. . . The news raises the stakes for U.S. businesses to meet global standards for data protection, not only to earn users' trust in the marketplace but also — on a more fundamental level — to be able to bring their product to important markets in the first place."

In a May 20, 2021 commentary, Vinson & Elkins partner Devika Kornbacher, senior associate Christopher W. James, and law clerk Lara McMahon contended that Barniville's ruling could have significant implications for SCCs. They wrote that although "[t]he individualized inquiry into Facebook's specific data protection safeguards casts doubt on the likelihood of a *per se* prohibition on SCCs[,] . . . the efficiency of adopting SCCs may be lost if your company must still prove up its entire data protection program to EU regulators."

Kornbacher, James, and McMahon also noted that "the U.S. Department of Commerce and the European Commission are currently negotiating an 'enhanced' Privacy Shield agreement to replace the version invalidated by the CJEU in *Schrems II*. Recognizing the disruption the *Schrems II* decision caused to EU-U.S. data flows, the European Union and United States are arguably more motivated now than ever before to implement a workable solution."

Meanwhile, on Sept. 2, 2021, the DPC announced in a press release that it had fined WhatsApp Ireland Ltd. (WhatsApp), an instant-messaging platform owned by Facebook, $267 million (€225 million) for violating the GDPR. According to the press release, the DPC opened an investigation in December 2018 into "whether WhatsApp has discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of WhatsApp's service."

The DPC found that WhatsApp failed to provide EU citizens sufficient information about how their personal information was collected and used, including how WhatsApp shares the data with Facebook. In addition to the fine, the DPC "also imposed a reprimand along with an order for WhatsApp to bring its processing into compliance by taking a range of specified remedial actions." The full press release is available online at: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry.

On July 28, 2021, the European Data Protection Board (EDPB) had adopted a binding decision, which required the DPC to increase its initial $59 million (€50 million) fine, which was finalized as $267 million (€225 million). The EDPB's binding decision is available online at: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en.

Amazon Faces Record Fine Under GDPR

On July 30, 2021, *Bloomberg* reported that the Luxembourg National Commission for Data Protection (Commission Nationale pour la Protection des Données "CNPD"), Luxembourg's independent public data protection authority, imposed an $886.6 million (€746 million) fine against Amazon.com, Inc. (Amazon) for violation of the General Data Protection Regulation (GDPR). The fine marked the largest such penalty ever imposed under the GDPR.

IT Pro, a publication focused on technology news and reviews for IT professionals, reported on Aug. 2, 2021 that CNPD's decision "was made on the basis of the one-stop-shop principle set out in Article 60 of GDPR. This means Luxembourg was nominated as the lead supervisory authority in a case against

Amazon based on alleged violations that occurred across borders and in several EU territories. The CNPD was chosen to investigate Amazon because the [company]'s European headquarters is based in Luxembourg."

In June 2021, the Court of Justice of the European Union (CJEU), the EU's top court, had ruled that the GDPR allowed privacy authorities in different EU countries to pursue legal actions against tech companies and others even when they are not the lead regulators of those companies. Case C-645/19, *Facebook Ireland Limited v. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:483 (June 15, 2021). *Silicon Republic*, a European publication focusing on science and technology news, noted on Aug. 3, 2021 that "[t]his may lead to multinationals facing multiple simultaneous investigations from different regulators, especially given the criticism [the Data Protection Commission of Ireland's (DPC)] has faced for allegedly dragging its feet in numerous cases against big companies."

On July 30, 2021, *Politico* technology reporter Vincent Manancourt wrote that the fine meant Luxembourg was set to "emerge as Europe's unlikely new privacy sheriff." He continued, "The tiny, tax-light country has long been accused of being soft on the corporations that make it their home.. . . But the record sum for a U.S. heavyweight has thrust Luxembourg to the front line of Europe's war on Big Tech. In doing so, it asks tough questions of Ireland, which regulates the lion's share of Silicon Valley companies."

In a July 16 decision, the CNPD imposed the record fine against Amazon for allegedly processing personal data in violation of the GDPR. Amazon disclosed the fine in a July 30 filing with the U.S. Securities and Exchange Commission (SEC). In the filing, Amazon noted that the company "believe[d] the CNPD's decision to be without merit and intend to defend ourselves vigorously in this matter." The filing is available online at: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_7.

Amazon added in a separate statement, "There has been no data breach, and no customer data has been exposed to any third party.. . . These facts are undisputed. We strongly disagree with the CNPD's ruling." Amazon explained that the CNPD decision concerns "how we show customers relevant advertising." *Bloomberg* reported that the fine stems from a 2018 complaint from French privacy rights group La Quadrature du Net. In a statement, Bastien Le Querrec, a member of La Quadrature's litigation team, praised the CNPD's decision. "It's a first step to see a fine that's dissuasive, but we need to remain vigilant and see if the decision also includes an injunction to correct the infringing behavior," he wrote.

In a July 30 blog post, La Quadrature du Net expanded on the problems with Amazon's practices, contended that "advertising targeting system imposed by Amazon" was being carried out "without our free consent." The post added, "It is the targeted advertising system itself that our complaints intend to wipe out as a whole, and not a few occasional security breaches.. . . The model of economic domination based on the exploitation of our privacy and our free will is deeply illegitimate and contrary to all the values that our democratic societies claim to defend. We will therefore continue to fight against this domination, with your help."

Pinsent Masons LLP partner Wouter Seinen noted in a July 30 commentary that "[t]he unconfirmed reports of the origins of this decision highlight the increased risks businesses face from complaints raised by private individuals and interest groups. We have already seen a rise in data protection-related litigation in Europe and now this case of the CNPD's in Luxembourg against Amazon shows their potential influence in driving enforcement action by data protection authorities. This case is unlikely to be the last of this kind."

Conversely, *CPO Magazine* senior correspondent Scott Ikeda contended on June 15, 2021 that although the fine against Amazon would set a record under the GDPR, "it is far below the maximum of 4% of global turnover allowed by the privacy bill's rules. The proposed amount totals out to about 0.1% of Amazon's annual $386.1 billion in revenue. This new case illustrates a pattern of regulators taking it relatively easy on big tech, and often reducing large initial propositions after long periods of deliberation."

U.S. Federal Judge Dismisses Class Action Lawsuit Seeking to Apply the UK GDPR

On Aug. 16, 2021, U.S. District Court for the Northern District of California Judge Phyllis J. Hamilton granted a motion to dismiss in a case brought by a United Kingdom (UK) citizen, Hugo Elliott, in which he alleged that a U.S.-based digital advertising technology company, PubMatic, Inc. (PubMatic), violated the UK General Data Protection Regulation (UK GDPR). *Elliott v. Pubmatic, Inc.*, No. 21-cv-01497-PJH, 2021 WL 3616768 (N.D. Cal. 2021).

The case arose regarding Delaware-based PubMatic's use of targeted advertising and "assist[ing] websites with the management and sale of their advertising space." PubMatic's principal place of business is in Redwood City, Calif. Elliott was one user who browsed their website, among others, while residing in England. According to Hamilton, PubMatic, as part of these business practices, "placed unique and therefore individuating identifiers in the form of cookies on Elliott's device and used those uniquely identifying cookies to monitor and track Elliott's U.K.-based online activities."

In a class action complaint, Elliott contended that he "was harmed by PubMatic's alleged internet cookie placement practices in violation of his U.K. data privacy rights." He sought to represent a class of "[a]ll persons residing or who resided in England and Wales who used Chrome, Edge, or Internet Explorer browsers and have had a PubMatic cookie placed on their device during the Relevant Time Period," namely May 25, 2018, through the present.

Elliott brought the action under the UK GDPR, which was adopted in 2018 to implement the European Union (EU) GDPR after the UK left the EU in Brexit. The UK GDPR "contains 'materially identical' obligations to the EU GDPR," though with "one substantive difference relevant here: unlike the EU's GDPR, the U.K. GDPR does not require complaints to be filed in a European court." Elliott claimed that this allows "UK plaintiffs to sue outside of the UK, including within the United States." In June 2021, PubMatic filed a motion to dismiss Elliott's first amended complaint.

Judge Hamilton first noted that a U.S. district court "has discretion to decline to exercise jurisdiction in a case where litigation in a foreign forum would be more convenient for the parties," citing *Lueck v. Sundstrand Corp.*, 236 F.3d 1137, 1142 (9th Cir. 2001). However,

Privacy, *continued on page 32*

Privacy, *continued from page 31*

"[b]efore dismissing an action based on forum *non conveniens*," a district court must "analyze whether an adequate alternative forum exists, and whether the balance of private and public interest factors favors dismissal."

Hamilton concluded that "[t]here is no argument — there exists an adequate alternative forum. Defendant is amenable to process in the U.K. if this court dismisses the case on forum *non conveniens* or international comity grounds." She added, "Both sides acknowledge that the courts of the U.K. would serve as an adequate alternative forum."

Hamilton also reasoned that although "a plaintiff's choice of forum is typically entitled to substantial deference, the choice of Mr. Elliott, as a foreign plaintiff, deserves less deference." This was especially the case given that "Elliott seeks to represent a putative class comprised solely of foreign putative class members."

Turning to the private interests in the case, Hamilton noted that such factors included: "(1) the residence of the parties and the witnesses; (2) the forum's convenience to the litigants; (3) access to physical evidence and other sources of proof; (4) whether unwilling witnesses can be compelled to testify; (5) the cost of bringing witnesses to trial; (6) the enforceability of the judgment; and (7) all other practical problems that make trial of a case easy, expeditious and inexpensive." Hamilton concluded that these factors "do not cut sharply in favor of either the U.S. or the U.K. as a forum. The court does not consider all the private interest factors again here, but they generally come out neutral where neither jurisdiction is entirely convenient to either side and the locations of necessary evidence and witnesses remains unclear."

However, the public interest factors — "(1) the local interest in the lawsuit, (2) the court's familiarity with the governing law, (3) the burden on local courts and juries, (4) congestion in the court, and (5) the costs of resolving a dispute unrelated to a particular forum" — "weigh heavily in favor of the U.K. as the appropriate forum for this dispute." Regarding the first factor, Hamilton found that it weighs in favor of the UK because Elliott "is a resident of England and suffered his alleged injuries in England; the Proposed Class is made up entirely of residents or former residents of England and Wales, who suffered any alleged injuries in England and Wales; and Plaintiff's claims expressly arise only under (a new) U.K. law."

Addressing the second public interest factor, Hamilton found that it "weighs against this court as the appropriate forum. This court lacks familiarity with the U.K. GDPR, a law that is still being developed in the U.K. It would be burdensome for the court to familiarize itself with, interpret, and apply this foreign law." Regarding the final factors, Hamilton concluded that they "additionally weigh against this forum where plaintiff asks California jurors to apply foreign law to award damages to an entirely foreign class."

Hamilton therefore concluded that "[o]n balance, the private interest factors and the public interest factors together weigh in favor of dismissal on forum *non conveniens* grounds. California has little interest in hosting this dispute, and PubMatic's willingness to submit to U.K. jurisdiction mitigates against this foreign plaintiff's choice of forum. The court therefore dismisses the case on forum *non conveniens* grounds."

Second, Hamilton turned to international comity, which "is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws," citing *In re Simon*, 153 F.3d 991, 998 (9th Cir. 1998). Here, Hamilton once again concluded that "[t]he courts of the U.K. provide an adequate alternative, and defendant already certified its acceptance of U.K. jurisdiction over this case should it be dismissed here."

Hamilton further held that "this case is properly adjudicated in a foreign state. The U.K. has a strong interest in addressing injuries to English and Welsh subjects, particularly injuries to rights created by U.K. legislation.. . . Moreover, the U.K. has a strong interest in interpreting and applying its own regulatory scheme for Internet privacy, a scheme largely lacking in precedent. All of these considerations lead to the conclusion that this court must abstain from this case." Hamilton therefore "alternatively dismisse[d] the case on international comity grounds."

On Aug. 17, 2021, *Law360* noted that the ruling was "the first to weigh in on whether U.K. plaintiffs can sue in U.S. courts over alleged data protection violations."

European Commission Publishes New Standard Contractual Clauses (SCCs)

On June 4, 2021, the European Commission adopted new standard contractual clauses (SCCs) governing the transfer of European Union (EU) citizens' personal data to countries outside the EU. Commission Implementing Decision (EU), No. 2021/914 (June 4, 2021). Following the release of the new SCCs, several observers pointed out key changes from previous versions, though they also reiterated the unknown future of the clauses in relation to data privacy more broadly.

In the final version of its implementing decision (decision), dated June 4, 2021, the European Commission first set out the reasons for amending SCCs, including that "[t]echnological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade. At the same time, it is necessary to ensure that the level of protection of natural persons guaranteed by [EU regulations]," including when such data is "transferred to a third country."

The decision continued, "[T]he digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. This calls for modernisation of the standard contractual clauses to reflect those realities better, by covering additional processing and transfer situations, and to allow a more flexible approach, for example with respect to the number of parties able to join the contract."

The decision then laid out the new SCCs, which were "considered to provide appropriate safeguards [under EU laws and regulations] for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-) processor whose processing of the data is not subject to [EU regulations] (data importer)." The full decision is available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

In a June 7, 2021 "Privacy Law Blog" commentary, Proskauer Rose

LLP partner Ryan P. Blaney, attorney Vishnu V. Shankar, and associate Kelly McMullon highlighted the key features of the new SCCs, of which "[m]any organizations that transfer or receive personal data originating in the European Economic Area (EEA) outside the EEA will be required to implement . . . with their customers, suppliers and affiliates by December 2022 to comply with the [GDPR]."

First, the commentary emphasized the "modular" nature of the new SCCs, which "allow[] controller-to-controller and controller-to-processor data transfers and also processor-to-controller, and processor-to-processor transfers, new forms that were not provided for under the old SCCs." The commentary called these new forms "advantageous in complex data processing chains where the old SCCs may have been too rigid." Furthermore, the new SCCs now explicitly state that data exporters can be non-EU entities.

Second, the updated SCCs "have *Schrems II* in mind." The commentary explained that the ruling "requires companies that use SCCs to undertake a TIA [(also known as a "*Schrems* privacy impact assessments")] to determine if so-called 'supplementary measures' (for example, encryption) need to be put into place (in addition to those measures required by the SCCs) in light of the laws of the country of data import."

Third, the new SCCs impose "[o]bligations regarding certain governmental data access requests," as well as additional requirements related to accountability. Such provisions include "(i) maintaining data processing records; (ii) notifying data subjects about the details of the data transfers; (iii) personal data breaches; (iv) whether/how parties may contractually limit their liability under the SCCs (including under companion commercial agreements); and (v) choice of law and dispute resolution."

Fourth, the new SCCs include provisions for "[o]nward data transfers," meaning the transferring of data to a fourth party, fifth party, etc. Fifth, the commentary asserted that the new SCCs placed "[r]enewed focus on cybersecurity" under the GDPR, including by requiring "a detailed description of the technical and organisational measures implemented is set out for each of the modules."

Finally, the commentary noted that "the new SCCs also permit new parties to accede to executed (new) SCCs more easily through a 'docking' clause rather than requiring the SCCs to be re-executed every time that a new party (such as a new group company) is to be added." The full commentary is available online at: https://privacylaw.proskauer.com/2021/06/articles/gdpr/navigating-the-new-standard-contractual-clauses-for-international-data-transfers-under-the-gdpr/.

> "Given the potential extent of the obligations created by the New SCCs, and the limited transition periods, businesses will need to act quickly to analyze their current compliance with the New SCCs, the nature of their data transfers, and the correlating contractual obligations[.]"
>
> **— Carol A. F. Umhoefer and Andrew Serwin, DLA Piper partners**

In a June 7, 2021 IAPP commentary, Fieldfisher partner Phillip Lee wrote that the European Commission should be "lauded for its efforts to strike a difficult balance between the interests of data subjects, the looming specter of a potential '*Schrems III*,' and the needs of data exporting organizations." However, he noted that "only time will tell" whether the new SCCs will be successful.

In a June 8 commentary, DLA Piper partners Carol A. F. Umhoefer and Andrew Serwin laid out several "[p]ractical impacts" of the new SCCs, including that they require "new and significant obligations for data importers, particularly importers acting as controllers. Adopting and complying with the New SCCs may require considerable effort for these importers, particularly those that are not otherwise directly subject to GDPR." They added, "Given the potential extent of the obligations created by the New SCCs, and the limited transition periods, businesses will need to act quickly to analyze their current compliance with the New SCCs, the nature of their data transfers, and the correlating contractual obligations, in order to adopt or update their GDPR compliance program, develop a strategy for updating templates to include the New SCCs, and ultimately conclude New SCCs for current and ongoing transfers."

Umhoefer and Serwin also clarified that the "new SCCs will not apply for transfers of personal data *from the UK* to a third country. Data exports from the UK should continue to be based on the existing SCCs until the UK publishes its own SCCs."

In a June 14 piece published by *The National Law Review*, several Ogletree, Deakins, Nash, Smoak & Stewart, P.C. attorneys provided a series of recommendations to employers currently using SCCs to transfer EU personal data, including that although they "have 18 months to transition to the new controller-to-processor SCCs and third-country SCCs, they may want to consider beginning the transition process immediately." This is for several reasons, including that "[e]mployers and their data processors must conduct the risk assessments and implement the technical, contractual, and organizational supplementary measures required by *Schrems II* as part of the transition."

Discussions Continue About EU-U.S. Privacy Shield Successor

In the summer of 2021, talks continued regarding the replacement of the EU-U.S. Privacy Shield (Privacy Shield). On July 1, 2021, the International Association of Privacy Professionals (IAPP) noted that during one of its live events, U.S. Department of Commerce Deputy Assistant Secretary for Services Christopher Hoff provided an update on the talks between the EU and U.S. regarding a replacement to the Privacy Shield agreement. "I definitely would assuage anyone's fears that we are at the beginning of this negotiation. We are not at the beginning of this negotiation," Hoff said during the event. "A good diplomatic friend mentioned to me allies get into these conversations where there's often 95% agreement and 5% disagreement. Without saying that that's where we are, it feels like that is essentially where we are. I am confident that we will figure out the remaining percent, whatever percent that it is. We are absolutely not at the beginning at these conversations and we will figure out the rest."

Privacy, *continued on page 34*

Privacy, *continued from page 33*

IAPP reported that the talks around a new Privacy Shield agreement were part of the discussions between President Joe Biden and European Commission President Ursula von der Leyen at a June 15, 2021 summit in Brussels. The two leaders took several actions at the summit, including establishing a new "high-level U.S.-EU Trade and Technology Council (TTC)." According to the White House, the goals of the TTC will be to "grow the bilateral trade and investment relationship; to avoid new unnecessary technical barriers to trade; to coordinate, seek common ground, and strengthen global cooperation on technology, digital issues, and supply chains; to support collaborative research and exchanges; to cooperate on compatible and international standards development; to facilitate regulatory policy and enforcement cooperation and, where possible, convergence; to promote innovation and leadership by U.S. and European firms; and to strengthen other areas of cooperation." The full White House statement is available online at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

The European Commission explained that the TTC "will serve as a forum for the United States and European Union to coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on shared democratic values." The full press release is available online at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

"Data transfers and data flows are foundational to the rest of any trade and technology conversation. It's the lifeblood of trade and technology and of business. Privacy Shield is a very big part of the conversation in Brussels," Hoff said. "We are following up on those high-level leaders and principles meetings in Brussels with more and more and more meetings, including today with the commission." However, Hoff did not provide a definitive timeline on a new Privacy Shield agreement.

European Data Protection Board Releases Guidance on Data Transfers to Non-EU Countries, Raising Concerns about Data Localization

On Nov. 10, 2020, the European Data Protection Board (EDPB) published two draft documents providing guidance related to personal data transfers from the European Union (EU) to non-EU countries, including the United States. The documents raised concerns from observers, including that the guidance amounted to "hard data localization," meaning personal data could not or would not be transferred outside the EU. On June 18, 2021, the EDPB adopted its final recommendations, which generally followed the draft documents, but included some changes.

The first document published by the EDPB in November 2020 was titled, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." The document first cited the Court of Justice of the European Union's (CJEU) ruling in *Schrems II*, noting that "the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."

Second, the document contended that standard contractual clauses (SCCs) and other transfer mechanisms "do not operate in a vacuum" and that the General Data Protection Regulation (GDPR) requires that "controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools."

Finally, the document presented six steps that data exporters should follow regarding transfers of EU citizens' personal data to non-EU countries. The document stated that the steps serve as "a roadmap . . . to take in order to find out if you (the data exporter) need to put in place supplementary measures to be able to legally transfer data outside the EEA."

The first step is to "know your transfers," meaning that exporters should be "aware of where the personal data goes [because it] is . . . necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed."

The second step advises that exporters "verify the transfer tool your transfer relies on," especially if the European Commission had not "already declared the country, region or sector to which you are transferring the data as adequate." The tools provided for by the GDPR include SCCs, binding corporate rules (BCRs); codes of conduct; certification mechanisms; [and] ad hoc contractual clauses."

The third step recommends that exporters "assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer." A main consideration should be the relevant law and legislation in that country.

The fourth step advises exporters to "identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence."

The fifth step then requires the exporter to "take any formal procedural steps the adoption of your supplementary measure may require."

The final step recommended that exporters "re-evaluate at appropriate intervals the level of protection afforded to the data you transfer to third countries and to monitor if there have been or there will be any developments that may affect it. The principle of accountability requires continuous vigilance of the level of protection of personal data." The full draft document is available online at: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

The second draft document published by the EDPB on Nov. 10, 2020 was titled, "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures." The purpose of the document was to "further develop the European Essential Guarantees [(EEGs)]," which were originally drafted after *Schrems I*. The document clarified that the EEGs were drafted to ensure "interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society." According to the document, the EEGs represent just one "part of the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU but do not aim on their own at defining all the elements which are necessary to consider that a third country provides such a level of protection in accordance with Article 45 of the GDPR."

The updated guidance on the EEGs aimed to "provide elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not."

The document then detailed the four EEGs, which include:

A. Processing should be based on clear, precise and accessible rules;

B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;

C. An independent oversight mechanism should exist; and

D. Effective remedies need to be available to the individual.

The document detailed the relevant EU laws and regulations comprising each of the EEGs, including requirements under the GDPR.

According to the document, "the assessment of the third country surveillance measures against the EEG may lead to two conclusions," namely that the third country's legislation "does not ensure the EEG requirements" or that it does satisfy the EEGs. If the latter is the case, data exporters need "to ensure that the law at stake will not impinge on the guarantees and safeguards surrounding the transfer, in order for a level of protection essentially equivalent to that guaranteed within the EU to be still provided."

The document emphasized that each of the EEGs "are to be seen as core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection. They should not be assessed independently, as they are closely interlinked, but on an overall basis, reviewing the relevant legislation in relation to surveillance measures, the minimum level of safeguards for the protection of the rights of the data subjects and the remedies provided under the national law of the third country." The full draft document is available online at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

Following the publication of the draft documents, several observers raised concerns that they would "have the effect of hard data localization, limiting many routine data flows from the EU." In a Jan. 26, 2021 commentary, IAPP member contributors Peter Swire and DeBrae Kennedy-Mayo outlined several significant effects of data localization, including that "numerous major data flows, beyond digital platforms, . . . would be affected." One disruption "could include pharmaceuticals research, which would be especially important to consider during the COVID-19 pandemic, when sharing of personal data is so important concerning the safety and efficacy of vaccines and treatments, as well as other medical information."

> "The impact of *Schrems II* cannot be underestimated: Already international data flows are subject to much closer scrutiny from the supervisory authorities who are conducting investigations at their respective levels. The goal of the EDPB Recommendations is to guide exporters in lawfully transferring personal data to third countries while guaranteeing that the data transferred is afforded a level of protection essentially equivalent to that guaranteed within the European Economic Area."
>
> **— Andrea Jelinek, European Data Protection Board chair**

Swire and Kennedy-Mayo further contended that there are "technical obstacles to providing online services in a regime of hard data localization" and that "[s]eemingly simple and lawful international transfers may include background processing that may not be consistent with hard data localization." Finally, they argued that hard data localization can lead to cybersecurity risks, namely because "information can be an important component of defending against and responding to cyberattacks."

In a Nov. 17, 2020 piece for the "European Law Blog," Université Grenobles-Alpes professor Théodore Christakis found that "there are two central conclusions that emerge from the EDPB publications," including first that "[t]hird countries might rarely if ever meet the EEG requirements. This means that, beyond the 8 sovereign States/12 entities that have the opportunity of benefiting today from an EU adequacy decision, few other countries might be considered as offering a protection 'essentially equivalent' to that offered by EU law." Second, in the event that "third countries are not considered as 'adequate/essentially equivalent,' then data transfers to them are lawful only if supplemental measures are adopted by the data exporter. The EDPB Guidance seems nonetheless to prohibit almost all such transfers when the personal data is readable in the third country."

Christakis therefore concluded that there are three possible scenarios that could play out. First, companies could "ignore the EDPB guidance or to pretend that they are taking it into consideration for their everyday transactions while in reality hardly doing so." Second, Christakis contended that "[i]f European data has almost no way of leaving Europe (that is, in a readable format) that means that it needs to remain in Europe. This is called data localization." He added, "Before blindly embracing data localisation, Europe should better understand what data localisation technically means and study thoroughly what the adverse consequences of such policies could be." Finally, Christakis asserted that "[i]f the aforementioned solutions are not satisfactory and if Europe does not want to lower its standards of protection, then the only way out of this mess is for Europe to… change the world!"

On June 18, 2021, the EDPB adopted its final recommendations, which generally followed its draft documents. In particular, the final recommendations adopted the six steps data exporters should take to ensure they comply with the GDPR and EU law more broadly. The full final recommendations are available online at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasuretransferstools_en.pdf.

According to the EDPB, there were some modifications between its draft documents and final recommendations following public feedback. In a June

Privacy, *continued on page 36*

Privacy, *continued from page 35*

21 press release, the EDPB noted that "[a]mong the main modifications are: the emphasis on the importance of examining the practices of third country public authorities in the exporters' legal assessment to determine whether the legislation and/or practices of the third country impinge — in practice — on the effectiveness of the Art. 46 GDPR transfer tool; the possibility that the exporter considers in its assessment the practical experience of the importer, among other elements and with certain caveats; and the clarification that the legislation of the third country of destination allowing its authorities to access the data transferred, even without the importer's intervention, may also impinge on the effectiveness of the transfer tool."

In the press release, chair Andrea Jelinek was quoted as saying, "The impact of *Schrems II* cannot be underestimated: Already international data flows are subject to much closer scrutiny from the supervisory authorities who are conducting investigations at their respective levels. The goal of the EDPB Recommendations is to guide exporters in lawfully transferring personal data to third countries while guaranteeing that the data transferred is afforded a level of protection essentially equivalent to that guaranteed within the European Economic Area."

Jelinek continued, "By clarifying some doubts expressed by stakeholders, and in particular the importance of examining the practices of public authorities in third countries, we want to make it easier for data exporters to know how to assess their transfers to third countries and to identify and implement effective supplementary measures where they are needed. The EDPB will continue considering the effects of the *Schrems II* ruling and the comments received from stakeholders in its future guidance." The full press release is available online at: https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

European Commission Transmits Guidance on AI to European Parliament

On April 21, 2021, the European Commission transmitted a draft document outlining the regulation of artificial intelligence (AI) in the European Union (EU) to the European Parliament. Following the drafting of the AI regulation, which proposed the Artificial Intelligence Act (AIA), observers expressed mixed reactions to the draft regulation, calling it an important step for privacy associated with AI, but also having significant shortcomings. Observers also noted that the EU's approach differed from that of the United States, but that there were still opportunities for collaboration between the two in addressing privacy and security concerns arising from AI.

An explanatory memorandum connected to the draft regulation first laid out its reasons and objectives, including that "the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society."

Second, the memorandum named four "specific objectives" behind the regulation, including that the EU will:

- "ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."

Finally, the draft regulation laid out the provisions of the AIA. Title I included a broad definition of AI, including "systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content." An AI system is defined as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with[.]"A "provider" includes a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge[.]"

Title II created a list of prohibited AI, which are "differentiating between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk." Prohibited AI practices include those that "place[] on the market, put[] into service, or use" an AI system that "deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour" and/or "exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability" in way that is meant to "materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm[.]"

Other prohibited practices include "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement" except in certain limited instances and "the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score." Title II also emphasizes that AI should not be used for "detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected" and "that is unjustified or disproportionate to their social behaviour or its gravity[.]"

Title III focuses on "two main categories of high-risk AI systems: AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment; other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III." According to a May 18, 2021 commentary by Center for Strategic and International Studies, a Washington, D.C.-based think tank, AI systems under eight specific sectors automatically qualify as high-risk, including: "1. Biometric identification and categorization of natural persons; 2. Management and operation of critical infrastructure; 3. Education and vocational training; 4. Employment, workers management, and access to self-employment; 5. Access to and enjoyment of essential private services and public services and benefits; 6. Law enforcement; 7. Migration, asylum, and border control management; and 8.

Administration of justice and democratic processes."

Title III also sets out "the legal requirements for high-risk AI systems in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security." For example, Title III requires that "[a] risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems."

The risk management system must follow several steps, including: "(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system; (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61; (d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs."

Title III also lays out several additional obligations of providers of high-risk AI, including that they must "draw-up the technical documentation of the high-risk AI system" and "ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service," among several other requirements.

Titles IV through XII set out several additional requirements and provisions, including transparency obligations for AI systems, implementation of the AIA, and codes of conduct, among other elements. The AIA provided that EU national supervisory authorities take the lead in conducting "market surveillance" of AI products and services, though enforcement could be handled by other EU bodies as well. The full proposal is available online at: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

In a May 6, 2021 commentary, several Arthur Cox LLP attorneys contended that the AIA, which was "heralded as the new 'GDPR for AI'" marked a "welcome legal and ethical framework" in "introducing a risk based approach for producers and users of AI Systems and applying extra-territorial effect."

In an April 28, 2021 commentary, Brookings Institution Senior Fellow Mark MacCarthy and Europe Center of the Atlantic Council Senior Fellow Kenneth Propp also noted the importance of addressing privacy and security related to AI, contending that the AIA "is a direct challenge to Silicon Valley's common view that law should leave emerging technology alone." However, MacCarthy and Propp pointed out several "Surprising Omissions and Gaps" in the European Commission's proposal, including that "the text of the regulation is surprisingly thin on the need for conducting and publishing disparate impact assessments" regarding "concerns about the risks of algorithmic bias." They continued, "The regulation does not treat the algorithms used in social media, search, online retailing, app stores, mobile apps or mobile operating systems as high risk. It is possible that some algorithms used in ad tracking or recommendation engines might be prohibited as manipulative or exploitative practices. But as noted above, this would take an assessment by a regulator to determine."

MacCarthy and Propp also noted that "[t]he regulation is light on information that must be disclosed to the people who are affected by AI systems. The regulation requires that people be informed when they 'interact with' an AI system or when their emotions or gender, race, ethnicity or sexual orientation are 'recognized' by an AI system. They must be told when 'deepfake' systems artificially create or manipulate material. But not in other cases."

MacCarthy and Propp therefore asserted that "Big Tech emerges virtually unscathed under the new AI legislation despite being the object of widespread and growing concern over the use of AI-driven algorithms and the focus of most of the cutting-edge applied AI research." They also contended that the "EU regulation contrasts with the piecemeal approach to AI taken in the United States. The Trump administration delegated AI responsibility to specific regulatory agencies, with general instructions not to overregulate — an extension of the Obama administration's treatment of AI regulation. The Biden administration is likely to maintain this decentralized approach, with perhaps a greater emphasis on the need to regulate to avoid potential AI risks." However, MacCarthy and Propp suggested that "there are [still] opportunities for trans-Atlantic cooperation on AI," including because the European Commission, as part of a larger plan of cooperation with President Joe Biden's administration, is focusing on AI work and agreement.

In a May 18, 2021 commentary, Center for Strategic & International Studies (CSIS) Scholl Chair in International Business Senior Adviser Meredith Broadbent and intern Sean Arrieta-Kenna similarly wrote that the "proposal by the European Commission for a regulatory framework to monitor AI is a watershed in tech regulation and marks a good time for the United States and Europe to engage in a dialogue on their respective approaches to its regulation."

They continued, "AI technology is a fundamental battleground in the geopolitical competition with China to 'win the twenty-first century.' The United States and Europe have a shared interest in holding the line against China, which seeks to export its intrusive model of data governance and AI regulation — a model anchored in state control of all information and communication, draconian surveillance, data localization, and other protectionist and autocratic practices. To succeed, Europe and the United States should agree on a basic framework of topline, democratic, regulatory principles for AI that can be promoted with trading partners in the Asia-Pacific, where China is proselytizing its model as an element of the Belt and Road Initiative."

— Scott Memmel
Postdoctoral Associate
Silha *Bulletin* Co-editor

First Circuit Rejects First and Fourth Amendment Challenges to Border Searches and Seizures of Travelers' Electronic Devices

On Feb. 9, 2021, the U.S. Court of Appeals for the First Circuit held that the First and Fourth Amendments do not require that U.S. Customs and Border Protection (CBP) agents have probable cause to conduct searches on electronic devices, including "advanced searches," nor reasonable suspicion to conduct a "basic" search. *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021). Following the ruling, several observers expressed concern over the privacy rights of travelers, including journalists, lawyers, and others. On April 23, 2021, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the ACLU of Massachusetts filed a petition for a writ of *certiorari* to the U.S. Supreme Court. In a response brief, the United States called for the petition to be held pending the disposition in *United States v. Cano*, a 2019 ruling in which the Ninth Circuit held that forensic searches require reasonable suspicion, but that such searches, along with manual searches, must be directed at finding contraband on electronic devices.

SEARCHES AND SEIZURES

In 1977, the Supreme Court affirmed in *United States v. Ramsey* the constitutionality of suspicionless, warrantless border searches so long as they are "routine." 431 U.S. 606, 616 (1977). According to the EFF, the Supreme Court, in *Ramsey* and other cases, articulated the border search exception to the Fourth Amendment's warrant requirement, which generally "permit[s] government agents to search travelers' luggage, vehicles or persons without a warrant and almost always without any individualized suspicion of wrongdoing."

In 2018, the U.S. Department of Homeland Security (DHS) and CBP released Directive No. 3340-049A, titled "Border Searches of Electronic Devices," in order to "provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information" contained in travelers' electronic devices, including mobile phones, computers, and others. Among other provisions, the policy differentiates a "basic search" from an "advanced search." "Advanced" searches of electronic devices, also referred to as "forensic searches" or "extended border searches," are conducted at a remote facility in which sophisticated software is used to search the device(s), before they are, eventually, returned to the owners. This is in contrast to "basic" or "manual" searches that occur immediately at the border crossing without additional software and without viewing deleted or encrypted files. The policy requires that there be "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern" in order to conduct advanced searches. The policy includes some exceptions, including when the device contains "possibly sensitive information, such as medical records and work-related information carried by journalists."

The case before the First Circuit arose on Sept. 13, 2017 when the ACLU, EFF, and the ACLU of Massachusetts filed a complaint in the U.S. District Court for the District of Massachusetts on behalf of 11 travelers. The plaintiffs consisted of 10 U.S. citizens and one lawful permanent resident, and included "a military veteran, journalists, students, an artist, a NASA engineer, and a business owner." The journalists included Jeremy Dupin, "[a]n award-winning journalist and filmmaker who covers news coming out of South America and the Caribbean," and Isma'il Kushkush, a freelance journalist in Virginia. Additionally, the plaintiffs included Zainab Merchant, a Florida-based journalist and graduate student in international security at Harvard University, and Akram Shibly, a New York-based independent filmmaker who runs his own production company.

The complaint alleged that federal CBP agents "seized and searched Plaintiffs' electronic devices at U.S. ports of entry without probable cause to believe that the devices contained contraband or evidence of a violation of immigration or customs laws." The ACLU and EFF also alleged that officers had "confiscated and kept the devices of several plaintiffs for weeks or months," including one individual's device which had been held since January 2017. The complaint argued that CBP and ICE had therefore violated the travelers' Fourth Amendment rights. The complaint further argued that the searches and seizures had violated the 11 travelers' First Amendment rights, including because the searches and seizures of their "journalistic work product[s]" impinged on their "constitutionally protected . . . right to engage in newsgathering." The full complaint is available online at: https://www.eff.org/document/alasaad-v-duke-complaint.

On May 9, 2018, District Judge Denise J. Casper denied a motion by the DHS, CBP, and ICE to dismiss the case. She first ruled that the plaintiffs had standing to bring the case, finding that they had "plausibly alleged that they face a substantial risk of future harm from Defendants' ongoing enforcement of their border electronics search policies." *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL 2170323 (D. Mass. May 9, 2018).

Second, Casper held that the plaintiffs had stated a plausible Fourth Amendment claim regarding manual searches of electronic devices at U.S. borders. She found that "[i]n the absence of controlling precedent to the contrary, this Court cannot rule that this Fourth Amendment principle [of heightened privacy concerns for electronic devices] would not extend in some capacity to the border." She further concluded that searches of electronic devices at U.S. borders may require a heightened standard above "reasonable suspicion."

Casper also denied the defendants' motion to dismiss the plaintiffs' claim that CBP and ICE "violate[d] the Fourth Amendment by confiscating travelers' electronic devices, for the purpose of effectuating ['forensic'] searches of those devices after travelers leave the border, absent probable cause [as they are] unreasonable at their inception, and in scope and duration." She ruled that because the plaintiffs had alleged a plausible Fourth Amendment claim

regarding "manual" searches, they had also done so for "forensic searches" when electronic devices are confiscated by CBP or ICE. However, she noted that confiscations raise an additional Fourth Amendment concern in that they must "be reasonable not only at their inception[,] but also for their duration."

Finally, Casper addressed the plaintiffs' First Amendment claims, finding that the defendants "[did] not argue that warrantless searches would not be a significant or substantial burden on travelers' First Amendment rights, nor do they explain their assertion that a heightened standard is not 'required by the First Amendment.'" Thus, Casper ruled that the plaintiffs had "plausibly alleged that the government's digital device search policies substantially burden travelers' First Amendment rights." For more information on the background of the case, Casper's ruling, and other relevant federal circuit court rulings, see "U.S. Customs and Border Protection Actions Continue to Raise First and Fourth Amendment Questions" in the Summer 2018 issue of the Silha *Bulletin*.)

On Feb. 9, 2021, the First Circuit reversed several portions of Casper's ruling. Judge Sandra Lynch wrote for the unanimous court and first addressed the plaintiffs' Fourth Amendment claims. Lynch discussed the Supreme Court's ruling in *Riley v. California*, in which the Court held that law enforcement officers are required to obtain a warrant before searching an arrested individual's cell phone data. 573 U.S. 373 (2014). Lynch concluded that *Riley* "does not command a warrant requirement for border searches of electronic devices nor does the logic behind *Riley* compel us to impose one." She further held that "given the volume of travelers passing through our nation's borders, warrantless electronic device searches are essential to the border search exception's purpose of ensuring that the executive branch can adequately protect the border." Thus, Lynch concluded that "neither a warrant nor probable cause is required for a border search of electronic devices," including advanced searches.

Furthermore, Lynch ruled that basic searches at U.S. borders can be performed without reasonable suspicion because they constitute "routine" searches that "do not involve an intrusive search of a person," citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 539–40 (1985). She further reasoned that basic searches do not reveal deleted or encrypted files on travelers' electronic devices, at least according to CBP policies. Lynch added that the privacy concerns associated with electronic devices "are nevertheless tempered by the fact that the searches are taking place at the border."

Second, Lynch dismissed several additional arguments by the plaintiffs, including that "border searches of electronic devices 'must be limited to searches for contraband.'" She reasoned that the border search exception's purpose goes beyond finding contraband and that Congress would be better suited "to identify the harms that threaten us at the border."

Third, Lynch turned to the plaintiffs' First Amendment claim, namely that "because electronic devices may contain sensitive personal data, the threat of warrantless or suspicionless border searches will impermissibly chill speech" and implicate newsgathering. Although Lynch acknowledged that the First Amendment "provides protections — independent of the Fourth Amendment — against the compelled disclosure of expressive information," she held that the Supreme Court and lower courts had not "specified the appropriate standard to assess alleged government intrusions on First Amendment rights at the border." Nevertheless, Lynch concluded that "[u]nder any standard[,] plaintiffs have not shown that the content-neutral border search Policies facially violate the First Amendment."

Finally, Lynch concluded that the district court had "adequately justified its conclusions that expungement was not warranted" regarding "any data obtained in violation of the Constitution."

In a Feb. 19, 2021 commentary, Vinson & Elkins LLP attorney Jennifer Freel and associates Meghan Natenson and Michael Riggins wrote that the First Circuit's ruling "presents various data-security challenges for companies and organizations of all sizes." The commentary continued, "The *Alasaad* decision highlights the data privacy challenges for companies and international travelers. In an increasingly interconnected global economy, employees often travel with confidential, privileged, personal, or proprietary data on their electronic devices. Warrantless searches and copying of data from travelers' electronic devices could lead to the exposure of sensitive data to outside parties. This is particularly troublesome for a wide range of businesses, such as law firms and healthcare companies, that are obligated to protect certain data."

In a February 25 article, Cleary Gottlieb partner David E. Brodsky and several additional attorneys provided recommendations for businesspeople, executives, lawyers, and others crossing U.S. borders following the First Circuit's ruling. Among the recommendations were "[u]sing password protection for email and messaging services, as well as any confidential, privileged, or sensitive documents" and "[s]ecuring files with encryption." The article added, "The simplest and lowest risk option is not to carry any confidential information across the border, although that might not always be a practical option. Clients and lawyers alike should consider using a temporary smartphone or laptop computer (without sensitive information) while traveling, removing confidential information from their devices, disabling automatic syncing processes, logging off and disabling auto-password features, and turning off syncing of cloud services, among other measures."

In a Feb. 16, 2021 piece for *Techdirt*, staff writer Tim Cushing noted that the First Circuit's ruling "deepens the split between circuits and their interpretation of the Constitution's effectiveness within 100 miles of the border," including rulings by the Fourth, Ninth, and Eleventh Circuits. Whereas the Fourth and Ninth Circuit ruled that border agents need to demonstrate at least "reasonable suspicion" in order to forensically search and/or seize travelers' devices, the Eleventh Circuit held that border agents do not need reasonable suspicion, probable cause, or a search warrant when conducting a forensic search, instead favoring law enforcement interests.

Following the First Circuit's ruling, Ghassan Alasaad, Nadia Alasaad, and Jérémie Dupin were no longer named as plaintiffs, resulting in the case name changing to *Merchant v. Mayorkas*.

On April 23, 2021, the ACLU, EFF, and ACLU of Massachusetts filed a petition for a writ of *certiorari* to the Supreme Court, posing the question,

Devices, *continued on page 40*

Devices, *continued from page 39*

"Does the Fourth Amendment require that searches of electronic devices at the U.S. border be conducted pursuant to a warrant based on probable cause, or at least pursuant to an officer's determination of reasonable suspicion that the device contains digital contraband?"

The petition contended that a circuit court split exists regarding "how the border search exception applies to searches of electronic devices." It continued, "The First, Fourth, Ninth, and Eleventh Circuits have each decided some aspect of this question — and none of them agree. The courts of appeals are split on (1) whether and what level of individualized suspicion is required for border searches of electronic devices, and (2) whether warrantless border searches of electronic devices must be limited to searches for digital contraband, or otherwise limited in scope."

The petition argued that "[r]esolution of the question presented is a matter of great importance for the millions of travelers whose privacy rights are at stake every time they cross the border, as well as for the border officers who conduct device searches." The petition continued, "Device searches at the border are on the rise. And advancing technology increasingly enables individuals to store more personal information on their devices, while empowering government agents to conduct increasingly intrusive searches of those devices. The question presented here is of immediate significance to everyone who crosses our border with a cell phone or other electronic device — and these days, that is virtually every international traveler."

Additionally, the petition contended that the First Circuit erred in holding 1) that the Fourth Amendment does not require a warrant nor probable cause to execute a border search of electronic devices and 2) that reasonable suspicion is not required for any/all border searches. The petition reasoned that searches of electronic devices raise significant privacy interests and that searches of electronic devices are unlikely to accomplish the purposes behind the border search exception, including finding contraband.

The petition added, "If this Court rejects a warrant requirement, it should at a minimum require an officer determination of reasonable suspicion for all searches of electronic devices at the border, and should limit their permissible scope to finding digital contraband. While not as protective as a warrant requirement, such a rule would partially account for the significant privacy intrusions that searches of electronic devices present, and the substantially reduced likelihood that electronic devices themselves contain contraband." The full petition is available online at: https://www.aclu.org/legal-document/supreme-court-petition.

On May 25, 2021, the United States (government) filed a response brief, in which it contended that the First Circuit was correct in holding that "no warrant is required to search an electronic device that a traveler is seeking to carry across the U.S. border" and that "the Fourth Amendment does not impose an individualized-suspicion requirement on 'basic' searches of such devices during a border crossing."

The brief also argued that the First Circuit's ruling "accords with the decisions of every other court of appeals that has addressed them." Furthermore, the brief argued that the Supreme Court "has repeatedly and recently declined to review questions concerning the degree of suspicion that may be required for border searches of electronic devices." The brief therefore asserted that the Court "should follow the same course in this case." The full brief is available online at: https://www.supremecourt.gov/DocketPDF/20/20-1505/180108/20210525163008512_20-1505%20-%20Merchant%20Cert%20Response.pdf.

Finally, the brief called for the petition for a writ of *certiorari* to be held pending the disposition in *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019), in which the Ninth Circuit held that the border search exception only authorizes warrantless searches of cellphones when directed at digital contraband. That case arose in 2016 when "Defendant-Appellant Miguel Cano was arrested for carrying cocaine as he attempted to cross into the United States from Mexico at the San Ysidro Port of Entry." A CBP agent summarily seized Cano's cellphone and searched it, first manually and later using software capable of accessing all text messages, call logs, media, and more. Other agents also conducted two additional manual searches of the cellphone.

The Ninth Circuit ultimately held that manual searches of electronic devices "may be conducted by border officials without reasonable suspicion." Conversely, the court held that advanced searches require reasonable suspicion that the electronic device contains contraband because they amount to an "intrusive search," citing its 2013 ruling in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc). The court concluded that cell phones can contain contraband, such as child pornography, therefore falling under the border search exception. However, the court held that a manual search of the "recording of the phone numbers and text messages" had "no connection to ensuring that the phone lack[ed] digital contraband." The court further held that the advanced search of "Cano's cell phone exceeded the scope of a valid border search" because the border agents could not have had reasonable suspicion that the cellphone contained contraband." The court therefore concluded that "most of the evidence obtained from the searches of Cano's cell phone should have been suppressed."

On Jan. 29, 2021, the government filed a petition for a writ of *certiorari*, contending that the Ninth Circuit erred in ruling that the searches of Cano's cellphone violated the First Amendment. The petition continued, "The Ninth Circuit's erroneous conclusion that 'the border search exception authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband,' and does not even permit 'a warrantless search for evidence of past or future border-related crimes,' warrants this Court's review." The full petition is available online at: https://www.supremecourt.gov/DocketPDF/20/20-1043/167671/20210129152435803_cert%20petition%20%20%20USA%20v.%20Cano.pdf.

On May 12, 2021, Cano filed a brief in opposition, asserting that the "Ninth Circuit's reasoning is sound" in holding that "the particular searches at issue here nevertheless violated the Fourth Amendment because they exceeded the permissible scope of a border search." The brief further argued that the Supreme Court's intervention would be premature" for a number of reasons, including that "technological developments may soon transform the relevant terrain, and legislative action may obviate any need for this Court to

Devices, *continued on page 41*

Federal Judge Allows Privacy Lawsuit Against Thomson Reuters to Continue

DATA PRIVACY

On Aug. 16, 2021, U.S. District Court Judge Edward Chen of the Northern District of California allowed a class action privacy lawsuit against Thomson Reuters Corporation (Thomson Reuters) to continue. *Brooks v. Thomson Reuters Corp.*, No. 21-cv-01418-EMC, 2021 WL 3621837 (N.D. Cal. 2021). Chen weighed the significant privacy concerns arising from Thomson Reuters's CLEAR database, which contained individuals' identities and related information, with the company's arguments that it provides a valuable resource containing information of public concern. In addressing several of the defendant's arguments and legal claims regarding its database, Chen concluded that Thomson Reuters, despite being a media organization, "is not a journalist performing a 'public benefit[.]'"

The case arose from a class action complaint by plaintiffs Cat Brooks and Rasheed Shabazz targeting Thomson Reuters's practice of "aggregat[ing] both public and non-public information about millions of people" to create "detailed cradle-to-grave dossiers on each person, including names, photographs, criminal history, relatives, associates, financial information, and employment information." Included in the information not available to the public obtained by Thomson Reuters is "information from third-party data brokers and law enforcement agencies . . ., including live cell phone records, location data from billions of license plate detections, real-time booking information from thousands of facilities, and millions of historical arrest records and intake photos."

Thomson Reuters sells the aggregated information "to its customers — without the knowledge or consent of the persons to whom the information concerns — through an online platform it calls CLEAR." Brooks and Shabazz, both Black civil rights activists, "are Californians whose identities Thomson Reuters sells to its customers through CLEAR. Neither consented to the company selling their personal information — and neither wants the company to do so." Shabazz further alleged that the "CLEAR profile on him incorrectly indicates that he is divorced and has failed to pay child support when he was never legally married and at the time had no children."

Brooks and Shabazz filed their complaint in December 2020 "on behalf of all California residents 'whose name, photographs, personal identifying information, or other personal data is or was included in the CLEAR database[.]" They cited four causes of action: "(1) violations of the California common law right of publicity; (2) a claim for monetary relief for violations of California's Unfair Competition Law (UCL), Cal Bus. & Prof. Code § 17200; (3) unjust enrichment; and (4) a claim for injunctive relief for violations of the UCL." In February 2021, Thomson Reuters removed the action to federal court and filed a motion to dismiss.

Judge Chen first addressed the right of publicity claim, finding first that "California has long recognized a right of publicity (also known as a "commercial misappropriation" claim), which protects a person's name and likeness against appropriation by others for their commercial advantage." The right is found under common law and statutory law under section 3344 of the California Civil Code. According to Chen, to state a common law claim, a plaintiff needs to prove: "(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury." To state a statutory claim, "a plaintiff must plead all the elements of the common law claim and must also prove (5) 'a knowing use by the defendant,' and (6) 'a direct connection between the alleged use and the commercial purpose.'"

Thomson Reuters challenged only the "use" and "appropriation" elements of the right of publicity claims, as well as asserting that they "are barred by the First Amendment and that their section 3344 claim is barred by the newsworthy exception." Regarding whether Thomson Reuters used the plaintiffs' identities, Chen held that the CLEAR platform is not third-party content, but is instead "created by Thomson Reuters, albeit from third-party sources." This was in contrast to other cases where companies, such as Google or Facebook, "simply provid[ed] the websites or platforms where *others* posted that information" (emphasis in original). Thus, Chen concluded "that Plaintiffs' have properly pled that Defendant has 'used' their names and likenesses for

Privacy Lawsuit, *continued on page 42*

Devices, *continued from page 40*

address the issue at all." The full brief is available online at: https://www.supremecourt.gov/DocketPDF/20/20-1043/179038/20210512171223452_20-1043%20Cano%20Brief%20in%20Opposition%20final.pdf.

Following the First Circuit's ruling in *Alasaad*, the government filed a reply brief to the petition for *certiorari* in *Cano* on June 1, 2021 emphasizing that "[t]he need for this Court's intervention [in *Cano*] has become even more apparent since the petition for a writ of certiorari was filed, as [the First Circuit] recently rejected the Ninth Circuit's unprecedented and unjustified restriction on the scope of the United States' sovereign authority to protect its borders." The brief continued, "This Court should grant review and resolve the circuit conflict by rejecting the Ninth Circuit's approach. The 'longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment.'" The full brief is available online at: https://www.justice.gov/brief/file/1401271/download.

On June 28, 2021, the Supreme Court denied *certiorari* in both *Merchant* and *Cano*. *Merchant v. Mayorkas*, 988 F.3d 8 (1st Cir. filed May 25, 2021), *cert. denied*, No. 20-1505 (2021); *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019), *cert. denied*, No. 20-1043 (2021).

— Scott Memmel
Postdoctoral Associate
Silha *Bulletin* Co-editor

Privacy Lawsuit, *continued from page 41*

purposes of stating a right of publicity claim."

Chen also dismissed Thomson Reuters's argument that "it does not appropriate Plaintiffs' name, likeness, or personal information for a commercial advantage because it is not using that information 'for purposes of publicity,' i.e., 'for promotional purposes or to imply an endorsement.'" He held that "the Ninth Circuit and the California Court of Appeal have held that commercial appropriation in a right of publicity case does not require the suggestion of an endorsement."

However, Chen found Thomson Reuters's second argument — that "this is not a right of publicity case because Thomson Reuters is not using Plaintiffs' name or likeness 'for promotional purposes,' i.e., to advertise or promote a separate product or service" — "more persuasive." He reasoned that "the injury Plaintiffs suffered here — although deeply concerning and perhaps a violation of their privacy — is not a violation of their right of publicity because their name or likeness is not being 'appropriated' and used to advertise a separate product or service." Chen therefore held that the plaintiffs "failed to state a claim for a violation of the right of publicity because Thomson Reuters did not appropriate their name or likeness."

Second, Chen turned to the claims under the UCL, which "prohibits, and provides civil remedies for, unfair competition, which it defines as 'any unlawful, unfair or fraudulent business act or practice.'" The plaintiffs contended that "Thomson Reuters engaged in unlawful and unfair (but not fraudulent) business practices." Chen held that the plaintiffs "failed to plausibly plead their claim under the unlawful prong of the UCL" because he had dismissed their claim for a violation of the right of publicity.

However, Chen disagreed with Thomson Reuters that the California Consumer Privacy Act (CCPA), Cal Civ. Code §§ 1798.100–1798.199.95 (2020), permitted their collection of personal information. The CCPA requires that consumers be able, "at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out." Thomson Reuters claimed that it allowed such an opt-out. However, the complaint contended that the company only "places a 'tiny link' at the bottom of its CLEAR homepage and 'provides no notice to consumers that the link exists. Nor does the company enable consumers who happen to find out about the link to easily make use of it.'"

Chen found that there was "a question of fact as to whether CLEAR's opt-out mechanism complies with the CCPA." He also noted that Thomson Reuters did "not cite a single case where the court dismissed a plaintiff's claim that the dissemination of their personal information is unfair under the UCL simply because the defendant provided an adequate opt-out mechanism under the CCPA."

Chen therefore concluded that "compliance with the CCPA is not a defense to Plaintiffs' claims that the sale of their personal information is an unfair business practice under the UCL. At the very least, there is a serious question of material fact as to whether Thomson Reuters's opt-out mechanism even complies with the CCPA."

Additionally, Chen held that Thomson Reuters's actions were "unfair" under two different tests arising from such claims. The "balancing test" requires a court to weigh "the harm to the consumer against the utility of the defendant's practice." Chen emphasized that "the harm to Plaintiffs is tremendous: an all-encompassing invasion of Plaintiffs' privacy, whereby virtually everything about them — including their contact information, partially redacted social security number, criminal history, family history, and even whether they got an abortion, to name just a few — is transmitted to strangers without their knowledge, let alone their consent."

Chen questioned Thomson Reuters's claim that "its dossiers are mere compilations of publicly available information." He reasoned that the company "boasts on its website that the CLEAR platform allows its users to uncover information about Plaintiffs that is 'not ascertainable via public records or traditional search engine queries,' 'facts hidden online,' and "key proprietary and public records.'"

Chen also cited several U.S. Supreme Court cases, including *U.S. Department of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749 (1989), in which the Court "noted that there was a 'distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole.'" Chen added, "Here, too, compiling bits of Plaintiffs' personal information scattered throughout the internet (and allegedly in non-public sources) into a dossier is a significant invasion of privacy because it is much easier to access that information in one place. Otherwise why would CLEAR subscribers pay to access the dossiers? That some of Plaintiffs' personal information on the CLEAR dossiers comes from publicly available sources does not diminish the significant harm Plaintiffs suffer from the sale of that compiled information to whomever is willing to pay for it."

Chen also addressed Thomson Reuters's invocation of a series of Supreme Court cases allowing for the publication of lawfully obtained, truthful information, including *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 494–95 (1975), *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979), and *Bartnicki v. Vopper*, 532 U.S. 514 (2001), among other cases. He held that "Thomson Reuters is not a journalist performing a 'public benefit' by making Plaintiffs' personal information available to the public. Rather, the company's dissemination of this information only benefits the private parties who purchase the CLEAR dossiers." Chen added, "All the other cases cited by Thomson Reuters to suggest that there is no privacy right in speech derived from public records are similarly inapposite because they involve *journalists* disclosing publicly available information *to the general public*" (emphasis in original).

Chen therefore ruled that "Thomson Reuters's sale of Plaintiffs' most private and personal information states a claim under the unfair prong of the UCL." He reached the same conclusion under the "tethering test," which requires that "the unfairness . . . 'be tethered to some legislatively declared policy.'" Chen also held that "Plaintiffs can seek equitable relief in the form of an injunction for their UCL claims."

Third, Chen "reject[ed] Thomson Reuters's argument that unjust enrichment is not a standalone cause of action and thus cannot be asserted, because that argument is based on outdated law."

Fourth, Chen wrote that he was "not persuaded by Thomson Reuters's contention" that Section 230 of the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230, immunizes the company "from civil liability stemming from the unauthorized sale of Plaintiffs'

personal information." As explained by Chen, Section 230 "immunizes providers of an 'interactive computer service' (i.e. Facebook, Twitter, LinkedIn, etc.) from liability for content independently created or developed by third-party 'information content providers' (i.e., users), unless the interactive computer service created or developed part of that content."

Chen cited the U.S. Court of Appeals for the Ninth Circuit's ruling in *HomeAway.com, Inc. v. City of Santa Monica* that Section 230 "only immunizes '(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.'" 918 F.3d 676, 681 (9th Cir. 2019) (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009)) Chen held that Thomson Reuters failed the second prong, reasoning that the plaintiffs were "not seeking to hold Thomson Reuters liable 'as the publisher or speaker' because they are not asking it to monitor third-party content; they are asking to moderate its *own* content" (emphasis in original).

Regarding the third prong, Chen concluded that "the 'information' at issue here — the dossiers with Plaintiffs' personal information — is not 'provided by another information content provider.'" He continued, "Here, there is no user-generated content — Thomson Reuters generates all the dossiers with Plaintiffs' personal information that is posted on the CLEAR platform.. . . In other words, Thomson Reuters is the 'information content provider' of the CLEAR dossiers because it is 'responsible, in whole or in part, for the creation or development of' those dossiers. It is nothing like the paradigm of an interactive computer service that permits posting of content by third parties."

Finally, Chen dismissed Thomson Reuters's motion under Section 425.16 of the California Civil Code, California's Strategic Lawsuit Against Public Participation (anti-SLAPP) statute. He reasoned that the company failed to pass the first step of the statute, namely that "the defendant must show that the plaintiff's action arises from 'an act in furtherance of the person's right of petition or free speech.'"

Chen rejected Thomson Reuters's claim that the CLEAR platform constituted a public forum, holding that only websites accessible to the general public, meaning available to anyone who chooses to visit the website, constitute such a forum. Conversely, the CLEAR platform "requires payment." Chen further held that Thomson Reuters "fail[ed] to explain how the dossiers it posts on the CLEAR platform are 'in connection with an issue of public interest.'"

He cited a series of Supreme Court cases emphasizing the importance of protecting speech of public concern, which was not at issue in the present case because "[t]he public does not have a particular cognizable interest in the 'speech' at issue here — the dissemination of Plaintiffs' personal information — because that information is purely a matter of private concern, does not relate to any matter of 'political' or 'social' concern, and does they seek to communicate a political or social point of view." Chen added that "Thomson Reuters's attempt to characterize its unauthorized sale of Plaintiffs' personal information on the CLEAR platform as '[t]he dissemination of news and information about current and historical events' is unpersuasive."

Chen therefore allowed the case against Thomson Reuters to continue, granting in part and denying in part the company's motion to dismiss.

In a June 2021 hearing before Chen, Gibbs Law Group attorney Andre Mura, who represented the plaintiffs, said, "Information is being collected without consent and used to define and make clear the identity of the individuals and provide third parties who pay for this information secretly.. . . They are controlling the use of your identity without permission."

During the same hearing, Perkins Coie attorney Susan Fahringer, who represented Thomson Reuters, countered that the company could publish factual information. "There is a right to publicity that means you can't stop someone from disclosing factual information about you," Fahringer said. According to *Courthouse News Service* on Aug. 16, 2021, Fahringer contended "that if Thomson Reuters was using individual identities to endorse a product or create an advertisement, that would be unlawful. But providing access to a database with factual information about individuals is legal under U.S. law."

— Scott Memmel
Postdoctoral Associate
Silha *Bulletin* Co-editor

36th Annual Silha Lecture: "The First Amendment and Diversity: A Marketplace Failure?"

SILHA CENTER EVENTS

Billions of people use social media platforms and have access to a 5000-plus-channel streaming and broadcasting universe, yet citizens are less informed than ever before. They select their preferred sources, often based on ideology and politics, but rarely seek out media options that challenge their preconceptions. Coupled with the lack of diversity in 'media' ownership and management, it appears that the concept of a robust 'marketplace of ideas' in today's America has failed.

Can we change this? Diversity in the media by itself is not enough to elevate and reinvigorate the national conversation. But without welcoming disparate and even antagonistic voices, how can we hope to mitigate polarization and advance the core purposes of the First Amendment?

On Oct. 26, 2021, the Silha Center for the Study of Media Ethics and Law will present the 36th Annual Silha Lecture, "The First Amendment and Diversity: A Marketplace Failure?" Our speaker is S. Jenell Trigg, Esq., CIPP/US, Chair of Privacy, Data Protection and Cybersecurity Practice Group, and Director of Diversity, Equity & Inclusion at Lerman Senter PLLC, Washington, D.C.

S. Jenell Trigg's remarkable career in media and law, as well as her volunteer experience working with numerous nonprofit groups, give her unique insight into current issues of diversity and free speech. She began as a broadcast television sales and marketing executive whose advertising career spanned 16 years in the Chicago and Baltimore markets. Ms. Trigg then earned her law degree *magna cum laude* from The Catholic University of America, Columbus School of Law.

She worked at the Federal Communications Commission and as Assistant Chief Counsel for Telecommunications in the Office of Advocacy, U. S. Small Business Administration, before becoming the first African-American partner at Lerman Senter PLLC in Washington, D.C. She has been nationally recognized for her longstanding dedication and commitment to promoting minority, women, and small business ownership and employment in the media and communications industries, receiving lifetime achievement awards from the Rainbow PUSH Coalition and the Multicultural Media, Telecom, and Internet Council.

More information about Ms. Trigg is available at: https://www.lermansenter.com/attorneys/s-jenell-trigg/.

The 36th Annual Silha Lecture is sponsored by the Silha Center for the Study of Media Ethics and Law. It will be live-streamed on Tuesday, Oct. 26, 2021, beginning at 7:00 p.m. CDT. The lecture is free and open to the public, but advance registration is required. Please visit: https://z.umn.edu/2021SilhaLecture to register.

Silha Center activities, including the annual Silha Lecture, are made possible by a generous endowment from the late Otto and Helen Silha. For further information, please contact the Silha Center at 612-625-3421 or silha@umn.edu, or visit https://hsjmc.umn.edu/research-centers/centers/silha-center-study-media-ethics-and-law.

36th Annual Silha Lecture

The First Amendment & Diversity: A Marketplace Failure?

Featuring:

S. Jenell Trigg, Esq., CIPP/US

Lerman Senter PLLC, Washington, DC

This will be a Livestreamed Event

Tuesday, Oct. 26, 2021

7 p.m. CDT

Advance Registration Is Required

To register, visit:

https://z.umn.edu/2021SilhaLecture

S. Jenell Trigg, Esq., CIPP/US

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW

HUBBARD
SCHOOL OF JOURNALISM
& MASS COMMUNICATION

COLLEGE OF LIBERAL ARTS

SILHA CENTER

FOR THE STUDY OF MEDIA ETHICS & LAW

HUBBARD
SCHOOL OF JOURNALISM
& MASS COMMUNICATION

COLLEGE OF LIBERAL ARTS

SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW
Hubbard School of Journalism and Mass Communication
University of Minnesota
111 Murphy Hall
206 Church Street SE
Minneapolis, MN 55455
Silha@umn.edu
www.silha.umn.edu
(612) 625-3421