THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | SUMMER 2020

Journalists Covering Fallout from George Floyd Death Take Legal Action; Misinformation Underscores Lessons from 2020 Silha Spring Ethics Forum

Journalists and news organizations covering the fallout from the May 2020 death of George Floyd in Minneapolis filed numerous lawsuits and took other legal action seeking to vindicate their newsgathering rights and obtain information. Meanwhile, false information circulated about the events surrounding Floyd's death provide a case study about the pernicious nature of misinformation and how it spreads, particularly online, which was the subject of the 2020 Silha Spring Ethics Forum.

On May 25, 2020, Floyd, a 46-year-old African American man, was arrested in south Minneapolis after he allegedly used a counterfeit $20 bill. Surveillance footage released on May 27 showed Floyd being dragged out of his vehicle. After Floyd was pulled out of his vehicle at the intersection of East 38th Street and Chicago Avenue, Minneapolis Police Department (MPD) Officer J.A. Kueng held Floyd's back and Officer Thomas Lane held his legs. Officer Tou Thoa, who arrived at the scene with MPD Officer Derek Chauvin, blocked witnesses from interfering. Chauvin "dug his knee into the man's neck," despite Floyd pleading that he was in pain and could not breathe, as reported by the Associated Press (AP) on May 28. Chauvin continued to press his knee down on Floyd's neck for nearly nine minutes, causing Floyd to fall silent and unresponsive. Officers eventually called an ambulance, which transported Floyd to the Hennepin County Medical Center where Floyd was pronounced dead at approximately 9:25 p.m.

In a May 29 statement, Hennepin County Attorney Mike Freeman announced criminal charges against Chauvin, including for third-degree murder and manslaughter. Freeman noted that Chauvin "is the first white officer in Minnesota to be criminally prosecuted in the death of a black civilian." The Minneapolis *Star Tribune* explained on May 29 that Hennepin County charged former MPD Officer Mohamed Noor in the 2017 shooting death of Justine Damond. Noor was later convicted in 2019 of third-degree murder and second-degree manslaughter. (For more information on the shooting and trial of Noor, as well as the legal battles around press and public access, see "Recent Minnesota Legal Disputes Involve Information Access and Defamation Liability" on page 32 of this issue of the Silha *Bulletin*; see also "Twin Cities Media Seek Juror Names in Noor Trial; Minneapolis Advisory Committee Allegedly Violates Open Meeting Law" in the Winter/Spring 2020 issue; "Judge Allows Media and Public to Make Copies of Evidence from Trial of Former Minneapolis Police Officer, Restricts Live Streaming of Noor Sentencing Hearing" in the Summer 2019 issue, and "Media Coalition Wins Legal Victory to Access Body Camera Video in Trial of Former Minneapolis Police Officer" in the Winter/Spring 2019 issue.)

On May 29, Minnesota Gov. Tim Walz's office announced that the governor had signed Executive Order 20-65, which "implement[ed] a temporary nighttime curfew that will provide safety for Minnesota residents from individuals who have engaged in unlawful and dangerous activity in recent days and threatened the security of lawful demonstrators and first responders." However, the news media were among those exempt from the curfew order.

On June 1, 2020, the Hennepin County Medical Examiner (ME) released its updated findings and ruled that Floyd's death was a homicide, finding that he died of "cardiopulmonary arrest complicating law enforcement subdual, restraint, and neck compression." The ME's report claimed that the "injury occurred" because the "[d]ecedent experienced a cardiopulmonary arrest while being restrained by law enforcement officer(s)," though it also noted that Floyd had other "significant conditions, including "[a]rteriosclerotic and hypertensive heart disease; fentanyl intoxication; [and] recent methamphetamine use." Also on June 1, an independent autopsy commissioned by Floyd's family called Floyd's death a homicide and determined that he died of "asphyxiation from sustained pressure," meaning a lack of blood flow to the brain due to compression on his back and neck caused by officers kneeling on him.

On May 31, Walz announced that Minnesota Attorney General Keith Ellison would take over the investigation and prosecution of the MPD officers involved in Floyd's death. On June 3, Ellison announced that he had upgraded the charges against Chauvin to second-degree murder and had also charged Kueng, Lane, and Thoa with aiding and abetting.

Meanwhile, in the days following Floyd's death, peaceful and violent protests erupted in Minneapolis, including at the scene of the incident and near the MPD's Third Precinct police station. Local and national journalists provided live coverage

Protests, *continued on page 3*

Inside This Issue

Summer 2020: Volume 25, No. 3

Silha Center Staff

Protests, *continued from page 1*

of the protests each night that they took place. Amidst the protests, numerous journalists in Minneapolis and around the country faced arrests, attacks, and threats by law enforcement. For example, on May 29, 2020, CNN correspondent Omar Jimenez, his producer Bill Kirkos, and photojournalist Leonel Mendez were arrested by Minnesota State Patrol officers while reporting live from the protests in south Minneapolis. The arrests prompted significant criticism from observers, including the Silha Center for the Study of Ethics and Media Law. On May 30, Tom Aviles, a veteran photographer at WCCO, the Twin Cities' CBS affiliate, was arrested while covering the ongoing protests over the death of Floyd.

For a full list of the incidents between the press and police around the country, see the U.S. Press Freedom Tracker, a database of press freedom violations in the United States and around the world managed by the Freedom of the Press Foundation, available online at: https://pressfreedomtracker.us/. (For more information on the protests around the death of George Floyd, as well as the incidents between the press and police, see "Special Report: Journalists Face Arrests, Attacks, and Threats by Police Amidst Protests Over the Death of George Floyd" in the Winter/Spring 2020 issue of the Silha *Bulletin*.)

COVER STORY

Incidents Between Press and Police Amidst Protests Over George Floyd's Death Lead to Multiple Lawsuits, Reporter Sues Newspaper for Barring Her From Covering Protests

The incidents between journalists and members of law enforcement in the Twin Cities and around the United States amidst the protests over the death of George Floyd prompted several lawsuits, including two by members of the news media at the protests in Minneapolis, who argued that arrests and/or attacks by police violated their First and Fourth Amendment rights, among other claims. The incidents also prompted at least one lawsuit regarding police transparency. Meanwhile, a Black reporter for the *Pittsburgh Post-Gazette* sued the newspaper after she was barred from covering the protests in Pittsburgh, Penn.

On June 2, 2020, the American Civil Liberties Union (ACLU) of Minnesota filed a class action lawsuit in the U.S. District Court for the District of Minnesota on behalf of freelance journalist Jared Goyette and "other similarly situated individuals," namely several additional journalists who faced arrests, rubber bullets, pepper bullets, tear gas, physical attacks, and more by law enforcement.

The complaint first contended that the defendants — The City of Minneapolis, Minneapolis Chief of Police Medaria Arradondo, Minneapolis Police Lieutenant Robert Kroll, Minnesota Department of Public Safety Commissioner John Harrington, and Minnesota State Patrol Colonel Matthew Langer, in their official capacities — each had 1) "a custom or policy of deploying chemical agents and injurious, less-lethal ballistics against members of the news media," 2) "a custom or policy of failing to provide warnings and/or dispersal orders before using chemical agents and injurious, less-lethal ballistics against protesters and members of the news media," and 3) "a custom or policy of arresting or detaining news media lawfully reporting on protests and other First Amendment expressive activity."

The complaint provided previous examples, including the arrest of *Democracy Now!* journalist Amy Goodman during the 2008 Republican National Convention (RNC) in St. Paul, Minn. and the arrests of *City Pages* journalist Susan Du and *Minnesota Daily* reporter David Clarey during the protests following the fatal shooting of Philando Castile by Jeronimo Yanez, a Hispanic-American police officer in St. Anthony, Minnesota, in 2017. (For more information on the arrest of Goodman and other reporters at the 2008 Republican National Convention, see "Dozens of Journalists Arrested at Republican National Convention in St. Paul" in the Fall 2008 issue of the Silha *Bulletin*. Goodman also faced arrest after covering oil pipeline protests in North Dakota in 2016. For more information on the warrant issued against Goodman, see *North Dakota Officials Issue Warrant for* Democracy Now! *Reporter During Pipeline Protests* in "Independent Journalists Face Threats to Newsgathering Rights" in the Fall 2016 issue of the Silha *Bulletin*.)

Second, the complaint further argued that the defendants had "a history of deficient or non-existent training with respect to the Constitution in general and Plaintiff's First Amendment rights in particular." The complaint provided the example of Minneapolis Police Policy and Procedure Manual Section 6-200, which provides that "MPD employees shall not unnecessarily obstruct news media personnel from performing their duties at emergency scenes," but does not provide any "other instruction or guidance on how to identify the media or ensure their First Amendment rights are respected." The complaint added that the MPD "has not investigated, disciplined, or suspended any officer involved in any of the unlawful conduct described in this Complaint."

Third, the complaint alleged three counts against the defendants under 42 U.S.C. § 1983, known as a "1983 action." The first count claimed that the defendants "retaliated against Plaintiff and the Plaintiff Class for engaging in constitutionally protected [reporting] activity," in violation of the First Amendment. The complaint argued that the police's actions created a chilling effect on constitutionally protected activity, namely journalists' ability "to observe and record some events of public interest, including constitutionally protected demonstrations and the conduct of law enforcement officers on duty in a public place."

The second count alleged that the defendants violated the Fourth Amendment protections against unlawful seizure and excessive force. The complaint claimed that the plaintiff and plaintiff class "were seized by Defendants" when officers 1) detained and/or arrested the members of the news media and 2) "intentionally, through the use of force and threat of arrest, chemical agents, and nonlethal projectiles, terminated their freedom of movement." The complaint claimed that law enforcement officers did so even though the journalists "did not commit a crime."

The third count alleged that the "Due Process rights of Plaintiff and the Plaintiff Class were violated" when police "arrested members of the Plaintiff Class without probable cause, and deployed chemical agents and nonlethal projectiles without providing a warning and opportunity to disperse in a way that a person of ordinary intelligence could understand and comply with."

Finally, the complaint sought several forms of relief, including a permanent injunction "barring Defendants

Protests, *continued on page 4*

Protests, *continued from page 3*

from engaging in unconstitutional conduct targeting journalists." The complaint also sought a "declaration that Defendants' conduct violated the First, Fourth, and Fourteenth Amendments of the U.S. Constitution." Additionally, the complaint sought "[d]amages compensating [Goyette] for his injuries, including but not limited to compensatory, pecuniary, and medical expense damages."

The full complaint is available online at: https://www.aclu.org/legal-document/goyette-v-city-minneapolis.

In a press release accompanying the lawsuit, the ACLU of Minnesota stated, "Throughout the George Floyd protests, there have been numerous, well-documented instances of deliberate abuse against journalists by law enforcement officers.. . . These attacks violate the press's clearly established First Amendment right to report on public protests and police activities. An open society depends on a free press to keep the public informed and to bear witness to government actions. When law enforcement officers target members of the press with impunity, they strike at the root of our democracy." The press release added, "Law enforcement officers who perpetrate these abuses must be held accountable for their actions to the fullest extent of the law."

On June 9, 2020, District of Minnesota Judge Wilhelmina M. Wright dismissed Goyette's motions for a temporary restraining order (TRO) and class certification. Regarding the TRO, Wright held that Goyette "d[id] not allege that any of the conduct that he seeks to enjoin — occurring over a five-day period of unprecedented civil unrest — has occurred since May 31, 2020, or facts that plausibly demonstrate that such conduct is likely to recur imminently." As a result, he did not meet his burden of showing "irreparable harm," according to Wright.

However, Wright wrote that she "recognize[d] the gravity of Goyette's claims." She continued, "Essential to free government, the freedom of speech and freedom of the press are among our most fundamental rights and liberties. Abridgment of these rights 'impairs those opportunities for public education that are essential to effective exercise of the power of correcting error through the process of popular government,'" citing *Thornhill v. State of Alabama*, 310 U.S. 88, 95 (1940). She added, "The protests in Minnesota, and now around the globe, are rooted in acts of shocking police brutality. The police response to those protests is of exceptional importance to how the community moves forward. Media reporting on events like those at issue here enables the public to meaningfully participate as citizens in a constitutional democracy."

> "The protests in Minnesota, and now around the globe, are rooted in acts of shocking police brutality. The police response to those protests is of exceptional importance to how the community moves forward. Media reporting on events like those at issue here enables the public to meaningfully participate as citizens in a constitutional democracy."
>
> **— District of Minnesota Judge Wilhelmina M. Wright**

Wright therefore wrote that members of the news who were "allegedly threatened or subject to unlawful arrests" and/or "sustained severe, permanent injuries while reporting on events of intense public concern . . . deserve better." But that was not enough, according to Wright, for Goyette to "establish[] that the 'extraordinary' equitable relief he seeks." She therefore denied his motion for a TRO without prejudice.

Regarding the motion for class certification, Wright held that although "Goyette's claims may ultimately be suitable for class-wide resolution, the Court concludes that fact discovery is necessary to determine" whether the requirements for filed a class action were met. She therefore dismissed the motion without prejudice.

As the *Bulletin* went to press, the ACLU of Minnesota had not filed a revised complaint, nor had the lawsuit moved to discovery.

On June 10, 2020, Linda Tirado, a freelance journalist who permanently lost vision in one eye after being hit with a rubber bullet while covering the protests in Minneapolis, filed a lawsuit against Arradondo, Kroll, Harrington, Langer, and four unnamed police officers in the District of Minnesota. The complaint first stated that "[u]ntil recently, few Americans could have imagined police officers shooting at journalists reporting on civil protests."

Second, the complaint alleged that police tear gassed Tirado even though "her press credentials were displayed prominently around her neck" and was allowed to photograph the protests because members of news media were exempt from the city-wide curfew. The complaint also noted that Tirado yelled "I'm press, I'm press" as the police fired tear gas at protesters and herself.

Third, the complaint asserted that Tirado was acting under color of law and that the police's actions were an affront to freedom of the press. The complaint read, "Whatever one's view of police conduct in relation to the protestors, and of protestors' actions, there can be no doubt that under the . . . First Amendment, the police must not shoot journalists reporting on civil protests. Journalists, like Linda Tirado, cover the protests and capture any tactics employed by law enforcement. If the press is silenced, the story does not get amplified, and nobody can see the police violence committed against citizens for exercising their First Amendment rights[.]"

Fourth, the complaint raised several causes of action, including § 1983 actions alleging violations of the First Amendment. The complaint contended that the defendants "used excessive force against [Tirado] to prevent her coverage of the matters of public concern," therefore violating her "First Amendment rights to free press, speech and the right to peacefully assemble." The complaint also alleged that the defendants "retaliated against Plaintiff and other members of the press by use of excessive force in response to the exercise of their constitutional rights." Additionally, the complaint asserted that law enforcement's actions "chill[ed Tirado] from exercising her constitutional rights" because she was "not medically cleared to visit the protests because the tear gas utilized by

law enforcement is a chemical irritant, and may further damage her eye." Additional causes of action included § 1983 actions regarding violations under the Fourth Amendment and "Civil Conspiracy to Violate Plaintiff's Constitutional Rights," as well as claims under state law for assault and battery.

Finally, the complaint sought a permanent injunction "enjoining Defendants from engaging in the use of excessive force against Plaintiff in violation of her constitutional rights. The complaint also asked the District of Minnesota to declare that the defendants' actions were unconstitutional, including under the First and Fourth Amendments. Lastly, the complaint sought "[d]amages compensating Plaintiff for her injuries against all Defendants, jointly and severally," as well as punitive damages.

The full complaint is available online at: https://www.courthousenews.com/wp-content/uploads/2020/06/Tirado-v-Minneapolis.pdf. As the *Bulletin* went to press, the District of Minnesota had not ruled on the lawsuit.

According to Minnesota Public Radio (MPR) on June 16, 2020, MPD spokesperson John Elder acknowledged that an MPD officer may have fired the rubber bullet at Tirado.

In a June 10 interview with *Courthouse News*, Tirado said, "I had no reasonable expectation for being in any sort of trouble for being out at that hour, because the press was specifically expected [to cover the protests]." She continued, "My goal here is to ensure that this does not continue to happen, to bring attention to the fact that this has happened a lot around the country, that this happened in Minneapolis, and that it's really not fair." Tirado added that she hoped to donate a portion of proceeds from the lawsuit to communities affected by the fallout of the protests and riots.

On July 8, 2020, Kroll, one of the defendants in the case and the president of the union representing MPD officers, filed a motion to dismiss pursuant to Rule 12(B)(6). The memorandum in support of the motion argued that there was "no allegation" that Kroll "deployed the projectile that allegedly injured Plaintiff" or "directed MPD officers to deploy a projectile (or use force on Plaintiff)." The memorandum continued, "In fact, there is no allegation that Defendant Kroll was even on duty as a police officer at the time of the alleged injuries.. . . The Complaint should be dismissed because it does not contain 'enough facts to state a claim to relief that is plausible on its face.'"

The memorandum further argued that "[t]o allow this case to move forward would have a significant chilling effect on [the Minneapolis Police] Unions' and its elected union officials to engage in speech on matters of public concern." The memorandum added, "It would decimate the protections of the First Amendment and create a deluge in litigation based solely on the content of a Defendant's speech.. . . The irony that this lawsuit comes from a member of the media, traditional stalwarts of First Amendment protections, against Defendant Kroll based solely upon Defendant Kroll's protected speech cannot be lost."

The full memorandum is available online at: https://www.courtlistener.com/recap/gov.uscourts.mnd.188119/gov.uscourts.mnd.188119.20.0.pdf. As the *Bulletin* went to press, the District of Minnesota had not ruled on Kroll's motion.

A final lawsuit arose amidst growing concerns regarding police not releasing public records in the wake of the protests. On June 8, 2020, Tony Webster, a journalist and open records advocate in the Twin Cities, filed a lawsuit against the MPD, City of Minneapolis, and Casey Joe Carl in his official capacity as statutory responsible authority in the Minnesota Fourth Judicial District Court.

The complaint first argued that the MPD "has been systemically withholding police officer complaint and discipline data from the public in violation of state law, and releasing inaccurate data."

Second, the complaint explained that in October 2019, Webster filed an open records request to the MPD under the Minnesota Government Data Practices Act (MGDPA) seeking police officer complaint and discipline data for all current MPD officers, including "complaints and charges, the final disposition of disciplinary action, and the complete terms of any employment dispute settlement agreement." According to the complaint, such records are classified as "public" under the MGDPA and are therefore subject to release.

Third, the complaint alleged that six weeks after Webster submitted the request, the MPD had not provided any responsive data, despite the MGDPA requiring "prompt" compliance with requests. A week later, the MPD provided some limited responsive records, but they did not match what was available on the City of Minneapolis' website, according to the complaint. In a June 8 tweet, Webster noted that "[i]n what little complaint and discipline data Minneapolis Police did give me, they illegally redacted officer names and removed the factual details in discipline matters, which is public under law. And the complaint quantity is wildly inaccurate as compared to prior data releases."

According to the complaint, seven months after Webster filed his request, the MPD had "still not produced *any* discipline details or letters for *any* Minneapolis police officers; the MPD has not produced the substantive details on *any* sustained complaints or discipline for *any* Minneapolis police officers; and the MPD has not produced *any* employment settlement agreements for *any* Minneapolis police officers" (emphasis in original). The complaint added that the MPD "ignored Webster's request for a time and cost estimate, and for a rolling production of responsive data." According to the complaint, the result was that Webster "currently does not know when or if the MPD will ever comply with his request. And Webster has heard from other community members that they, too, have been unable to get access to this data, which is public under law."

Finally, the complaint asked the court "to enjoin the MPD's further violations, issue an order compelling their compliance with the MGDPA, award damages, costs, and attorney's fees, order a civil penalty, and order such other relief as allowed by law." The full complaint is available online at: https://assets.documentcloud.org/documents/6939235/Complaint-Webster-v-Minneapolis-Police-Department.pdf.

On June 18, Webster tweeted that the MPD had "started sending me some discipline records! I'll start putting them online once I have a bigger set. I am appreciative for their work, but it sucks that I have to sue to get basic compliance with the law."

On June 22, Webster filed a "stipulation to extend time for defendants to answer," meaning he and the defendants agreed to grant more time for the City of Minneapolis to respond to his complaint. The stipulation noted that "[w]ithout admitting liability

Protests, *continued on page 6*

Protests, *continued from page 5*

at this juncture, the City agrees Webster is entitled to copies of the data he requested, subject to any provisions of law which would require redaction or withholding of some of the data, and the City avers that it is working to evaluate how much time it needs to complete production." The stipulation added, "So that the Parties may attempt to work toward an early resolution of the case, this extension of time is warranted. Additionally, the ongoing COVID-19 pandemic and civil unrest in Minneapolis further warrants the extension of time." The full stipulation is available online at: https://tonywebster.com/files/20200622-Webster-v-MPD-Stipulation-to-Extend-Time-for-Defendants-to-Answer.pdf.

Concerns about law enforcement transparency following the protests over George Floyd's death prompted a statement by the National Freedom of Information Coalition and the Brechner Center for Freedom of Information. The statement was signed by more than 50 organizations, including the Silha Center for the Study of Media Ethics and Law. The statement read in part, "Many of our nation's cities have experienced unrest and violence in response to the death of George Floyd at the hands of a Minneapolis police officer with a long record of public complaints. 'Business as usual' in the oversight of law enforcement is not a satisfactory response to urgent and well-founded concerns that police officers are able to avoid consequences for wrongdoing, abetted by a tight regime of official secrecy. Change must happen."

The statement added, "More public oversight leads to better policing, which leads to better public safety and stronger communities. A small, but concrete, show of good faith would be for every state to enact reforms opening every aspect of the police misconduct oversight process to public scrutiny. Only by seeing the substance of each complaint, how it is resolved, and what consequences are imposed can the public trust that justice is being dispensed without favor." The full statement is available online at: https://www.nfoic.org/sites/default/files/2020-06/Statement%20on%20law%20enforcement%20transparency%20and%20accountability%20issues%20June%202020%20%282%29.pdf.

Meanwhile, on June 16, 2020, Alexis Johnson, a black reporter for the *Pittsburgh Post-Gazette*, filed a lawsuit under the Civil Rights Act of 1866, 42 U.S.C. § 1981, against the newspaper in the Western District of Pennsylvania, alleging that the news outlet refused to allow her to cover the protests over the death of George Floyd in Pittsburgh because of a tweet from her personal account regarding racial biases towards riots and looting.

On May 31, 2020, Johnson tweeted four photographs showing debris-strewn parking lots. The photos were accompanied by a message reading, "Horrifying scenes and aftermath from selfish LOOTERS who don't care about this city!!!…oh wait sorry. No these are pictures from a Kenny Chesney concert tailgate. Whoops." The tweet is available online at: https://twitter.com/alexisjreports/status/1267081467731103749?s=20.

> "More public oversight leads to better policing, which leads to better public safety and stronger communities. A small, but concrete, show of good faith would be for every state to enact reforms opening every aspect of the police misconduct oversight process to public scrutiny."
>
> **— Statement signed by the Silha Center for the Study of Media Ethics and Law and other media advocacy organizations**

Johnson's complaint first explained that the tweet, which was "posted on her private Twitter account," was her "object[ion] to the racial bias exhibited by those members of society and public officials who equated property damage to human life." The complaint continued, "By sharing these photographs and commentary on her private Twitter page, Johnson intended to mock and ridicule, and thus to protest, the racial bias and discrimination in a society that condemns African Americans who oppose racial injustice by protests that result in some property damage, while tolerates similar property damage by predominately white crowds who attend Chesney concerts."

Second, her complaint alleged that Johnson had worked for the *Pittsburgh Post-Gazette* since October 2018 and had "often" been assigned "to cover social issues that manifested themselves in online social media platforms."

The complaint further alleged that on June 1, 2020, three *Post-Gazette* editors, including the managing editor, "told Johnson her tweet showed she could not cover the protests fairly and that therefore she would not be assigned to report on them." The complaint added, "Defendant's Managing Editor informed Johnson that because she had opposed and spoke out [*sic*] about racism and the murder of black people at the hands of police, and offered an opinion opposing those things, she was theretofore [*sic*] precluded from covering any story involving protests or demonstrations concerning racial discrimination or the murder of black people by white police."

According to *Courthouse News* on June 16, members of Johnson's union, the Newspaper Guild of Pittsburgh, started a protest on Twitter supporting Johnson. The complaint asserted that the 80 journalists employed by the *Post-Gazette* were similarly barred from covering the protests. The complaint also alleged that Michael Santiago, "an African American Pulitzer Prize-winning photojournalist who was at the time employed by Defendant, and who had tweeted in support of Johnson's Twitter protest[,] also was removed from photographing racial demonstrations."

Fourth, the complaint argued that the *Post-Gazette* had "not treated reporters and journalists who have commented on bias toward whites in a similar manner." It provided the example of Joshua Axelrod, a white *Post-Gazette* employee, who called a man accused of vandalism and looting a "scumbag." According to the complaint, Axelrod was not prevented from covering the protests. The complaint also referenced how the *Post-Gazette* did not prevent reporters who had made similar public statements against race discrimination from covering the 2018 shooting at the Tree of Life Synagogue in Pittsburgh.

The complaint alleged one count under the Civil Rights Act of 1866, 42 U.S.C. § 1981, for retaliation, arguing

that the *Post-Gazette* "precluded and removed Johnson, and others from covering major stories involving race based protests and demonstrations in retaliation for opposing race discrimination and publically [*sic*] announcing her opposition to such practices." The complaint further argued that such actions were "materially adverse employment action[s] because a reasonable newspaper reporter would have been dissuaded from complaining of race discrimination had she known she would have been precluded from the assignment of coverage of a major story[.]" The complaint added that the actions "deprived Johnson of the same right to make and enforce contracts as is enjoyed by white citizens in violation of . . . 42 U.S.C. §1981."

The complaint also alleged one count of race discrimination under 42 U.S.C. § 1981, arguing that the *Post-Gazette* precluded and removed Johnson from covering the protests "because of her race, and therefore[,] deprived Johnson of the same right to make and enforce contracts as is enjoyed by white citizens." The complaint alleged that Johnson suffered "[g]reat mental anguish and emotional strain," "[h]umiliation and inconvenience," and "[d]iminished career advancement because of the inability to cover one of the major newspaper stories of her time."

Finally, the complaint requested several forms of relief, including that the *Post-Gazette* "be ordered to cease precluding Johnson from coverage of racial discrimination protests and demonstrations" and "be required to compensate Johnson for the diminishment of her career advancement she would have obtained had it not been for Defendant's illegal treatment," among other relief.

The full complaint is available online at: https://www.courthousenews.com/wp-content/uploads/2020/06/Post-Gazette-complaint.pdf. As the *Bulletin* went to press, the Western District of Pennsylvania had not ruled in the case.

According to KDKA, Pittsburgh's CBS affiliate, at a June 8 press conference, Newspaper Guild of Pittsburgh president Michael Fuoco called the *Post-Gazette*'s actions a "national embarrassment" and that the *Post-Gazette* "is on the wrong side of history. We're on the right side of history." He added, "[Y]ou hire diversity to get all points of view, different lived experiences. For them to thumb their nose in that to me is only racial discrimination. Prove me wrong and put them back on the coverage."

Johnson told reporters at the press conference, "None of us should be here today.. . . We should be covering one of the pivotal moments in history."

Multiple Disputes Arise About Access to Information

George Floyd's death led to multiple disputes over public access to information about the killing, subsequent criminal proceedings, and the people involved in the case. One significant legal issue involving the news media related to access to footage of videos recorded by body-worn cameras that the charged police officers were wearing when they encountered Floyd. On July 7, a lawyer for Thomas Lane, one of the police officers charged, filed the footage with the court as exhibits as part of a motion to dismiss the criminal charges for lack of probable cause. Hennepin County District Judge Peter Cahill allowed members of the press and public to view the videos but not make copies; he had previously raised concerns about the possibility that pretrial publicity would prejudice the defendants' Sixth Amendment right to a fair trial. On July 13, a coalition of media organizations, including the Silha Center for the Study of Media Ethics and Law, filed a motion seeking permission to get copies of the videos. The Court held a hearing on the motion on July 21.

On August 7, Cahill granted the coalition's request to obtain copies "upon payment of an appropriate fee established by this Court's administrative personnel." In a memorandum opinion filed August 11, Cahill explained the rationale for his decision, writing: "Cases that generate intense public interest and media scrutiny highlight the tension between two fundamental rights: the right guaranteed under the federal and state constitutions to criminal defendants to receive a fair trial before an impartial jury, on the one hand, and the right of the public and press to attend criminal trials, on the other hand."

Cahill first discussed various positive benefits that courts have found flow from public access to judicial information. Citing *Richmond Newspapers v. Virginia*, 448 U.S. 555 (1980), Cahill acknowledged that the "the open processes of justice serve an important prophylactic purpose, providing an outlet for community concern, hostility, and emotion." Cahill also cited *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982), which found that public and press access to a criminal trial "enhances the quality and safeguards the integrity of the factfinding process," "fosters an appearance of fairness, thereby highlighting public respect for the judicial process," and "permits the public to participate in and serve as a check upon the judicial process." Finally, Cahill quoted *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986): "The value of openness lies in the fact that people not actually attending trials can have confidence that standards of fairness are being observed; the sure knowledge that anyone is free to attend gives assurance that established procedures are being followed and that deviations will become known. Openness thus enhances both the basic fairness of the criminal trial and the appearance of fairness so essential to public confidence in the system."

However, Cahill explained that the defendants in the criminal cases "are entitled to a fair trial, before an objective and impartial jury, applying the evidence that will be presented in open court during a trial governed by the rules of evidence to the law applicable to the crimes with which they are charged." Cahill wrote that the Supreme Court of the United States has "made clear that trial judges have an 'affirmative constitutional duty to minimize the effects of prejudicial pretrial publicity' to safeguard a criminal defendant's due process rights," citing *Gannett Co., Inc. v. DePasquale*, 443 U.S. 368 (1979). Cahill also quoted at length from *Sheppard v. Maxwell*, 384 U.S. 333 (1966), in explaining why the court must take steps to ensure the defendants "receive a trial by an impartial jury free from outside influences." Cahill added, "Important, fundamental rights oft times find themselves in tension; that is unavoidable. This Court is committed to the management of pretrial proceedings and the eventual trial(s) in these cases not only to vindicate the public's and press' rights of access guaranteed by the First Amendment, the common law, and court rules but also Lane and his fellow co-defendants' Sixth Amendment rights to a fair trial, and this Court's and the parties' interests in seeing that justice be done by a fair and objective jury determining the facts based solely on evidence that will be admitted at trial."

Protests, *continued on page 8*

Protests, *continued from page 7*

Cahill wrote that he did not issue the gag order or restrict copying of the body camera video "in the interests of 'secrecy,'" and he pointed out that court filings in the cases have been posted online and that the body camera footage was made available for inspection. Rather, Cahill wrote, "the Court was attempting to mitigate what some might colloquially characterize as efforts to 'try the case in the press,' to seek to avoid or at least to ameliorate the prospects of unduly tainting the prospective jury pool engendered by the intense media interest and reporting on these cases, and to seek to vindicate the Defendants' rights and the State's interest in ensuring justice is done in these cases by a fair and impartial jury deciding whether the Defendants are guilty or not guilty of the State's charges based solely upon the evidence presented during trial, not based on media reporting, public speculation, and extraneous information, inadmissible at trial, circulating during the months of pretrial preparation."

In his analysis, Cahill first found that the media coalition had standing to intervene, citing federal court access cases such as *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982) and *Richmond Newspapers v. Virginia*, 448 U.S. 555 (1980), as well as state cases including *Mankato Free Press Co. v. Dempsey*, 581 N.W.2d 311 (Minn. 1998), and *Northwest Publications, Inc. v. Anderson*, 259 N.W.2d 254 (Minn. 1977). Cahill then cited Minn. R. Crim. P. 25.03 subds. 1-3 in finding that the "Minnesota Rules of Criminal Procedure expressly confer standing on the news media to challenge certain orders 'restricting public access to public records relating to a criminal proceeding.'"

Second, Cahill found that the public and press have a right of access to the body-camera video under both the common law and court rules. Cahill found that access was governed under *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978), and *Minneapolis Star Tribune Co v. Kammeyer*, 341 N.W.2d 550 (Minn. 1983), as well as the Minnesota Rules of Criminal Procedure and Rules of Public Access to Records of the Judicial Branch. Cahill rejected some cases the media coalition cited because the cases were either materially distinguishable or arose in other jurisdictions and were not binding.

Third, Cahill did not rule on whether the public and press have a First Amendment right of access to the body-worn camera footage because he granted access under the "Minnesota Rules of Criminal Procedure, the Minnesota Rules of Public Access to Records of the Judicial Branch, and the common law."

On August 3, several days before Cahill's ruling allowing copies of the body-camera footage to be released, the U.K.'s *Daily Mail* newspaper published leaked segments of the footage, which was obtained in apparent violation of Cahill's earlier order authorizing viewing of the videos but prohibiting recording or distribution of them. The *Daily Mail* reported that the footage had been "leaked" to the newspaper. On August 3, the *Star Tribune* reported that a Hennepin County District Court spokesperson said an investigation had been launched into the leaked video.

> "The law does not tolerate this level of secrecy."
>
> **— Media coalition memorandum seeking to unseal divorce file of Kellie and Derek Chauvin**

The court had made the videos available for viewing on laptops in a room where attendees were required to put away phones and personal computers. "Sheriff's deputies and court staff were stationed throughout the room as several members of the media and public viewed the videos," the *Star Tribune* reported.

In response to the *Daily Mail*'s posting of the videos, the media coalition filed a letter with Cahill on August 4 informing the court that members of the media coalition "respect the Court's orders and were surprised by the leak of this footage." The media coalition further argued that the leak "serves only to bolster the Coalition's argument for making all of the [body-worn camera] footage available, through official channels, for copying and distribution." Following Cahill's order allowing for copies of the body-worn camera footage, journalists sought and obtained copies and published the footage.

Another access issue that arose was the sealing of court records about divorce proceedings between Minneapolis Police Officer Derek Chauvin — the officer who kneeled on Floyd's neck — and his wife, Kellie Chauvin, who filed for divorce days after Floyd's death. Both Kellie and Derek Chauvin filed a joint motion to seal the divorce case, arguing that sealing was warranted because they had been subject to "rage and violence" and alleged identity theft and financial crimes, according to the *Star Tribune*. Public access to the case records would enable additional harassment of Kellie Chauvin and open hearings would allow the public to know where the Chauvins reside and "negatively affect the parties from a safety standpoint," the joint motion argued, according to the *Star Tribune*. On July 24, information about the case became unavailable through the state's online electronic docketing system, the *Star Tribune* reported, "presumably because a judge had granted the Chauvins' request."

On July 27, 2020, a coalition of local and national news organizations, as well as the Minnesota Coalition on Government Information, filed a motion to intervene and unseal the case file and a memorandum in support of that motion. The memorandum argues that the apparent wholesale sealing of the case file, including the docketing information and the existence of the case, is not permissible. "The law does not tolerate this level of secrecy," the memorandum reads. It added that there was considerable public interest in Derek Chauvin, the criminal and civil proceedings involving him, and the broader social issues that Floyd's death highlighted, such as the Black Lives Matter movement. The memorandum linked the divorce proceedings directly to Floyd's death by asserting that the divorce "may be an attempt to shield the couple's assets from criminal forfeiture or from recovery by the Floyd family in the civil lawsuit," and that information in the divorce proceedings may also be relevant to felony tax fraud charges filed against the couple, all of which increase the public interest in the divorce case. The coalition argued that they have a right to intervene in the divorce case to pursue access to public records, that the press and public are presumptively entitled to access court files, including divorce proceedings, and that there is sufficient justification for sealing the records at issue.

On Oct. 8, 2020, Washington County District Judge Juanita C. Freeman granted the media coalition's request to intervene in the divorce proceedings, finding that the coalition satisfied the four-part test that a non-party must meet to intervene as a matter of right. Freeman found that the coalition's motion was timely, that the coalition had an interest in the proceedings, that the court had previously restricted access to court records, and the coalition's interests were not sufficiently represented by the other parties.

Freeman analyzed the coalition's arguments that access was required under both the First Amendment and common law and rejected both arguments. Under the First Amendment, a court may restrict access when there is a compelling government interest and the restriction is narrowly tailored to serve that interest. Freeman found restricting access to the Chauvins' personal and financial information in court records served a compelling government interest in prevention of crime, and withholding this information was narrowly tailored. "The record amply demonstrates that restricting access to this information is not only warranted but necessary to counteract the persistent efforts of criminals, hackers, and other malicious actors who seek to exploit the Chauvins' personal information to commit theft, fraud, stalking, harassment, property damage, and other crimes," Freeman wrote.

Freeman also explained why the court file can be sealed under common law, balancing "the interests favoring access, along with the presumption in favor of access, against those asserted for restricting access." Freeman cited the various harms to the Chauvins that she discussed in the First Amendment analysis, and added that "the Chauvins' marital status is not a matter of public concern, nor is the division of their material assets and debts."

Although Freeman denied the media coalition's motion to unseal the divorce file, she ordered that the case be listed on the court system's public docket and that various filings be public. Freeman also ordered that the divorce petition be sealed, but attached a redacted version of the petition to the order. The order stated that all personal information about the Chauvins should be sealed, including financial and property information and "descriptions of unlawful acts[] and the effects of such acts." The order did not preclude the public from attending court hearings held in connection with the case.

A third dispute that arose about public access to information involved a gag order that Cahill imposed on speech related to the case. On July 9, Cahill issued a gag order after some attorneys involved in the case spoke to the news media. Cahill expressed concern that pretrial publicity "by the attorneys involved will increase the risk of tainting a potential jury pool and will impair all parties' right to a fair trial." The text of the order restricted speech of "all parties, attorneys, their employees, agents, or independent contractors working on their behalf."

On July 17, a coalition of local and national media outlets, as well as the Silha Center for the Study of Media Ethics and Law and the Minnesota Coalition on Government Information, filed a motion objecting to the gag order. The objection argued that the gag order was impermissibly overbroad in violation of the First Amendment. The coalition argued that the order "threatens the right of the press and the public to engage in important dialogue with a wide range of people on a broad range of topics that could be viewed as 'related' to these prosecutions. The Order could also directly (if inadvertently) delay communications, to the public, about important work government officials are doing to address critical issues of public safety, racial equality and police reform. Such issues, while carrying little to no risk of prejudicing the Defendants' right to a fair trial, are nonetheless 'related' to the prosecutions." Defense counsel also objected to the gag order. On July 21, the *Star Tribune* reported that Cahill vacated the gag order.

Misinformation About George Floyd's Death and Ensuing Protests Spreads on Social Media

On June 1, 2020, *The New York Times*, among several other media outlets, reported that "untruths, conspiracy theories, and other false information [were] running rampant online as the furor over [the death of George Floyd] has built." Among the misinformation online was the unfounded rumor that Floyd was still alive and that "Antifa" activists were responsible for the riots and looting in several U.S. cities, including Minneapolis.

The *Times* noted that President Donald Trump "stoked the divisive information" in a May 31 tweet that blamed "Antifa-led anarchists" in Minneapolis for the violence and damage and called Antifa a "Terrorist Organization," whereas it as an anti-fascist protest movement.

On June 5, KSTP, the Twin Cities' ABC affiliate, reported that some of the false information spread about Floyd and the protests was repeated and shared by local politicians in Minnesota. KSTP provided the example of Minnesota Rep. Ryan Winkler (DFL-Golden Valley), the Minnesota House Majority Leader, who tweeted about the tanker truck driving into a crowd of protesters on Interstate 35W on May 31. Winkler tweeted, "Protestors I know are saying truck driver drove into a crowd and intentionally ran into them. Confederate flags and white supremacist insignia. [*sic*]" It later turned out, according to KSTP, that such claims were not true. Winkler deleted the tweet, but not before it was retweeted or shared more than 500 times.

Winkler told KSTP in an interview, "I think I behaved reasonably under the circumstances. I was clear that this was not something that I saw. This was something that people were saying."

However, in a June 5 interview with KSTP, Clair Wardle, the co-founder of First Draft, a nonprofit dedicated to fighting misinformation around the world, explained that even unintentionally false information can be a problem. "Right now, when emotions are so high on both sides, everybody is more susceptible than ever, but we're weaponizing information. These tweets are not harmless," she said. "Anybody can post anything on social media. They might have a blue tick next to their name, they might be in a position of leadership.. . . We have always looked to gatekeepers for the truth and so, when you see information from those people, we are hard-wired to believe that, so that does make it more dangerous."

KSTP also noted how Minneapolis Council Members Alondra Cano and Phillipe Cunningham also shared misinformation about the presence of the Minnesota National Guard and the Ku Klux Klan (KKK), respectively. The Minneapolis *Star Tribune* similarly found on June 6, 2020 that "[t]hrough the chaos of a riotous string of days following George Floyd's death under the knee of a Minneapolis police officer,

Protests, *continued on page 10*

Protests, *continued from page 9*

Winkler was hardly the only public official to unwittingly disseminate false or unverified information about the facts on the ground." The *Star Tribune* and KSTP both reported that media research company Zignal Labs had tracked more than 1.7 million mentions of misinformation related to Floyd's death and the subsequent protests.

Additionally, KSTP described how misinformation was also spread by public officials offline, including when Minnesota Gov. Tim Walz, among others, incorrectly stated in May 30 and May 31 news conferences that all or most of the people arrested during the protests and riots were from "out of state" or "outside the region." Officials later corrected those assertions when jail records were released, according to KSTP. KSTP's full report is available online at: https://kstp.com/news/amid-flood-of-misinformation-surrounding-george-floyd-death-days-of-unrest-local-leaders-share-false-information/5752299/.

In an interview with the *Star Tribune*, retired Carleton College political scientist Steven Schier said public officials face "a higher bar" for reporting and sharing accurate information, including on social media. However, he acknowledged that meeting that standard can be especially challenging amid a "fog of conflict." "They're trying to make real-time assessments," he said. "A lot of that information is going to be fuzzy or false and they have to correct it as they occur."

Emily Vraga, an associate professor at the University of Minnesota Hubbard School of Journalism and Mass Communication similarly told the *Star Tribune* on June 6, 2020, that "[t]here is a special emphasis for people who do have that power, whose voice will not just be heard but have a lot of credibility, that they have to get it right to the extent they can from the get-go." She added that it "is incumbent on people who have a prominent platform to be especially careful" and that public officials delete and correct inaccurate posts if possible to try to prevent misinformation from spreading further.

In a June 1 interview with *The New York Times*, Graham Brookie, director of the Atlantic Council's Digital Forensic Research Lab, explained that the combination of racial tensions and political polarization during the COVID-19 pandemic led to a significant increase in misinformation, including related to Floyd's death and the ensuing protests. "The combination of evolving events, sustained attention and, most of all, deep existing divisions make this moment a perfect storm for disinformation," he said. "All of it is toxic, and make our very real challenges and divisions harder to address." (For more information about the spread of mis- and disinformation during the COVID-19 pandemic, see *COVID-19 Pandemic Raises New Concerns About Misinformation Online* in "Special Report: COVID-19 Pandemic Raises Media Law and Ethics Issues, Challenges, and Opportunities" in the Winter/Spring 2020 issue of the Silha *Bulletin*.)

In a June 1, 2020 article, *USA Today* provided several tips to identify false or misleading claims online, including related to Floyd and the protests. The article encouraged members of the public to "[d]o your homework before sharing" and "[w]atch out for posts that make your blood boil." The article also recommended that individuals "check [their] bias" and "[d]on't trust everything you see," among other tips and advice. The full article is available online at: https://www.usatoday.com/story/tech/2020/06/01/george-floyd-protests-disinformation-misinformation-surging-online/5313920002/.

A June 2 article by *Rolling Stone* magazine also provided a number of ways that members of the public can "differentiate between truth and fiction on social media." Among the pieces of advice were to "[c]heck the source of the story" and "[a]pproach posts about missing people with caution." The article also encouraged people looking to make donations to do so through "an accredited organization." The full article is available online at: https://www.rollingstone.com/culture/culture-features/misinformation-facebook-george-floyd-protest-1008909/.

(The 2020 Silha Spring Ethics Forum featuring Barbara Allen, the director of college programming at the Poynter Institute of Media Studies (Poynter), focused on the spread of mis- and disinformation online and how journalists and members of the public can spot and address it. For more information on the forum, see "2020 Spring Forum Webinar Addresses the Impact of Fact-Checking and Misinformation on Journalism" in the Winter/Spring 2020 issue of the Silha *Bulletin*.)

— Scott Memmel
Postdoctoral Associate

— Jonathan Anderson
Silha *Bulletin* Editor

Director's Note

The Summer 2020 issue of the Silha *Bulletin* includes several articles adapted from "Global 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 2020.

Professor Kirtley gratefully acknowledges the contributions of Silha research assistants Jonathan Anderson, Scott Memmel, and Sarah Wiley, and Silha staff member Elaine Hargrove.

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

COVID-19 Pandemic Raises Data Privacy and Security Questions and Concerns

PRIVACY

In spring and summer 2020, the COVID-19 pandemic raised a number of challenges and issues related to data privacy and security, including regarding 1) Zoom Video Communications, Inc. (Zoom) and 2) the tracking of individuals' mobile location data to combat the spread of the coronavirus.

According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 is an illness caused by "a new coronavirus that can spread from person to person." As early as late 2019, the virus began spreading around the world, therefore constituting a global pandemic. The spread of the coronavirus, especially beginning in March 2020, prompted a range of responses by different countries, including the United States, in which states took varying degrees of action.

Privacy and Security Concerns Arise from Zoom Services, Practices, and Claims Amidst the COVID-19 Pandemic

Zoom, a video communications app and video conferencing platform, originally launched in 2013, but it was not a household word until the COVID-19 pandemic forced people to work and attend school from home. However, Zoom's platform raises multiple privacy and security concerns, including "Zoombombing," hacking of meeting recordings stored in the cloud, unauthorized data sharing, surveillance, bugs and malware, domestic and international hacking threats, and encryption deficiencies. Amidst these privacy and security concerns, Zoom took several actions to address such problems, leading to mixed reactions by observers and those affected. Meanwhile, Zoom was the target of several legal actions, including a 2019 lawsuit filed by the Electronic Privacy Information Center (EPIC), as well as four class action lawsuits filed in federal court in March and April 2020 and a lawsuit filed in the District of Columbia in August 2020.

Zoom was founded in 2011 by CEO Eric Yuan and launched in January 2013 before going public in April 2019. According to an Aug. 5, 2020 letter sent by Yuan and other Zoom executives to their clients, Zoom is a "video-first communications platform for the enterprise segment." *The Washington Post* described Zoom as a "business-friendly video chat." According to its website, Zoom, which is headquartered in San Jose, Calif., runs across mobile devices, desktops, telephones, and room systems. Among Zoom's features are a software application and a video conferencing platform.

When the COVID-19 pandemic forced large numbers of people worldwide to stay at and work from home in the first months of 2020, Zoom's use expanded from businesses meetings to school and university classes and church services, surpassing the popularity of video teleconferencing services such as Facebook's Messenger Rooms, Google Meet, Apple's Facetime, and others. According to an Aug. 5, 2020 statement by Zoom, usage increased from 10 million daily users in December 2019 to 300 million by April 2020.

Amidst the COVID-19 pandemic in 2019, several media outlets and observers highlighted a variety of privacy and security issues raised by Zoom, including "Zoombombing"; the vulnerability of recordings; problematic data sharing; surveillance; bugs and malware; domestic and international hacking; and encryption deficiencies.

First, several observers noted significant privacy and security concerns associated with Zoombombing, which occurs when a Zoom meeting is interrupted by a hacker engaging in activities that disrupt the event, such as posting pornography. According to CNET and "Krebs on Security," a blog by former *Washington Post* reporter Brian Krebs, Zoom conference calls are assigned a Meeting ID that consists of 9 to 11 digits. If meetings are not protected by passwords or by other means, they can be easily interrupted. In some cases, hackers simply guessed or automated the guessing of random IDs within that space of digits. Additionally, tools such as "Tor" allowed hackers to find about 100 open Zoom meetings every hour.

News outlets reported a number of instances of Zoombombing, including on March 30, 2020 when the Federal Bureau of Investigation's (FBI) Boston, Mass. office issued a warning that hackers had interrupted online instruction of a Massachusetts high school class, shouted a profanity, and revealed the teacher's home address. In a separate incident at another Massachusetts school, the hacker was visible on the video camera and displayed swastika tattoos.

On April 2, 2020, *Vice* reported that the white supremacist group 8chan had plans to highjack the Zoom meetings of a Jewish school in Philadelphia, Pa. in an anti-Semitic campaign. The following day, *The New York Times* reported that an analysis carried out by the newspaper revealed that "thousands" of people had gathered on "153 Instagram accounts, dozens of Twitter accounts and private chats on Reddit and 4Chan" to organize Zoom harassment campaigns, sharing meeting passwords and plans to disrupt public and private meetings. These plans included disrupting meetings with "shocking imagery, racial epithets and profanity." Disruptions included someone who embedded a racial slur in a presentation slide during a meeting of the Concordia Forum, a global network of Muslim leaders, followed by a pornographic video; projecting a GIF of a person drinking during Alcoholic Anonymous meetings; and writing racist messages during a meeting of the American Jewish Committee in Paris.

On April 21, *The Hill* reported that an April 20 virtual Holocaust memorial service held by the Israeli Embassy in Germany was Zoombombed with anti-Semitic slogans, photos of Adolf Hitler, and pornographic images. Hackers also shouted pro-Palestinian slogans.

Additional instances of Zoombombing were committed by high school students in several parts of the United States who disrupted their online classes with "disruptive but largely inoffensive jokes." These and other issues led some school districts to ban the use of Zoom.

Second, observers pointed out privacy issues associated with the recording features on Zoom. On April 16, 2020, CNET reported that a security researcher had discovered a way to access and download previously recorded videos in the cloud through an unsecured link. In addition, the

COVID-19, *continued on page 12*

COVID-19, *continued from page 11*

researcher discovered that previously recorded videos may "live" in the cloud for hours, even after being deleted by the users. As a result, Zoom provided updates to prevent malicious access to such videos. In addition, it changed its "Record to Cloud" default setting to request that the user add a password to the video file. CNET cautioned, however, that these updates might not protect videos that had previously been made available via shared links.

On April 3, 2020, *The Washington Post* reported that "[t]housands of personal Zoom videos have been left viewable on the open Web, highlighting the privacy risks to millions of Americans as they shift many of their personal interactions to video calls in an age of social distancing." The exposed videos included one-on-one therapy sessions, a training orientation for workers doing telehealth calls that included people's names and telephone numbers, small business meetings that included private company financial statements, and elementary school classes, in which children's faces, voices, and personal details were revealed. The *Post* further reported that a number of the videos included personally identifiable information and "deeply intimate" conversations, some of which were recorded in people's homes. Other recordings contained nudity, such as in an instructional video provided by an aesthetician.

The *Post* noted that many of these videos were recorded through Zoom's software, then saved without a password. Videos that were stored in Zoom's own system did not appear to be as vulnerable. Because Zoom has a consistent formula for naming videos, the *Post* stated that anyone who knew Zoom's system of naming could find, download, and watch the vulnerable videos. The *Post* did not reveal Zoom's naming system, and stated that the newspaper had alerted Zoom to the issue before running the story.

Third, on March 26, 2020, *Vice*'s "Motherboard" blog found that Zoom's iOS app sent "some analytics data to Facebook, even if Zoom users don't have a Facebook account." The report noted that although such data transfers were "not uncommon," Zoom users may not have been aware it was happening, "nor understand that when they use one product, they may be providing data to another service altogether." "Motherboard" noted that Zoom was "not forthcoming with the data collection or the transfer of it to Facebook. Zoom's policy says the company may collect users' 'Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products),' but doesn't explicitly mention anything about sending data to Facebook on Zoom users who don't have a Facebook account at all."

In a statement to "Motherboard," Zoom confirmed the data collection, writing, "Zoom takes its users' privacy extremely seriously. We originally implemented the 'Login with Facebook' feature using the Facebook SDK in order to provide our users with another convenient way to access our platform. However, we were recently made aware that the Facebook SDK was collecting unnecessary device data."

The statement continued, "To address this, in the next few days, we will be removing the Facebook SDK and reconfiguring the feature so that users will still be able to login with Facebook via their browser. Users will need to update to the latest version of our application once it becomes available in order for these changes to take hold, and we encourage them to do so. We sincerely apologize for this oversight, and remain firmly committed to the protection of our users' data."

In a message to *Vice*, privacy advocate Pat Walshe, who had previously analyzed Zoom's privacy policy, called the revelation "shocking." He added, "There is nothing in the privacy policy that addresses that."

About one week after "Motherboard" reported its findings, *The New York Times* wrote on April 2, 2020 that a "data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users — without Zoom asking for their permission during the meeting or even notifying them that someone else was snooping on them." According to the *Times*, "when people signed in to a meeting, Zoom's software automatically sent their names and email addresses to a company system it used to match them with their LinkedIn profiles."

The *Times* found that "even when a reporter signed in to a Zoom meeting under pseudonyms — 'Anonymous' and 'I am not here' — the data-mining tool was able to instantly match him to his LinkedIn profile. In doing so, Zoom disclosed the reporter's real name to another user, overriding his efforts to keep it private." Additionally, the *Times* discovered that Zoom "automatically sent participants' personal information to its data-mining tool even when no one in a meeting had activated it."

Josh Golin, the executive director of the Campaign for a Commercial-Free Childhood, a nonprofit group in Boston, told the *Times*, "People don't know this is happening, and that's just completely unfair and deceptive." The *Times* noted that its findings added "to an avalanche of reports about privacy and security issues with Zoom, which has quickly emerged as the go-to business and social platform during the [COVID-19] pandemic."

In an April 2020 statement, Zoom said it took users' privacy "extremely seriously" and was "removing the LinkedIn Sales Navigator to disable the feature on our platform entirely." In a separate statement, LinkedIn said it worked "to make it easy for members to understand their choices over what information they share" and would suspend the profile-matching feature on Zoom "while we investigate this further."

Fourth, the Electronic Frontier Foundation (EFF) posted several findings related to how the hosts of Zoom meetings, as well as school administrators, can conduct varying forms of surveillance on those using the app. EFF determined that the host of a Zoom meeting had "the capacity to monitor the activities of attendees while screen-sharing." According to EFF, this meant that "[i]f attendees of a meeting do not have the Zoom video window in focus during a call where the host is screen-sharing, after 30 seconds the host can see indicators next to each participant's name indicating that the Zoom window is not active." Furthermore, EFF found that Zoom "allows administrators to see detailed views on how, when, and where users are using Zoom, with detailed dashboards in real-time of user activity. Zoom also provides a ranking system of users based on total number of meeting minutes. If a user records any calls via Zoom, administrators can access the contents of that recorded call, including video, audio, transcript, and chat files, as well as access to sharing, analytics, and cloud management privileges."

EFF criticized these practices, especially in light of the increasing use of Zoom as part of online learning. "Surveillance shouldn't be a

prerequisite for getting an education," EFF contended. "But even before more school districts started moving their classes and coursework to digital forums for purposes of social distancing, surveillance has become more and more common in schools. With the advent of COVID-19 and the associated uptick in distributed digital learning, the potential for this surveillance to ramp up is alarming."

EFF therefore recommended that "[o]ne of the best things you can do to keep yourself and others safe during this crisis is to learn how to minimize risk. Many of the problems presented in this post can be mitigated or circumvented with careful consideration of the risks, employing 'privacy as a team sport' tactics, and minimizing the data that corporations, employers, and others can track."

Fifth, on May 8, 2020, CNET reported that several "bugs" or pieces of malware were plaguing Zoom users, including one that allowed people's passwords to be stolen. Another bug allowed malicious users to assume control of a Zoom user's microphone or webcam, and another allowed Zoom to gain root access to MacOS desktops. Additionally, on April 22, 2020, researchers at Morphisec Labs, which describes itself as an endpoint security solutions company, identified a bug that could enable hackers to record Zoom sessions and capture chat text without the knowledge of any of the participants, even if the host has not enabled any of the participants to record. The result was that the bug effectively allowed the hackers to spy on meetings.

On April 16, 2020, ZDNet reported that Zoom had hired Luta Security, a company specializing in managing system vulnerabilities and "bug bounty" programs, which pay people to identify problems and weaknesses with websites and company security systems. Luta Security, which is known for setting up bug bounty programs for Microsoft, Symantec, and the Pentagon, was given a "free hand" to rebuild Zoom's existing program.

Sixth, on April 28, 2020, ABC News reported that Zoom "could be vulnerable to intrusions by foreign government spy services, including China." ABC News had acquired a federal intelligence analysis report issued jointly by the U.S. Department of Homeland Security's (DHS) Cyber Mission and Counterintelligence Mission Centers. The report, dated April 27, 2020, was prepared by the DHS Intelligence Enterprise, Cyber Mission Center, and Counterintelligence Mission Center and was coordinated with the Department of Energy, Department of State, Department of the Treasury, and the FBI, among other government entities.

The report listed a number of concerns involving the use of Zoom, including that hackers "likely will identify new or use existing vulnerabilities in Zoom to compromise user devices and accounts for further exploitation of corporate networks." The report added that malicious actors could view Zoom users as targets of hacking efforts to exploit a broad range of public and private sector entities including critical infrastructure. Additionally, the report concluded that although Zoom is headquartered in the United States, the main Zoom application appears to be developed by three companies in China, employing at least 700 workers.

The report concluded that "Zoom's sudden immense growth and use across both public and private sector entities in combination with its highly publicized cybersecurity issues creates a vulnerable, target-rich environment that [Advanced Persistent Threat] actors likely see value in exploiting to achieve nation-state objectives against the Homeland, which could include disruption, espionage, or financial gain. Successful compromise of a critical infrastructure entity could inflict economic loss on at least the targeted organization, and if left undetected, preposition the cyber actors for future operations. Any organization currently using — or considering using — Zoom should evaluate the risk of its use."

An unidentified Zoom spokesperson told ABC News that the company disagreed with the government's report, saying it was "heavily misinformed, includes blatant inaccuracies about Zoom's operations, and the authors themselves admit only 'moderate confidence' in their own reporting. We are disappointed the authors did not engage with Zoom to verify the accuracy of these claims and understand the real facts about Zoom." The Zoom spokesperson stated, "We actively and quickly addressed specific security concerns as they were raised over the past few weeks."

Regarding the statements that Zoom was vulnerable to infiltration by the Chinese, the Zoom spokesperson told ABC News that Zoom's systems are "designed to maintain geofencing around China ensuring that users outside of China do not have their meeting data routed through servers in China." Additionally, the Zoom spokesperson asserted that paid Zoom customers "are now able to further customize which data center regions their account can use for real-time meeting traffic," allowing them to "opt in or out of specific data center locations." Furthermore, the Zoom spokesperson told ABC News that not only did Zoom use cloud data centers globally, the company also had 17 data centers "around the world," but only one in China. "All Zoom source code is stored and versioned in the United States," the Zoom spokesperson said.

Josh Cohen, a former DHS acting undersecretary and current ABC News contributor, noted that in general, "China, Russia and other hostile nations view the coronavirus as an opportunity to expand their intelligence-gathering efforts and they are actively targeting the private communications of those in government, the private sector, academia and others, who have increasingly turned to online communications." He added, "Private conversations using online communications and video conferencing apps are vulnerable to being intercepted by criminals and foreign intelligence operatives. Securing these platforms must be a priority especially since they are being used more frequently during the current health crisis."

Finally, several news outlets and experts have also pointed out issues with Zoom's encryption efforts. On March 31, 2020, *The Intercept* reported that although Zoom "claim[ed] to implement end-to-end encryption, widely understood as the most private form of internet communication," the company was "using its own definition of the term, one that lets Zoom itself access unencrypted video and audio from meetings."

The Intercept further alleged that Zoom "actually does not support end-to-end encryption for video and audio content, at least as the term is commonly understood. Instead it offers what is usually called transport encryption . . . which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. So when you have a Zoom meeting, the video and audio content will stay private from anyone spying on

COVID-19, *continued on page 14*

COVID-19, *continued from page 13*

your Wi-Fi, but it won't stay private from the company."

In an April 3, 2020 report, Citizen Lab, a research laboratory at the University of Toronto, examined the encryption that protected Zoom meetings, and found that Zoom "rolled" its own encryption scheme, which had significant weaknesses. The report, titled "Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings," found that although Zoom claimed that its applications used "AES-256" encryption for its meetings, the mode of encryption that was actually used was Electronic Code Book (ECB) mode, which is "not recommended because patterns present in the plaintext are preserved during encryption."

The report also found that Zoom was unclear about the encryption it offered. According to Citizen Lab, "[s]ome Zoom documentation (as well as the Zoom app itself) claims that Zoom offers a feature for "end-to-end" (E2E) encrypted meetings." However, other documentation claimed that Zoom's meeting software for Windows, MacOS, and Linux used the industry-standard TLS 1.2 scheme, whereas a September 2014 blog post by Zoom implied that TLS 1.2 was not used.

On April 1, 2020, Zoom released a blog post apologizing for the confusion surrounding its encryption practices and saying that it did, in fact, use end-to-end encryption. "Zoom has always strived to use encryption to protect content in as many scenarios as possible, and in that spirit, we used the term end-to-end encryption. While we never intended to deceive any of our customers, we recognize there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it." The blog continued, "To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt at any point before it reaches the receiving client." Citizen Lab noted, however, that the Zoom blog post did not provide further details as to how Zoom's encryption works, or clarify whether they use TLS or AES-256.

Citizen Lab also flagged a number of additional Zoom security issues, including Zoom's features designed to reduce "friction" in meetings, which then also reduce privacy and security. These features include Zoom installing a hidden web-server on Mac computers to circumvent a Safari popup that users must click through before joining a Zoom meeting; a Zoom feature that removes a password prompt during the installation process, a Zoom feature intended to allow Zoom users at the same company or ISP to find one another, and Zoom's 9 or 10 digit code, which is sufficient to join a meeting created with default settings, but can lead to Zoombombing.

Citizen Lab concluded its report by noting that Zoom lacked a transparency report requested on March 18, 2020 by Access Now, a nonprofit organization that defends the digital rights of people around the world. A July 1, 2020 post on Zoom's website stated that although the report was not yet ready, the company has "made significant progress defining the framework and approach for a transparency report that details information related to requests Zoom receives for data, records, or content." The post noted that a transparency report could be expected later in 2020.

On May 22, 2020, Zoom released a draft design of its end-to-end encryption after the company said it had consulted with civil liberties organizations, child safety advocates, encryption experts, government representatives, users, and others. However, the company came under fire in early June 2020 when several media outlets reported that the company was implementing "real end-to-end encryption" for its users, but only for those paying for a subscription.

A June 5, 2020 piece by *Forbes* magazine senior contributor Kate O'Flaherty argued that "if you delve deeper, Zoom's reasoning behind this is clearer." She continued, "First, you lose a lot of functionality if you make Zoom end-to-end encrypted. There are no more dial ins to calls, so you can't join by phone, and you also lose features like cloud recordings and streaming to YouTube. Plus, remember that Zoom's main competitors don't have end-to-end encryption: Microsoft Teams, Blue Jeans, Google Meet, Cisco Webex (although Webex has e2e for some enterprise users too)."

Nevertheless, on June 17, 2020, Zoom founder and CEO Eric Yuan announced in a blog post that the company had "released an updated [end-to-end encryption] design on GitHub. We are also pleased to share that we have identified a path forward that balances the legitimate right of all users to privacy and the safety of users on our platform. This will enable us to offer [end-to-end encryption] as an advanced add-on feature for all of our users around the globe — free and paid — while maintaining the ability to prevent and fight abuse on our platform."

In response to many of the privacy and security concerns faced by the company, Zoom announced — through an April 1, 2020 message by Zoom founder and CEO Eric Yuan, a July 2020 white paper, and an Aug. 5, 2020 letter to Zoom clients — several initiatives to better protect its users. However, some observers asserted that Zoom would need to step up its efforts to better ensure the privacy and security of its users.

Yuan wrote in an April 1, 2020 message, "[W]e recognize that we have fallen short of the community's — and our own — privacy and security expectations. For that I am deeply sorry." Yuan explained that Zoom was created for customers such as "large institutions with full IT support," including financial services companies, telecommunications providers, government agencies, universities, healthcare organizations, and telemedicine practices. According to Yuan, "exhaustive security reviews of our user, network, and data center layers" had been completed, and organizations had "confidently" selected Zoom for their use. "However," Yuan continued, "we did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home. We now have a much broader set of users who are utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived."

Yuan's message included several measures Zoom had taken to that point. The company explained to users how to address "Zoombombing," removed the Facebook SDK in their iOS client and reconfigured it to prevent it from collecting unnecessary device information from users, and updated its privacy policy to be more clear and transparent. Yuan also announced training and tutorial webinars, live daily demos, upcoming webinars, video trainings, and more. He also noted new guides for administrators on how to set up a virtual classroom, how to better secure a classroom, and revealed a dedicated K-12 privacy policy.

Yuan ended his blog post by disclosing a 90-day plan with further steps, which included shifting all of Zoom's engineering resources to focus on the most pressing trust, safety, and privacy issues; conducting a comprehensive review with third-party experts and representative users to understand and ensure the security on new consumer use cases; and conducting penetration tests to identify problems. On Sept. 11, 2020, *The Verge* reported that Zoom was making two-factor authentication available for mobile and desktop applications. Two-factor authentication requires users to confirm their identity using a second method or device.

EPIC Files Complaint against Zoom with the FTC, Follows Up With Letter; Zoom Faces Additional Lawsuits

Although concerns about Zoom's privacy and security issues were not widely known until the COVID-19 pandemic forced people to stay at home and use it, nearly a year earlier, on July 11, 2019, the Electronic Privacy Information Center (EPIC) filed a "Complaint, Request for Investigation, Injunction, and Other Relief" (complaint) against Zoom with the Federal Trade Commission (FTC). The complaint stated that Zoom had "placed at risk the privacy and security of the users of its services" and "intentionally designed their web conferencing service to bypass browser security settings and remotely enable a user's web camera without the consent of the user." As a consequence, according to the complaint, "Zoom exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks."

The complaint first asserted the "[i]mportance of [p]rivacy [p]rotection," including that the "right of privacy is a personal and fundamental right in the United States." The complaint added that the FTC, through Section 5 of the FTC Act, "has routinely investigated companies for violations of privacy when the company has engaged in '[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.'" 15 U.S.C. § 45.

Second, the complaint outlined a number of ways in which Zoom previously jeopardized users' privacy, including in October 2018 when "Tenable, a cyber exposure company, discovered a flaw in Zoom that allowed attendees and remote attackers 'to hijack control of presenters' desktops, spoof chat messages, and kick attendees out of Zoom calls,'" among other examples.

Third, the complaint cited several security vulnerabilities associated with Zoom, including that "[i]f a Zoom user does not opt-out of video, Zoom may enable the user's webcam and subject the user to remote surveillance," among multiple additional concerns.

Fourth, the complaint argued that through July 2019, Zoom had failed to address the privacy concerns highlighted by news outlets and other observers, despite significant opposition and concern from consumers to Zoom's failure to protect their privacy. The complaint contended that "[w]hen informed of the vulnerabilities Zoom did not act until the risks were made public, several months after the matter was brought to the company's attention."

Fifth, the complaint argued that Zoom had violated the FTC Act by "engaging in unfair and deceptive acts and practices." The complaint therefore asserted that the "harms of Zoom's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act, and Zoom should face FTC action for these violations." The complaint further claimed that "Zoom's actions — including its decision to install a hidden web server on users' Macs and require consumers to manually change their default camera settings — placed users at risk of severe violations of their privacy." The complaint went on to highlight several instances in which the FTC "previously barred companies from circumventing privacy settings without user consent" and "from propagating deceptive claims about privacy and security, as well as "enjoined companies from maintaining inadequate privacy policies."

Finally, the complaint asked the FTC to "investigate Zoom, enjoin its unfair and deceptive business practices, and require Zoom to protect the privacy of Zoom users."

Nearly nine months later, on April 6, 2020, EPIC sent a letter to FTC Chairman Joseph J. Simons and the other FTC commissioners, demanding that the agency open an investigation into Zoom's privacy and security practices and to issue a "Best Practices for Online Conferencing Services." The letter read, "[T]he FTC never acted on the flaws we identified with Zoom, and the problems have only become worse.. . . Each day that passes presents a new report of a previously undisclosed problem with Zoom."

EPIC's letter acknowledged that Zoom had addressed some problems, but that the company's "haphazard approach to consumer privacy does little to assure consumers that Zoom is a reliable service." Citing the number of schoolchildren needing to use Zoom for remote learning and the need for patients to seek online health advice from medical professionals, EPIC again asked the FTC to "make clear its commitment to consumer privacy precisely because we are all more dependent on online services today than we were just a few weeks ago. The [FTC] should open the investigation that EPIC proposed last summer. The [FTC] should publish Best Practices for Online Conferencing."

On May 11, 2020, Reuters reported that Simons, during a teleconference with a subcommittee of the U.S. House of Representatives Committee on Energy and Commerce, had indicated that the FTC "was looking at" the privacy complaints regarding Zoom. "We are very happy to take complaints from any source," he said. "If you're reading about it (an issue) in the press, in the media, then you can be assured that we're looking at it already or we will because of the media attention. If it's out there in the media, we're on it." As of October 2020, the FTC had not announced any actions regarding Zoom.

In addition to the lawsuit filed by EPIC, beginning in March 2020, Zoom faced at least four class action lawsuits filed in federal court regarding various privacy and security issues. The lawsuits included:

- *Cullen v. Zoom Video Communications, Inc.*, No. 5:20-cv-02155-SVK (N.D. Cal. filed March 30, 2020), available online at: https://www.courtlistener.com/recap/gov.uscourts.cand.357336/gov.uscourts.cand.357336.1.0.pdf
- *In Re: Zoom Video Communications, Inc.*, No. 5:20-CV-02155-LHK (N.D. Cal. filed July 30, 2020), available online at: https://www.courtlistener.com/recap/gov.uscourts.cand.357336/gov.uscourts.cand.357336.114.0.pdf
- *Taylor v. Zoom Video Communications, Inc.*, No. 3:20-

COVID-19, *continued on page 16*

COVID-19, *continued from page 15*

cv-02170 (N.D. Cal. filed March 31, 2020), available online at: https://www.dropbox.com/s/h078rfxsq4x22um/TZ_TaylorVZoom_Complaint_Final.pdf?dl=0

• *Ohlweiler v. Zoom Video Communications, Inc.*, No. 2:20-cv-03165-SVW-JEM (C.D. Cal. April 3, 2020), available online at: https://www.courtlistener.com/recap/gov.uscourts.cacd.778595/gov.uscourts.cacd.778595.1.0.pdf.

• *Hurvitz v. Zoom Video Communications, Inc.*, No. 2:20-cv-3400 (N.D. Cal. filed April 13, 2020), available online at: https://www.law360.com/articles/1263127/attachments/0.

Additionally, on Aug. 10, 2020, Consumer Watchdog, a Washington, D.C. non-profit which says it is dedicated to protecting consumers' online privacy and security, filed a lawsuit in the Superior Court for the District of Columbia Civil Division against Zoom, alleging that the company made "false and deceptive representations to consumers about its data security practices in violation of the District of Columbia Consumer Protection Procedures Act (CPPA)," D.C. Code § 28-3901, *et seq.* (2019). *Consumer Watchdog v. Zoom Video Communications, Inc.*, No. 2020 CA 003516 (filed Aug. 10, 2020). The lawsuit is available online at: https://www.consumerwatchdog.org/sites/default/files/2020-08/Zoom%20Complaint.pdf. (For more about *Cullen v. Zoom Video Communications, Inc.* and *Hurvitz v. Zoom Video Communications, Inc.* cases, as well as the CCPA, see "California Consumer Protection Act Takes Effect" on page 23 of this issue of the Silha *Bulletin*.)

COVID-19 Pandemic Prompts Questions and Concerns About Government Entities and Private Companies Tracking Individuals' Locations

In spring and summer 2020, government entities and private companies in the United States and abroad began tracking individuals' locations through their smartphones and electronic devices to help address and combat the spread of the COVID-19 pandemic through contact tracing and geo-tracking. Such moves prompted concern from observers regarding the privacy implications of surveilling members of the public, as well as the potential ineffectiveness of location tracking efforts to combat the coronavirus.

Human Rights Watch defines "mobile location data" as "geolocation and proximity information from mobile phones and other devices." Mobile location data can be obtained by government and private entities from a variety of sources, including cell site location information (CSLI), Global Positioning System (GPS) signals, and Bluetooth beacons.

Human Rights Watch explained on May 13, 2020 that "[g]overnments view mobile location data as a key component of measures to contain the spread of Covid-19. They are presenting individualized tracking as a reliable way to track the movement of people who are infected and identify individuals with whom they came into contact during the period in which they are contagious. Individualized tracking can also be used to ascertain whether people are complying with social distancing and quarantine measures." The advocacy organization added, "Analysis of aggregate location data, on the other hand, might provide insight into the effectiveness of social distancing measures, model the potential for transmission, and identify potential 'hot spots' of transmission."

According to Human Rights Watch, mobile location data can be used for "contact tracing," which is "the process of identifying individuals who may have come into contact with an infected person. Its goal is to interrupt transmission by rapidly identifying individuals who have been in close contact of someone who is infected, defined by the United States Centers for Disease Control and Prevention (CDC) as within 6 feet of someone for approximately 10 or more minutes." Mobile location data can also be used to "[e]nforc[e] quarantine and social distancing orders," "[b]ig data analytics," and "[h]ot spot mapping."

On March 28, 2020, *The Wall Street Journal* reported that "[g]overnment officials across the U.S. are using location data from millions of cellphones in a bid to better understand the movements of Americans during the coronavirus pandemic and how they may be affecting the spread of the disease." More specifically, the report explained that the "federal government, through the [CDC], and state and local governments . . . started to receive analyses about the presence and movement of people in certain areas of geographic interest drawn from cellphone data.. . . The data comes from the mobile advertising industry rather than cellphone carriers."

According to *The Wall Street Journal*, the goal was to create a "portal" through which federal, state, and local government bodies and officials could track geolocation data across as many as 500 cities across the United States. In doing so, government officials could "learn how coronavirus is spreading around the country and help blunt its advance."

Private companies also took efforts in spring 2020 to increase tracking of individuals' locations to address the spread of the coronavirus and the COVID-19 pandemic. For example, on April 3, Google announced that it would begin publishing COVID-19 Community Mobility Reports, which would "use aggregated, anonymized data to chart movement trends over time by geography, across different high-level categories of places such as retail and recreation, groceries and pharmacies, parks, transit stations, workplaces, and residential."

The blog post explained that the company "use[s] aggregated, anonymized data showing how busy certain types of places are — helping identify when a local business tends to be the most crowded. We have heard from public health officials that this same type of aggregated, anonymized data could be helpful as they make critical decisions to combat COVID-19." The post added, "We will release these reports globally, initially covering 131 countries and regions. Given the urgent need for this information, where possible we will also provide insights at the regional level. In the coming weeks, we will work to add additional countries and regions to ensure these reports remain helpful to public health officials across the globe looking to protect people from the spread of COVID-19."

Since March 2020, several public and private entities, including the Massachusetts Institute of Technology (MIT), developed mobile phone apps used to track and trace who was tested for and/or diagnosed with COVID-19. For example, on April 11, 2020, *The New York Times* reported that Apple and Google were building software into smartphones that would enable them "to constantly log other devices they get close to through the short-range

wireless technology Bluetooth, enabling what is known as 'contact tracing' of the disease."

The *Times* noted that the rare partnership "could prove to be significant in slowing the spread of the coronavirus. Public-health authorities have said that improved tracking of infected people and their contacts could slow the pandemic, and such measures have been effective in places like South Korea that also conducted mass virus testing." On May 20, Alabama, North Dakota, and South Carolina became the first states to use the new tracing technology. *The Washington Post* reported on Aug. 17, 2020 that there were initiatives in 20 states and territories to adopt or otherwise use the Apple-Google technology.

In an April 16, 2020 blog post, the American Civil Liberties Union (ACLU) praised Apple's and Google's efforts as protecting privacy to a great extent. The post read, "To their credit, Apple and Google have announced an approach that appears to mitigate the worst privacy and centralization risks, but there is still room for improvement. We will remain vigilant moving forward to make sure any contact tracing app remains voluntary and decentralized, and used only for public health purposes and only for the duration of this pandemic." The *Post* noted that many of the tracking apps similarly "work by using Bluetooth technology to detect when a user has prolonged and close contact, typically at least 15 minutes and within about six feet, with another person who also is using such an app."

However, some observers pointed out that the use of individuals' smartphones and other electronic devices to track their location raises significant data privacy concerns. In an interview with *The New York Times*, Mike Reid, an assistant professor of medicine and infectious diseases at the University of California, San Francisco, said the software installed by Apple and Google "could be a useful tool, but it raises privacy issues." He added, "It's not going to be the sole solution, but as part of a robust sophisticated response, it has a role to play."

Human Rights Watch contended on May 13, 2020 that the "privacy risks of mobile location tracking are significant and well-established. Mobile location information can contain sensitive and revealing insights about a person's identity, location, behavior, associations, and activities. The use of mobile phone network data creates granular, real-time targeting opportunities, which can be used by governments to forcefully enforce quarantine, discriminate, or crackdown on populations for other reasons. And in the hands of abusive governments that already have adopted intrusive surveillance practices, this can serve to enhance repression."

The article continued, "The mobile phone tracking programs described above raise concern that governments are collecting, using, and retaining data beyond what is necessary for legitimate and targeted disease surveillance measures. The lack of transparency regarding many Covid-19 tracking initiatives . . . prevents the public from assessing whether there are meaningful limits on the types of personal information that will be collected, used, aggregated, and retained, or whether tracking and data collection will end once the pandemic is contained."

> "Because this is a free country where people have the right to make decisions like this, there is a real problem with trying to set up this kind of electronic system because it is going to require a buy-in from the American public. You're going to have to agree with it."
>
> **— Jane Kirtley,**
> **Silha Center Director and**
> **Silha Professor of Media Ethics and Law**

In a June 17, 2020 interview with WGN Radio, University of Minnesota Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley similarly argued that "there is a lot of concern for people, and I think rightfully so, about who will collect [mobile location and geo-tracking] data, where it will be collected, how long it will be kept, all of the classic questions that are raised in the context of data privacy, but [are] brought to the [forefront] here because people are so understandably anxious about what's going to happen with this data, could it be used against them, for example.. . . The question is whether you are comfortable . . . not knowing how they're using it not only for their own internal purposes, but for marketing purposes and passing it on to other people, maybe even the government."

Kirtley also noted that government entities and private companies using "geo-tracking" technology to determine the level of social distancing in American cities face a significant hurdle in the United States. "Because this is a free country where people have the right to make decisions like this, there is a real problem with trying to set up this kind of electronic system because it is going to require buy-in from the American public. You're going to have to agree with it.. . . Experts on this technological side of it say that if they don't get at least 60 percent buy-in on this then it's not going to work. So that is the first hurdle."

— Scott Memmel
Postdoctoral Associate
— Elaine Hargrove
Silha Center Staff

Federal Judge Finds Most of North Carolina's Ag-Gag Law Unconstitutional

On June 12, 2020, Judge Thomas D. Schroeder of the U.S. District Court for the Middle District of North Carolina ruled that several provisions of North Carolina's ag-gag law were unconstitutional under the First Amendment. *People for the Ethical Treatment of Animals, Inc. v. Stein*, No. 1:16CV25, 2020 WL 3130158 (M.D.N.C. 2020). Previously, Schroeder had held that the plaintiffs in the case, which included People for the Ethical Treatment of Animals (PETA) and the Animal Legal Defense Fund (ALDF), among other animal-rights organizations, did not have standing to bring the case, though his ruling was reversed and remanded by the U.S. Court of Appeals for the Fourth Circuit.

AG-GAG LAWS

Ag-gag laws vary from state-to-state, but generally criminalize or hold civilly liable individuals or groups who uncover or expose cases of animal abuse or food safety violations at agricultural facilities. Such statutes often prohibit the unauthorized recording of videos of agricultural operations and facilities. These laws raise First Amendment concerns from advocacy groups, as well as media organizations, who argue that such laws chill protected First Amendment activity, namely undercover investigations seeking to expose unsafe conditions or illegal practices. Ag-gag laws can also take the form of agriculture disparagement laws, which establish a cause of action for damages arising from negative statements or dissemination of false information about the safety of food products.

Since 2017, several federal courts have ruled in favor of animal rights and food activist groups in their lawsuits targeting ag-gag laws, including those in Iowa, Wyoming, North Carolina, Idaho, and Utah. (For more information on the conflict between journalism and ag-gag laws, as well as the federal court rulings, see "Federal Courts Rule Iowa and Kansas "Ag-Gag" Laws Violated First Amendment, Dismiss Lawsuit Challenging Arkansas' Statute" in the Winter/Spring 2020 issue of the Silha *Bulletin*, "Federal Judge Strikes Down Iowa's 'Ag-Gag' Law; Coalition of Animal Rights Groups Challenges Nation's Oldest 'Ag-Gag' Law" in the Winter/Spring 2019 issue, "Fourth Circuit Allows Lawsuit Targeting North Carolina Ag-Gag Law to Continue; District Court Rules Wyoming Law Unconstitutional" in the Fall 2018 issue, "Minneapolis Legislature Introduces an 'Ag-Gag' Law; Federal Appeals Courts Strike Down Two States' Laws" in the Winter/Spring 2018 issue, *Journalists Face Evolving, Uncertain Legal Landscape* in "'Drone Journalism' Presents Possibilities But Faces Legal Obstacles" in the Fall 2014 issue, and "States Consider Banning Undercover Recording at Agricultural Operations" in the Summer 2011 issue.)

The case regarding the North Carolina ag-gag law arose shortly after the law was passed in 2016 when PETA and the ALDF, among other animal-rights organizations, filed a lawsuit against North Carolina Attorney General Joshua Stein and University of North Carolina, Chapel Hill (UNC) Chancellor Carol L. Folt, alleging that the statute "interfere[d] with their plans to conduct undercover investigations of government facilities in North Carolina for the purpose of gathering evidence of unethical and illegal animal practices and to disseminate this information to the public, in violation of the First and Fourteenth Amendments."

The North Carolina Property Protection Act, N.C. Gen. Stat. § 99A-2 (2016), provides that "[a]ny person who intentionally gains access to the nonpublic areas of another's premises and engages in an act that exceeds the person's authority to enter those areas is liable to the owner or operator of the premises for any damages sustained." "Non-public" areas are defined as "those areas not accessible to or not intended to be accessed by the general public."

The statute provides several scenarios where this may occur, including an individual "[k]nowingly or intentionally placing on the employer's premises an unattended camera or electronic surveillance device and using that device to record images or data." The Act provides for equitable relief, as well as the recovery of compensatory damages, costs and attorneys' fees, and exemplary damages in the amount of $5,000 for each day that the person has acted in violation of the statute.

On May 2, 2017, Judge Schroeder ruled against the organizations. *People for the Ethical Treatment of Animals v. Stein*, 259 F.Supp.3d 369 (M.D.N.C. 2017). He found that they could not show an "injury-in-fact" and, therefore, did not have Article III standing under the U.S. Constitution to bring the case. Schroeder wrote that the lawsuit "contain[ed] not a single allegation" that the defendants, which included the state and the University of North Carolina, "had ever sued or threatened to sue PETA or [the] ALDF for investigatory conduct."

On June 5, 2018, the Fourth Circuit reversed the district court's dismissal of the lawsuit, finding that the animal-rights groups had alleged a plausible "injury-in-fact," namely that they could not conduct undercover investigations of public and private facilities in North Carolina for alleged animal cruelty, causing a "chilling effect" and "self-censorship." *People for the Ethical Treatment of Animals v. Stein*, 737 Fed.Appx. 122 (4th Cir. 2018). The Fourth Circuit remanded the case to the Middle District of North Carolina, after which the North Carolina Farm Bureau Federation, Inc. moved to intervene in the case, which was unopposed.

(For more information on North Carolina's ag-gag law, as well as the district court and Fourth Circuit rulings, see *Federal Appellate Court Allows Lawsuit to Continue Against North Carolina Ag-Gag Law* in "Fourth Circuit Allows Lawsuit Targeting North Carolina Ag-Gag Law to Continue; District Court Rules Wyoming Law Unconstitutional" in the Fall 2018 issue of the Silha *Bulletin*.)

On June 22, 2020, Judge Schroeder held that North Carolina's ag-gag law violated the First Amendment, finding that two provisions were facially unconstitutional, while two other provisions were unconstitutional as applied. Schroeder first held that the plaintiffs had established Article III standing in the case, reasoning that they had plausibly argued an "injury-in-fact" that was "a concrete and particularized invasion of a legally protected interest," citing the U.S. Supreme Court's 2016 opinion in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). (For more information on *Spokeo, Inc. v. Robins*, see "Ninth Circuit Addresses *Spokeo* after Supreme Court Remands

Case; Circuit Court Splits on Article III Standing Bar Following *Spokeo*" in the Summer 2017 issue of the Silha *Bulletin*, "Supreme Court Issues Long-Awaited *Spokeo* Ruling" in the Summer 2016 issue, and "U.S. Supreme Court Accepts Review of *Robins v. Spokeo, Inc.*" in the Summer 2015 issue.)

Schroeder found that the animal-rights groups had established that they "engaged in or supported undercover investigations in the past for the purpose of gathering and disseminating information or have relied on undercover investigations to disseminate information," and also that they "refrained from doing so out of fear of [civil] liability" under the ag-gag law. He added that the plaintiffs had also "set forth sufficient facts to establish both causation and redressability and consequently have standing."

Second, Schroeder turned to the plaintiff's motion for summary judgment arguing that subsections (b)(1), (b)(2), (b)(3) and (b)(5) of the ag-gag law violated the First Amendment "because they fail the requisite scrutiny and are unconstitutionally overbroad." He held that although North Carolina's law differed from others that had been struck down in that it imposed civil rather than criminal penalties, it still represented government restriction of speech, therefore constituting "state action." He reasoned that North Carolina, in passing the law, "identified speech (or in some cases, conduct which can include speech) it wishe[d] to allow to be proscribed and . . . empowered private parties to enforce the prohibition," citing *Cohen v. Cowles Media Co.*, 501 U.S. 663, 668 (1991).

Schroeder then held that the prohibition on undercover recording restricted speech, rather than only conduct. He rejected the defendants' argument that "image capture and recording following a trespass under the Act [are] unprotected speech." He reasoned that although "free speech cannot be used to justify violation of laws of general application that operate independent of speech, such as trespass," citing *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 521 (4th Cir. 1999), it does not mean that "that category of speech is unprotected."

Next, Schroeder determined that subsections (b)(2) and (b)(3), which prohibited the recording of images in the agriculture facilities, were subject to strict scrutiny review, meaning the court must determine whether there was a compelling government interest in restricting speech and whether the restrictions were narrowly tailored to achieve that interest.

Conversely, he held that the First Amendment challenge to subsection (b)(1) could only be brought as an applied challenge. Schroeder found that although the prohibition on "capturing" the owner of the facility's information and data constituted a prohibition on protected speech, he could "ignore the possible myriad legitimate applications of subsection (b)(1)." Schroeder reached a similar conclusion regarding subsection (b)(5), which "creates liability for acts that 'substantially interfere[] with the ownership or possession of real property.'" He reasoned that "[a]ll sorts of non-speech acts" could be proscribed by that provision and that the plaintiffs had failed "to show that subsection (b)(5) lacks any plainly legitimate sweep." Schroeder therefore concluded that these subsections were subject to intermediate scrutiny, a lower standard than strict scrutiny requiring that government prove that the law is "narrowly tailored to serve a significant government interest and leave[s] open ample alternative channels of communication."

Schroeder ruled that because the defendants "failed to defend the Act on strict scrutiny grounds" and did not "put forward any compelling interest," they had "failed to carry their burden as to subsections (b)(1) and (b)(2)." He further held that "even under intermediate scrutiny each of the challenged provisions fails." Schroeder reasoned that North Carolina's existing trespass law, among other statutes, provided alternative means to target those trespassing into agricultural facilities without implicating speech. As a result, Schroeder held that although the defendants had "identified a legitimate governmental interest in protecting private property, they have failed to demonstrate through evidence that the Property Protection Act is narrowly tailored to further that interest or that existing laws, such as trespass, are insufficient to address the problem."

Fourth, Schroeder turned to the plaintiffs' arguments that subsections (b)(1) and (b)(5) were unconstitutionally overbroad and unconstitutionally vague. Regarding the former, Schroeder held that "[c]onsidering the plainly legitimate sweep of subsections (b)(1) and (b)(5), and given where the statute does not reach, the court finds that the Act does not cover a substantial amount of protected activity to render it overbroad." Regarding vagueness, he held that the provisions were "not impermissibly vague as a facial matter, and Plaintiffs' motion for summary judgment will be denied."

Finally, Schroeder ruled that "subsections (b)(1) and (b)(5) of the Act are unconstitutional as-applied and subsections (b)(2) and (b)(3) are unconstitutional both facially and as-applied." He therefore ordered that the defendants, "as well as their officers, agents, employees, attorneys, and all other persons in active concert or participation with them, are therefore permanently enjoined from attempting to enforce subsections (b)(1) and (b)(5) against Plaintiffs in their stated exercise of speech." He further ordered that "[s]ubsections (b)(2) and (b)(3) are therefore struck down as unconstitutional. Defendants, as well as their officers, agents, employees, attorneys, and all other persons in active concert or participation with them, are permanently enjoined from attempting to enforce subsections (b)(2) and (b)(3) against Plaintiffs." The full ruling is available online at: https://www.rcfp.org/wp-content/uploads/2020/06/2020.06.12-PETA-v.-Stein-ag-gag-ruling.pdf.

In a statement following the ruling, North Carolina Rep. John Szoka (R-Cumberland), the ag-gag law's primary sponsor, said he was disappointed in the ruling. "I did everything I could to make sure that no one's First Amendment rights were being restricted," he said.

David Muraskin, an attorney with Public Justice, a nonprofit law firm representing the plaintiffs, called the ruling a "complete win" in a statement. "Essentially . . . anyone who wants to engage in an undercover investigation of a facility should not fear [this law]," he said. "To the extent the function of your activity is speech, rather than stealing . . . you should be protected by the First Amendment." He added, "I think this [ruling] should alleviate a lot of fear for people who want to come forward."

— Scott Memmel
Postdoctoral Associate

D.C. Circuit Affirms Ruling Requiring White House to Return White House Reporter's Press Credential

On June 5, 2020, the U.S. Court of Appeals for the D.C. Circuit ruled in favor of *Playboy* magazine senior White House reporter and CNN political analyst Brian Karem in his lawsuit against President Donald Trump's administration, which stemmed from the White House's August 2019 suspension of Karem's hard pass — a physical press credential granting him access to the White House. The D.C. Circuit unanimously held that Karem was "likely to succeed on his [Fifth Amendment] due process claim because, on this record, he lacked fair notice that the White House might punish his purportedly unprofessional conduct by suspending his hard pass," affirming a September 2019 preliminary injunction issued by Judge Rudolph Contreras of the U.S. District Court for the District of Columbia.

FIRST AMENDMENT

The case arose in August 2019 when the White House suspended Karem's press pass for 30 days. The White House cited Karem's July 11, 2019 confrontation with conservative radio host Sebastian Gorka. While waiting for a presidential press conference in the Rose Garden, Karem called the attendees of the preceding social media summit, which observers contended was largely meant for President Donald Trump's supporters, "a group of people eager for demonic possession." Karem and Gorka then shouted at each other, including Gorka yelling "You're a punk, you're not a journalist, you're a punk."

In an Aug. 2, 2019 tweet, *Playboy* wrote that Gibson, Dunn & Crutcher LLP attorney Theodore J. Boutrous would represent Karem and appeal the White House's decision. (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*. For more information on the background of Karem's case, see "White House Revokes and Suspends Hard Press Passes Under New Rules" in the Summer 2019 issue of the Silha *Bulletin*.)

On Aug. 20, 2019, Karem filed a lawsuit against President Trump and then-White House Press Secretary Stephanie Grisham, requesting that the federal District Court for the District of Columbia "vacate the suspension and order that Karem's hard pass be immediately restored." The complaint argued that the suspension violated Karem's Fifth Amendment rights, citing *Sherrill v. Knight*, 569 F.2d 124 (D.C. Cir. 1977), in which the D.C. Circuit "made very clear . . . [that] the White House may deny, revoke or suspend a press pass based only on 'explicit and meaningful standards' that have been 'publish[ed]' so as to afford fair notice to reporters, and to avoid arbitrary or discriminatory punishments."

> "Karem is likely to succeed on his due process claim because, on this record, he lacked fair notice that the White House might punish his purportedly unprofessional conduct by suspending his hard pass for a month."
>
> **— D.C. Circuit Judge David S. Tatel**

The complaint also argued that that the suspension violated the First Amendment, including because the suspension was "clearly meant to punish and deter his reporting on the Administration rather than based on anything he said in the Rose Garden in July." The complaint therefore argued that the suspension was "an impermissible content-based regulation of speech, and an attempt to censor the press and exclude from the White House reporters who challenge and dispute the President's point of view."

On Sept. 3, 2019, Judge Contreras granted the motion for a temporary restraining order and preliminary injunction brought by Karem, ordering the Trump administration to restore the reporter's hard pass. *Karem v. Trump*, 404 F.Supp.3d 203 (D.D.C. 2019). Contreras held that Karem had, "at this early stage of the proceedings, shown that he is likely to succeed on this due process claim, because the present record indicates that Grisham failed to provide fair notice of the fact that a hard pass could be suspended under these circumstances."

Contreras also held that Karem had adequately demonstrated that "even the temporary suspension of his pass inflict[ed] irreparable harm on his First Amendment rights." He reasoned that Karem's "First Amendment interest depends on his ability to freely pursue 'journalistically productive conversations' with White House officials." Contreras therefore held that "the only way to remedy the injury is to return the hard pass and the access that comes with it. Under those circumstances, Karem's First Amendment injury undoubtedly constitutes a concrete, unrecoverable harm sufficient to warrant preliminary relief."

(For more information on Karem's lawsuit and Contreras' ruling, see "Federal Judge Orders White House to Reinstate Reporter's Press Credential" in the Fall 2019 issue of the Silha *Bulletin*.)

On June 5, 2020, the D.C. Circuit affirmed Contreras' ruling, holding that "Karem is likely to succeed on his due process claim because, on this record, he lacked fair notice that the White House might punish his purportedly unprofessional conduct by suspending his hard pass for a month." Judge David S. Tatel wrote for the unanimous three-judge panel and first cited *Sherill*, including the D.C. Circuit's finding that "the protection afforded newsgathering under the [F]irst [A]mendment . . . requires that [access to White House press facilities] not be denied arbitrarily or for less than compelling reasons." Tatel wrote that "[f]orty years on, today's hard-pass system is little changed from the one described in Sherrill."

Second, Tatel cited the White House's previous attempt to revoke CNN reporter Jim Acosta's credential in November 2018, which led to a similar ruling by the District Court for the District of Columbia. That case arose on Nov. 7, 2018, when President Trump

called Acosta "a rude, terrible person" after he asked the president repeated questions during a press conference following the 2018 midterm elections. Boutrous filed a lawsuit on behalf of CNN and Acosta in November 2018 against President Trump and several members of his administration, arguing that Acosta's First and Fifth Amendment rights had been violated, and that President Trump's administration failed to follow the proper protocols, therefore violating the Administrative Procedure Act, 5 U.S.C. § 706.

On Nov. 16, 2018, Judge Timothy J. Kelly held that the White House was wrong to revoke Acosta's credentials, ordering the Trump administration to immediately return them. *Cable News Network, Inc. v. Trump*, No. 18 Civ. 2610 (D.D.C. 2018). Although Kelly did not rule on the underlying case regarding the First and Fifth Amendments, he found that the White House did not provide Acosta with the due process required to legally revoke his press pass, therefore causing Acosta "irreparable harm."

On Nov. 19, 2018, the White House restored Acosta's credential, but also sent a letter (the Acosta Letter) to the White House press corps detailing new rules at presidential press conferences, which included: "(1) a journalist called upon to ask a question will ask a single question and then will yield the floor to other journalists; (2) At the discretion of the President or other White House official . . . a follow-up question or questions may be permitted . . . (3) 'Yielding the floor' includes, when applicable, physically surrendering the microphone to White House staff for use by the next questioner." Failure to abide by these rules could "result in suspension or revocation of the journalist's hard pass." (For more information on the White House's attempt to revoke Acosta's hard pass, the ensuing legal battle, and the new rules for presidential press conferences, see *President Trump Calls CNN Reporter "Rude, Terrible Person," Revokes His Press Credentials; Federal Judge Requires Trump Administration Reinstate Credentials* in "President Trump Continues Anti-Press Rhetoric and Actions" in the Fall 2018 issue of the Silha *Bulletin*.)

Third, Tatel turned to Karem's due process claim and cited the U.S. Supreme Court's finding in *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012) that "[a] fundamental principle in our legal system . . . is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." He found that this "'essential . . . protection[]' of fair notice applies here."

Tatel held that "Karem's due process claim is likely to succeed because, on this record, nothing put him on notice of 'the magnitude of the sanction' — a month-long loss of his White House access, an eon in today's news business — that the White House 'might impose' for his purportedly unprofessional conduct at the non-press-conference event." He cited "the lack of formally articulated standards and sanctions" by the White House, including in the Acosta Letter. Tatel added that even if the White House had articulated such standards in the Acosta Letter, previous examples of "journalistic misbehavior . . . elicited no punishment at all, let alone a month's exile."

Tatel rejected several of the White House's arguments, including the claim that "'basic standards of professionalism' should have put Karem on notice that "breaches of [such] standards . . . can carry consequences stricter than an admonition not to engage in that behavior again." Tatel contended that the White House could not "rely on unarticulated standards of professionalism or 'the adage that some things go without saying' to justify the thirty-day suspension for the conduct at issue here."

Tatel also noted that the White House, "raising the specter of the absurd, . . . argue[d] that it cannot be the case that 'the Press Secretary would be powerless to take action even were a reporter to 'moon' the President, shout racial epithets at a foreign dignitary, or sexually harass another member of the press corps.'" Tatel held that the White House could not defend the suspension of Karem's hard pass "on the ground that some other, egregious conduct might justify the same sanction." He added, "And even if the White House could impose that sanction for such egregious conduct consistent with due process, Karem's behavior as reflected in the preliminary injunction record fell below that threshold. Notions of professionalism are, after all, context-dependent."

Fourth, Tatel held that Karem stood "to suffer immediate irreparable harm absent an injunction." He cited *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013), in which the D.C. Circuit concluded that "a prospective violation of a constitutional right constitutes irreparable injury for . . . purposes [of] . . . seeking equitable relief."

Finally, Tatel affirmed the district court's preliminary injunction, but clarified one aspect of its scope, holding that the injunction did not run to President Trump, but instead "only to the Press Secretary." He cited the defendants' uncontested argument that "[t]he President is not a proper defendant in this case and . . . no temporary injunctive relief can issue against him." The full ruling is available online at: https://www.cadc.uscourts.gov/internet/opinions.nsf/BC95D-2B55151A3A18525857E00506384/$-file/19-5255-1845846.pdf.

In a June 5 statement following the ruling, White House Correspondents' Association (WHCA) president Jonathan Karl praised the decision, writing, "Today the DC Circuit affirmed what we all know — the work of journalists reporting from the White House is essential to our republic. The WHCA stands ready to fend off efforts by any administration to constrain the rights of journalists or to threaten our ability to . . . exercise our First Amendment rights."

In a June 5 tweet, the Reporters Committee for Freedom of the Press (RCFP) wrote that the D.C. Circuit's ruling "upholds the rights of press covering the White House."

— Scott Memmel
Postdoctoral Associate

President Trump's Campaign Demands CNN Retract And Apologize for Poll, But Network Declines

On June 10, 2020, CNN reported that Donald J. Trump for President, President Donald Trump's re-election campaign, sent a cease-and-desist letter to CNN President Jeff Zucker demanding that CNN retract and apologize for a poll revealing that Trump was "well behind" then-presumptive Democratic presidential nominee and former Vice President Joe Biden. The same day, CNN Executive Vice President and General Counsel David Vigilante criticized the demands, calling them "factually and legally baseless."

PRIOR RESTRAINT

On June 8, 2020, CNN published a poll under the headline "CNN Poll: Trump losing ground to Biden amid chaotic week." The poll, which was conducted by SSRS, an independent research company, sampled 1,259 respondents between June 2 and June 5, including "an oversample of 250 black, non-Hispanic respondents." The poll found that President Trump trailed Biden by 14 points, 55%-41%, among registered voters. It also found that President's approval rating had fallen to 38%, the lowest rating since January 2019, according to CNN. The full poll results are available online at: http://cdn.cnn.com/cnn/2020/images/06/08/rel6a.-.race.and.2020.pdf. CNN's story about the poll is available online at: https://www.cnn.com/2020/06/08/politics/cnn-poll-trump-biden-chaotic-week/index.html.

The cease-and-desist letter sent by President Trump's campaign was dated June 9, 2020 and first contended that the "upcoming November 3, 2020 election is a ripe target for peddlers of misinformation and false manipulated content, including media polls." The letter argued that CNN's poll was "designed to mislead American voters through a biased questionnaire and skewed sampling." The letter cited an investigation by McLaughlin & Associates, a polling firm selected by President Trump's campaign, according to *The Hill* on Oct. 12, 2019. According to the letter, the investigation found that the poll was "only 23% Republican" and targeted adults, rather than likely voters.

The letter further criticized the poll and argued that CNN pollsters would continue to "manipulate polling data." The letter added that the poll was "intentionally false, defamatory, and misleading, and designed to harm [President Trump's campaign]." The letter therefore requested that CNN retract the poll and publish a "full, fair, and conspicuous retraction, apology, and clarification to correct its misleading conclusions." The full letter is available online at: https://twitter.com/tedstew/status/1270789222849548288/photo/1.

On June 10, Vigilante sent a letter responding to President Trump's campaign, including Senior Legal Adviser Jenna Ellis. Vigilante began the response by writing, "To my knowledge, this is the first time in its 40-year history that CNN had been threatened with legal action because an American politician or campaign did not like CNN's polling results." The response continued, "To the extent we have received legal threats from political leaders in the past, they have typically come from countries like Venezuela or other regimes where there is little or no respect for a free and independent media."

The response also discussed the reputation of McLaughlin & Associates, noting that the firm had a "C/D rating" from FiveThirtyEight, a website focused on opinion polling and analysis. The response added that the firm was able to evaluate and criticize CNN's poll because the network "is transparent and publishes its methodology along with its polling results." The response continued, "Because of this, McLaughlin was free to publish his own critique of CNN's analysis and share his criticisms across the U.S. media landscape. That's how free speech works. It's the American way."

The response concluded by stating, "Your letter is factually and legally baseless. It is yet another bad faith attempt by the campaign to threaten litigation and muzzle speech it does not want voters to read or hear. Your allegations and demands are rejected in their entirety." The full response is available online at: https://www.cnn.com/2020/06/10/politics/cnn-letter-to-trump-over-poll/index.html.

As the *Bulletin* went to press, President Trump's campaign had not taken any further action regarding the CNN poll.

Previously, on Oct. 18, 2019, attorney Charles Harder sent a letter on behalf of President Trump to Zucker and Vigilante accusing CNN of violating the Lanham Act of 1946, 15 U.S.C. § 1051 *et seq.*, a federal statute that governs trademarks and also includes provisions against false advertising. The letter contended that CNN Broadcasting, Inc., CNN Productions, Inc., and CNN Interactive, Inc. violated the statute by misrepresenting President Trump, and threatened legal action unless CNN agreed to an "appropriate resolution of the matter." Several observers criticized the letter, contending that such a lawsuit would face a significant First Amendment defense and was unlikely to succeed. For example, in an Oct. 18, 2019 tweet, Gibson, Dunn & Crutcher LLP attorney Theodore J. Boutrous called the letter "absolutely ridiculous," adding that "[n]o serious lawyer would ever think of sending such a frivolous letter making such a baseless threat." (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*. For more information on the letter and resulting criticism by observers, see "Letter Sent on Behalf of President Trump Threatens Legal Action Against CNN, Prompting Criticism" in the Fall 2019 issue of the Silha *Bulletin*.)

Harder, of Harder LLP, is best known for his successful lawsuit against media gossip website *Gawker* on behalf of former professional wrestler Hulk Hogan, as well as his more recent legal attacks on technology news website *TechDirt* and women's website *Jezebel*. (For more information on Harder and his lawsuits against media outlets, see *Book About the Trump Administration's White House Raises Ethical and Legal Questions* in "The Ethics of Covering President Donald Trump" in the Winter/Spring 2018 issue of the Silha *Bulletin*, "Attorney Charles Harder Continues Attacks on News Websites by Filing Defamation Suits" in the Fall 2017 issue, "*Gawker* Shuts Down After Losing Its Initial Appeal of $140 Million Judgment in Privacy Case" in the Summer 2016 issue, and "*Gawker* Faces $140 Million Judgment after Losing Privacy Case to Hulk Hogan" in the Winter/Spring 2016 issue.)

— Scott Memmel
Postdoctoral Associate

California Consumer Protection Act Takes Effect

PRIVACY

The California Consumer Protection Act (CCPA), which officially took effect on Jan. 1, 2020, continued to be a moving target for privacy regulation. After several draft regulations and comment periods, on June, 2, 2020, California Attorney General Xavier Becerra submitted final regulations to the California Office of Administrative Law (OAL) for approval as well as a final "statement of reasons" to clarify the requirements and enforcement of the CCPA. The final regulations were approved by the OAL on Aug. 14, 2020. Despite calls from businesses to delay enforcement because of business disruptions caused by the COVID-19 pandemic, as well as the delayed final regulations, the California Attorney General began enforcing the act on July 1, 2020. Meanwhile, several lawsuits have been brought under the CCPA that raise noteworthy questions about the scope of the CCPA's private right of action. Each event is discussed in more detail below after a broad overview of the CCPA.

Passed in 2018, the statute is the first law in the United States to establish a comprehensive set of rules around consumer data. The statute applies to any business that operates in California and either makes at least $25 million in annual revenue, gathers data on more than 50,000 users, or makes more than half its money from user data. For California residents, the statute grants more control over how covered businesses use their personal information. The law allows California residents to demand that businesses disclose any personal information they have collected, delete that information if asked, and refrain from selling or transferring it to third parties.

Businesses in violation of the CCPA face both private rights of action and investigation by the California Attorney General's Office. California consumers can bring private actions against businesses for failure to maintain reasonable security procedures that result in "unauthorized access and exfiltration, theft, or disclosure" of their nonencrypted and nonredacted personal information. For private rights of action, statutory damages will amount to the greater of actual damages, or between $100 and $750 per consumer, per incident. Additionally, following July 1, 2020, the California Attorney General began sending notifications of alleged violation to non-compliant businesses.

On July 1, 2020, the CCPA became enforceable by the California Attorney General, despite calls from the tech industry to delay due to business disruptions caused by the COVID-19 pandemic and concerns that final regulations had not yet been approved. The CCPA grants California residents more control over how certain businesses use their personal information. Although the CCPA went into effect on Jan. 1, 2020, a previous 2018 amendment added six months before enforcement by the California Attorney General could begin. However, businesses were required to begin complying by the January 1 effective date. Under the statute, businesses are granted 30 days to cure any alleged violations of the law after being notified of alleged noncompliance. If a business fails to cure the alleged violation, it may be subject to an injunction and liable for a civil penalty of up to $2,500 for each violation or $7,500 for each intentional violation.

On March 20, 2020, more than two dozen trade associations and business groups sent a joint letter to the office of the attorney general requesting that enforcement be delayed until Jan. 2, 2021. The letter, which was signed by the Internet Coalition and the California U.S. Chamber of Commerce, among others, also pointed out that the state-issued regulations for the law had yet to be finalized. "We are concerned that given current events and the presently unfinished status of the regulations implementing the CCPA, businesses will not have the operational capacity or time to bring their systems into compliance with the final regulatory requirements by July 1, 2020," the letter stated.

In an interview with *The Washington Post*, Becerra acknowledged the request but noted that the law had already gone into effect on January 1. "It'd be very awkward to continue another six months as some companies were requesting where people would have rights, companies would have obligations, but no one would be there to make sure those rights are being complied with," Becerra told the newspaper.

Meanwhile, privacy experts anticipated strong enforcement from Becerra during the COVID-19 pandemic, citing a coronavirus-related alert Becerra issued on April 10. "Whether it's our children's schooling, socializing with family and friends, or working remotely — we are turning to mobile phones and computers as a lifeline. With such a dependency on online connectivity, it is more important than ever for Californians to know their privacy rights," Becerra wrote.

Although Becerra had previously declined to state whether the office would begin enforcement on July 1, in a July 9 keynote presentation with the International Association of Privacy Professionals (IAPP), California Supervising Deputy Attorney General Stacey Schesser confirmed that initial compliance notice letters had been sent. Although the letters themselves remain confidential, according to ReedSmith privacy attorneys Samuel F. Cullari and Alexis Cocco, Deputy Schesser provided some insight into the letters' substance:

- "They targeted multiple industries and business sectors."
- "They focused on businesses that operated online and were missing either key privacy disclosures or a 'Do Not Sell' link (where AG thought one was necessary)."
- "The targets of the letters were identified based, at least in part, on consumer complaints, including complaints made using social media."

According to Cullari and Cocco, Deputy Schesser also offered insight into future enforcement actions by referencing past enforcement actions, which have focused on wide-scale impact and actual harm to Californians.

After several draft regulations and comment periods, on June, 2, 2020, Becerra submitted final regulations to the OAL for approval as well as a final "statement of reasons" to clarify the requirements and enforcement of the CCPA. Under the statute, the Attorney General is allowed to provide guidance through additional regulations "necessary to further the purposes of the [CCPA]." On Aug. 14, 2020, the OAL approved the Attorney General's CCPA regulations. Five provisions were withdrawn from OAL review; those provisions "required businesses to obtain express consent from consumers before using previously collected information for a materially different purpose, required businesses substantially interacting with consumers offline to provide notice of right to opt-out via an offline method, established minimum standards for submitting

CCPA, *continued on page 24*

CCPA, *continued from page 23*

requests to opt-out to businesses, and provided businesses with the ability to deny certain requests from authorized agents." The approved regulations put forth specific requirements and procedures for items such as the drafting of notices, the contents of web pages and privacy policies, opt-in and opt-out notices, and how businesses should respond to consumer requests.

Importantly, a GDPR-compliant program does not provide a safe harbor for CCPA compliance. As the Final Statement of Reasons explains: "[B]ecause of the key differences between the GDPR and CCPA, especially in terms of how personal information is defined and the consumer's right to opt-out of the sale of personal information (which is not required in the GDPR)," the Office of the Attorney General rejected a limited exemption for GDPR-compliant firms as "it would be less effective in carrying out the purposes of the CCPA." Therefore, as Strauss and Rogers highlighted, businesses subject to GDPR will need to take additional measures to comply with the CCPA as well. Further, compliance with Privacy Shield does not guarantee compliance with the CCPA or GDPR. For more information on the status of 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*.

Privacy experts raised frustrations that the final regulations failed to clarify how to interpret key terms, meaning that will be determined through litigation. Mary Stone Ross, consultant and past president of the advocacy group Californians for Consumer Privacy that helped draft the ballot initiative that spurred the enactment of the CCPA, stated "I'd imagine that, once the attorney general starts enforcing, there will be a lot of debates and arguments over the trickier definitions in these regulations, which will ultimately eventually lead to more consensus on these issues."

Litigation Under the California Consumer Privacy Act's Private Right of Action Begins

Several lawsuits have already been brought under the CCPA that raise noteworthy questions about the scope of the CCPA's private right of action. Although the extent of possible liability from private litigation brought under the CCPA is largely unknown as courts are just beginning to grapple with the new law, privacy attorneys have noted several themes arising from plaintiffs' complaints such as a preference for class actions and federal court, as well as attempts to bring broad claims under several CCPA provisions and use alleged CCPA violations as a basis for liability under other California statutes. Furthermore, privacy attorneys have noted that the popularity of video conferencing software and social media apps in light of the COVID-19 pandemic has spurred much litigation.

In addition to enforcement by the California Attorney General, the CCPA provides a narrow private right of action applicable only to the CCPA's data security provision. That provision states: "Any [California resident] consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." The definition of "personal information" in the context of the private right of action is narrower than the expansive definition applicable to other CCPA provisions and applies only to an individual's name together with an identifying data element, such as a Social Security number, driver's license number, or medical information. Under the provision, a plaintiff may seek injunctive or declaratory relief, actual damages or statutory damages in an amount not less than $100 and not greater than $750 per consumer, per incident. Before seeking statutory damages, however, the consumer must provide the business 30 days written notice to cure the alleged violation. The CCPA also explicitly prohibits plaintiffs from alleging that a CCPA violation constitutes a violation of other statues.

Privacy attorneys have noted that several of the current cases pending under the CCPA have been brought as class actions in federal court. McDermott Will and Emery partner Laura E. Jehl asserted that although the number of class actions is not surprising, the fact that the claims have been brought in federal court creates "an interesting dynamic whereby the federal courts may have the opportunity to examine and adjudicate CCPA before California state courts do." This trend, Jehl writes, "may incentivize the California attorney general to bring early enforcement actions to establish binding precedent in state courts before many cases are adjudicated by the federal courts."

Meanwhile, although the CCPA's private right of action is explicitly limited to allegations arising under the data security provision and the defendant's failure to provide "reasonable security," plaintiffs are attempting to bring claims for violations arising under other CCPA provisions. For example, in *Taylor v. Zoom Video Communications, Inc.*, plaintiffs alleged violations arising under Cal. Civ. Code § 1798.100(b), requiring notice at or before the point at which personal information is collected and limiting additional uses of personal information; and Cal. Civ. Code §1798.120(b), requiring a business to provide notice of the right to opt-out of sales of personal information.

In addition, plaintiffs have also attempted to use alleged violations of the CCPA as constituting claims under other California statutes, such as the California Unfair Competition Law. For example, in *Hurvitz v. Zoom Video Communications, Inc. et al.*, the plaintiffs alleged that defendant Zoom did not provide notice to consumers of the categories and uses of personal information it collects at or before the point of collection, in violation of the CCPA. However, because of the limited private right of action in the CCPA, the plaintiffs alleged that the violation constitutes an unlawful business practice in violation of the California Unfair Competition Law, even though the CCPA explicitly bars such action. Although the statute presumably bars such claims, it remains to be seen if courts will follow the statute.

Finally, lawsuits filed against videoconferencing companies such as Zoom Video Communications, Inc., may help clarify the meaning of the terms "unauthorized access" and "reasonable security procedures and practices" in the CCPA's private right of action. For example, in *Cullen v. Zoom Video Communications, Inc.*, plaintiffs highlight that Zoom's iOS app previously featured a digital advertising platform's software development kit that collected certain device identifiers, such as device carrier, device model and time zone. Several days after an article was published on the practice, Zoom released a blog post stating that it had been unaware that the software

was collecting device identifiers and had removed the advertising platform and software. The plaintiffs allege that Zoom's actions violated its duty to implement and maintain reasonable security procedures and practices, resulting in the unauthorized disclosure of plaintiffs' nonencrypted and nonredacted personal information. "Although the private right of action is widely understood to protect only against data breaches, the Cullen plaintiffs make at least a colorable allegation that the right of action may apply to exchanges of information between business partners," Jehl wrote. For more information about privacy issues with Zoom during the COVID-19 pandemic, see "COVID-19 Pandemic Raises Data Privacy and Security Questions and Concerns" on page 11 in this issue of the Silha *Bulletin*.

California Privacy Rights Act Qualifies for November Ballot

On June 25, 2020, California Secretary of State Alex Padilla certified that the California Privacy Rights Act (CPRA) qualified for and will appear on the California fall ballot. The referendum, backed by California real estate developer Alastair Mactaggart and consumer advocacy group Californians for Consumer Privacy, would amend the CCPA and establish a new California Privacy Protection Agency to replace the California attorney general's office as the main privacy rights regulator. Both privacy advocates and business experts expressed concerns about the initiative.

If passed, the CPRA would go into effect on Jan. 1, 2023. According to the International Association of Privacy Professionals the initiative would:

- create new rights around the use and sale of sensitive personal information (health, financial, racial or ethnic origin, precise geolocation);
- enhance children's privacy by tripling fines for violations of the CCPA's opt-in to sale right and create a new requirement to obtain opt-in consent to collect data from consumers under the age of 16;
- create transparency obligations around automated decision-making and profiling of consumers;
- create a right to data minimization, as well as providing notice to consumers about the length of time each category of personal information will be retained;
- create a right to correct inaccurate personal information;
- direct obligations on service providers to assist businesses with CPRA compliance activities;
- include email account credentials in the categories of personal information potentially subject to the CCPA "reasonable security" private right of action under Section 1798.150(a);
- create a new California Privacy Protection Agency that would replace the attorney general's office as the regulator implementing CPRA rules and enforcing its requirements against violators;
- expand the private right of action for consumers to cover breach of an email address in combination with a password and security question and answer permitting access to the email account.

In a statement following the qualification announcement, Mactaggart emphasized that "[d]uring these times of unprecedented uncertainty, we need to ensure that the laws keep pace with the ever-changing ways corporations and other entities are using our data." Mactaggart was the drafter of the 2018 California ballot initiative that served as the basis for the California Consumer Privacy Act of 2018. However, in an open letter announcing the new ballot initiative, Mactaggart stated that CCPA "now seems insufficient" and emphasized that "some of the world's largest companies have actively and explicitly prioritized weakening the CCPA."

Privacy advocates noted that the new initiative included several compromises between business and consumer privacy concerns. For example, in an October 2019 open letter, a coalition of eleven privacy groups including the Electronic Frontier Foundation (EFF), the Center for Digital Democracy, and the American Civil Liberties Union California Chapter, proposed several ways to strengthen the initiative. One of the proposals was that Mactaggart remove an exemption that states businesses do not have to comply with certain data requests if the data helps "ensure security and integrity;" however, the final ballot measure still includes such an exemption. EFF staff attorney Adam Schwartz noted that ad tech firms could use the exemption as an excuse to hoard data in the name of preventing click fraud. "On the whole, I think the initiative is a mixed bag with some steps forward, steps backward, some missed opportunities, and half steps," Schwartz told *Protocol*.

— Sarah Wiley
Silha Research Assistant

CJEU Strikes Down EU-U.S. Privacy Shield, Confirms Validity of Standard Contractual Clauses

On July 16, 2020, the Court of Justice of the European Union (CJEU), the European Union's (EU) top court, released its ruling in *Schrems II*, in which it struck down the EU-U.S. Privacy Shield (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 (July 16, 2020). However, the Court also confirmed the validity of standard contractual clauses (SCCs) — language widely adopted in EU data transfer written agreements used by companies, including Facebook, to transfer personal data — but required companies to ensure that third-party countries outside the EU meet EU privacy standards and requirements. Following the ruling, several observers raised concerns with the invalidation of the Privacy Shield and the increased requirements related to SCCs, providing several recommendations to companies that handle EU data.

PRIVACY

Schrems II arose following the European Court of Justice's (ECJ) October 2015 decision to invalidate the EU-U.S. Safe Harbor framework (*Schrems I*). Case C-362/14, *Schrems v. Data Prot. Comm'r.* (*Schrems I*), 2015 E.C.R. I-650 (Oct. 6, 2015). On July 12, 2016, the European Commission officially adopted an amended version of the Privacy Shield to replace the Safe Harbor framework. The Privacy Shield included several additional commitments by U.S. government agencies concerning surveillance of individuals in the United States. On Oct. 18, 2017, the European Commission released a report on the annual review of the Privacy Shield, which concluded that the United States had "put in place the necessary structures and procedures to ensure the correct functioning of the [Shield]."

Following the adoption of the Privacy Shield, several critics contended that it did not depart significantly from the Safe Harbor framework. The Article 29 Working Party, which provided the European Commission with independent advice on data protection matters, had several concerns, including a lack of specific rules on automated decisions; the general right of data subjects to object to the processing of data relating to them; the specific right of any data subject to be informed and to object to use of personal data without justification; and the lack of assurance that mass, indiscriminate collection of personal data would not take place.

Following *Schrems I*, Facebook switched to using SCCs with the belief that they would provide adequate privacy protections for its users. On Dec. 1, 2015, Max Schrems, an Austrian privacy advocate, filed a renewed complaint to the Data Protection Commissioner of Ireland (DPC), Helen Dixon, asking her to halt data transfers under SCCs. Schrems argued 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. Schrems contended that U.S. surveillance law was not in line with the *Schrems I* ruling.

Around the same time that Schrems filed his complaint, the Irish High Court overturned Dixon's earlier decision to not investigate Facebook Ireland in light of Schrems' original complaint. Dixon summarily 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, in which she explained her preliminary opinion that Schrems' complaint was "well-founded." Dixon wrote that U.S. law failed to adequately provide legal remedies to EU citizens. The 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. Furthermore, Dixon contended that she could not complete the investigation into Facebook without a CJEU ruling that the clauses were, in fact, invalid.

The proceedings in the Irish High Court, which has jurisdiction in criminal and civil cases, began in February 2017. During this period, Dixon provided her opening argument and explained the relevant EU and U.S. laws and authorities. Additionally, several experts provided testimony, including Peter Swire, a Georgia Institute of Technology Scheller College of Business professor, who served as an expert witness on behalf of Facebook. In a Sept. 11, 2017 commentary for *Lawfare*, Swire summarized his testimony into four findings. First, Swire provided a "detailed explanation documenting systemic protections under U.S. law for foreign intelligence surveillance." Second, Swire documented "how the U.S. legal system provides numerous ways for an individual to remedy violations of privacy." Third, Swire's testimony included "original research" into Foreign Intelligence Surveillance Court (FISC) oversight, with the general conclusion that "the FISC provides far stronger oversight than many critics have alleged." Finally, Swire contended that there are broader implications of an "inadequacy finding" of SCCs in *Schrems II* beyond cross-border data flows between Ireland and the United States, including on the Privacy Shield.

In October 2017, Irish High Court Justice Caroline Costello filed a 152-page opinion in which she addressed whether SCCs violate applicable law and court precedent in both the EU and the United States. Costello concluded that neither three ECJ decisions regarding SCCs in 2001, 2004, and 2010, nor the introduction of the Privacy Shield Ombudsperson mechanism, "eliminate[d] the wellfounded 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." As a result, Costello "refer[red] the issue of the validity of the SCC decisions to the [CJEU] for a preliminary ruling."

On July 9, 2019, the CJEU heard arguments in the case after the Supreme Court of Ireland previously rejected an attempt by Facebook to block the EU court from hearing the case. (For more

information on *Schrems I* and *II*, as well as the Privacy Shield, see "The United States, the European Union, and the Irish High Court Wrangle Data Privacy Concerns" in the Fall 2017 issue of the Silha *Bulletin*.)

On Dec. 19, 2019, Advocate General Saugmandsgaard Øe issued his opinion in *Schrems II*, finding that SCCs were valid. He first reasoned that "EU law applies to transfers of personal data to a third country where those transfers form part of a commercial activity, even though the transferred data might undergo processing, by the public authorities of that third country, for the purposes of national security."

Second, Øe found that SCCs "adopted by the [European] Commission provide a general mechanism applicable to transfers irrespective of the third country of destination and the level of protection guaranteed there." Øe emphasized that the "appropriate safeguards afforded by the exporter, inter alia by contractual means, must themselves ensure th[e] level of protection" required under the EU's General Data Protection Regulation (GDPR), a set of rules governing how businesses handle European Union (EU) citizens' personal data, which took effect on May 25, 2018.

Third, Øe wrote that "there is an obligation" placed on those handling EU citizens' data "to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with."

Fourth, Øe determined that it was not necessary to examine the validity of the Privacy Shield, including because "although the Court's answers to . . . questions [regarding the Privacy Shield] might, at a later stage, prove helpful to the DPC for the purposes of determining, in the context of the procedure underlying the dispute, whether the transfers in question should . . . be suspended because of the alleged absence of appropriate safeguards, it would, in my view, be premature to resolve them in the context of the present case."

Nevertheless, Øe wrote that he found "it appropriate to develop, in the alternative and with certain reservations, some non-exhaustive observations on that subject." He ultimately wrote that he had "certain doubts as to the conformity of the 'privacy shield' decision to Article 45(1) of the GDPR" and EU law more generally.

Øe's full opinion is available online at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=49246.

On July 16, 2020, the CJEU released its decision in *Schrems II*, which largely followed Øe's opinion. The Court first ruled that SCCs remained a valid method of transferring personal data outside the EU, but emphasized certain requirements for companies and organizations using such mechanisms. The Court wrote that a data "controller or processor may transfer personal data to a third country only if the controller or processor has provided 'appropriate safeguards', and on condition that 'enforceable data subject rights and effective legal remedies for data subjects' are available." The Court concluded that "such safeguards [are] able to be provided by the standard [contract] clauses adopted by the Commission."

> "Data flows are essential not just to tech companies — but to businesses of all sizes in every sector."
>
> **— U.S. Secretary of Commerce Wilbur Ross**

The Court further found that SCCs "provide[] . . . an "effective mechanism[]" that can, and must, ensure "compliance with the level of protection required by EU law." One way such clauses needed to do so, according to the CJEU, is allowing for a "competent [EU member state supervisory authority (SA)] . . . to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if . . . those clauses are not or cannot be complied with in that third country and the protection of the data transferred . . . cannot be ensured by other means."

Second, the CJEU turned to whether the United States "ensures an adequate level of protection" to make the Privacy Shield an effective and legal mechanism to protect EU citizens' data privacy. The Court concluded that the U.S. law and authorities did not adequately protect EU citizens' data to the extent required by EU law, including under the GDPR.

The Court provided several reasons why this was the case, including that U.S. law lacks "effective legal remedies for data subjects," as well as a "principle of proportionality" to ensure that data collection and use by the federal government only occurs when "necessary" to meet legitimate interests or "to protect the rights and freedoms of others."

The Court also cited U.S. government surveillance, including Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), which authorized the PRISM and Upstream programs by the National Security Agency (NSA). The Court held that "[i]n those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States . . . are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required . . . under EU law."

The Court further found that the "introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies which the Commission itself found in connection with the judicial protection of persons whose personal data is transferred to that third country." The Court therefore ruled that the Privacy Shield was incompatible with the GDPR and declared it "invalid." 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.

In a July 16, 2020 statement, U.S. Secretary of Commerce Wilbur Ross said that the U.S. Department of Commerce was "deeply disappointed that the court appears to have invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield." He continued, "We have been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that

Privacy Shield, *continued on page 28*

Privacy Shield, *continued from page 27*
is so vital to our respective citizens, companies, and governments."

Ross added, "Data flows are essential not just to tech companies — but to businesses of all sizes in every sector. As our economies continue their post-COVID-19 recovery, it is critical that companies — including the 5,300+ current Privacy Shield participants — be able to transfer data without interruption, consistent with the strong protections offered by Privacy Shield." Ross's statement is available online at: https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and

A Department of Commerce press release containing Ross' statement noted that the department would "continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List." It added, "Today's decision does not relieve participating organizations of their Privacy Shield obligations."

Similarly, the Federal Trade Commission (FTC) released a statement in which it clarified that it "continue[d] to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework. We also encourage companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers." The FTC statement is available online at: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield

Nevertheless, several observers raised concerns with the CJEU's ruling and provided recommendations to companies for how to proceed with transferring data between the EU and United States.

In a July 17, 2020 commentary, Nixon Peabody LLP attorneys contended that the CJEU's ruling "creates uncertainty for any business relying on the Privacy Shield." They argued that although "it is to be expected that a new mechanism will be created in the wake of the Privacy Shield," companies "[i]n the meantime . . . should review transfers of personal data from the EU to the U.S. and make sure they are protected by the Standard Contractual Clauses, which remain valid legal mechanisms to comply with the GDPR. Valid transfers of personal data are only one step toward compliance with the GDPR, however. Full compliance with the GDPR requires a fact-intensive review of all aspects of business operations, and should be undertaken with the assistance of experienced counsel." The Nixon Peabody LLP commentary is available online at: https://www.nixonpeabody.com/ideas/articles/2020/07/17/eu-privacy-shield-ruling

In a July 27, 2020 interview with *The National Law Review*, Kenneth K. Dort, a partner at Faegre Drinker Biddle & Reath LLP, laid out the two "main compliance concerns" arising from the invalidating of the Privacy Shield. "First, for those businesses relying on the Privacy Shield for data transfers from the EU to the US, they now lack the protective devices mandated by the GDPR. Because the decision did not provide for any grace period, they must adopt replacement measures immediately," Dort said. "Second, for those businesses relying on EU Standard Contractual Clauses (SCCs), the decision called into question their viability in light of questions over their ability to protect EU personal data against national security inquiries by the U.S. federal government." He added, "Thus, the major consequences of the decision for businesses transferring data into jurisdictions lacking an adequacy determination (such as the U.S.) will be to implement recognized protocols that address the national security issues raised in the decision and which also satisfy EU data protection authorities."

Dort also noted that the CJEU ruling required "additional safeguards" related to SCCs, which " may put U.S. businesses in a difficult position between their EU clients (the data transferors) and their legal obligations under U.S. national security law." He continued, "First, companies should carefully determine whether they handle personal data at all — and if they do not, these issues disappear. However, if personal data is being transferred, a careful analysis should be performed to determine if the transfer is actually necessary, and if not, minimize the scope of the transfers. Finally, if personal data transfers are at issue, then affected U.S. businesses need to confer with their EU controllers to determine what measures can be taken to satisfy both the controllers and their specific data processing agreements [(DPA's)]." Dort concluded, "Depending on the stridency of the DPA, some transfers to the U.S. may have to cease."

In a commentary following the CJEU ruling, four Jones Day partners laid out "three key takeaways," including that "[c]ompanies that until now have relied on the EU-U.S. Privacy Shield for data transfers from the European Union to the United States should implement alternative safeguards (e.g., SCCs, Binding Corporate Rules within their group)." Second, the commentary cautioned that "[a]lthough companies can continue to use [SCCs] as a safeguard for transferring personal data to processors outside the EU/EEA, they will have to follow the level of data protection provided in the third country and, where conflicts with the provisions of the Clauses arise, to suspend data exports. Monitoring the relevant aspects of the legal system of the third countries concerned should therefore be integrated into corporate compliance programs."

Finally, the commentary noted that the EU Commission was already working on "instruments for international transfers of personal data, including by reviewing the existing SCCs." The commentary therefore emphasized that "[t]he further development of new safeguards as announced by the EU Commission should be closely followed." The Jones Day commentary is available online at: https://www.jonesday.com/en/insights/2020/07/schrems-ii-confirms-validity.

— Scott Memmel
Postdoctoral Associate

Clearview AI Raises Privacy Concerns, Pursues First Amendment Defense

PRIVACY

In January 2020, *The New York Times* published an article detailing the practices of Clearview AI ("Clearview"), a technology company that created a groundbreaking facial recognition app in which a user can upload a picture of an individual and obtain a trove of "public photos of that person, along with links to where those photos appeared." Several lawsuits and class actions have been filed in response, alleging that Clearview's practices violate individuals' privacy. Some of the lawsuits, including one brought by the American Civil Liberties Union (ACLU) and other privacy advocacy groups, allege that Clearview's practices violate the Illinois Biometric Privacy Act (BIPA). In response, Clearview has argued that its data-scraping and sharing practices are protected by the First Amendment. Although the lawsuits have yet to be heard on their merits, they highlight growing concerns over data-scraping and facial recognition technology and the potential conflict between privacy and legitimate information gathering.

Clearview's app relies on a massive database of "more than three billion images" that Clearview claimed to have scraped from public-facing websites such as Facebook, YouTube, Venmo, and millions of other websites. Data-scraping — sometimes referred to as text and data mining — means extracting information from a website or computer database, and is often done using automated software. Clearview claimed that, through this enormous database, its app can instantaneously identify the subject of a photograph with unprecedented accuracy. According to court documents and news reports, Clearview's users include private individuals, companies such as Kohl's, Walmart, Wells Fargo, and the Chicago Cubs, as well as law enforcement agencies and other governmental entities throughout the United States at the federal, state, and local levels. According to a *Buzzfeed News* investigation, by February 2020, people associated with 2,228 companies, law enforcement agencies, and other institutions had collectively performed nearly 500,000 searches of Clearview's faceprint database.

Shortly after *The New York Times* article appeared, several lawsuits were filed in federal and state courts in California, Illinois, New York, and Virginia. On March 20, 2020, Vermont Attorney General Thomas J. Donovan also filed a lawsuit against Clearview for violations of the Vermont Consumer Protection Act. The complaint also alleges that Clearview AI violated Vermont's data broker law by fraudulently acquiring data through its use of data-scraping.

In Illinois, several cases, including *Mutnick v. Clearview AI*, *Inc.* and *ACLU et al.*, *v. Clearview AI*, *Inc.*, allege violations arising under BIPA, which limits how companies can collect and use biometric data. *Mutnick v. Clearview AI*, *Inc.*, No. 1:20-cv-00512 (N.D. Ill. Jan. 22, 2020); *American Civil Liberties Union v. Clearview AI*, *Inc.*, No. 9337839 (Ill. Cir. Ct. May 28, 2020). A copy of the *Mutnick* plaintiff's complaint is available online at: https://cdn.arstechnica.net/wp-content/uploads/2020/03/clearview_illinois_suit.pdf. A copy of the ACLU's complaint is available online at: https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint. Passed in 2008, the BIPA is considered the most comprehensive U.S. law regarding biometric information. The BIPA defines a "biometric identifier" to include "a retina or iris scan, fingerprint, or scan of hand or face geometry." However, the law also specifically excludes photographs from its definition of biometric identifiers. The BIPA also defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Among other measures, the BIPA prohibits companies from collecting or using biometric information unless they (1) inform the subject about the data's collection, (2) inform the subject in writing about the purpose and length of the data collection and use, and (3) receive a written release by the subject authorizing the collection and use of the data. Furthermore, the BIPA states that companies possessing biometric information cannot "disclose, redisclose, or otherwise disseminate" the data unless it obtains consent, it is required to complete an authorized financial transaction, it is required by state or local law, or it is required by warrant or subpoena.

In *Mutnick v. Clearview AI*, *Inc.*, plaintiffs alleged that Clearview covertly scraped individuals' images from the internet and then used artificial intelligence algorithms to unlawfully scan and retain the facial geometry of each individual depicted in the images in violation of the notice, consent, and retention requirements under the BIPA. Plaintiffs also allege that the data-scraping practices of Clearview were "in violation of the contractual terms governing its use of the websites from which the images originated," therefore, plaintiffs argue, that "Clearview impaired the rights of Plaintiff and Class Members, who were contractual parties and/or third-party beneficiaries of those contracts."

On August 12, Judge Sharon Johnson Coleman of the U.S. District Court for the Northern District of Illinois denied Clearview's motion to dismiss for lack of jurisdiction or alternatively to transfer the case to the Southern District of New York, where Clearview is based. Judge Coleman highlighted that Clearview had entered hundreds of agreements with local law enforcement and government agencies, including police departments in Chicago, to provide them access to its facial recognition database. "Through these agreements, defendants have sold, disclosed, obtained and profited from the biometric identifiers of Illinois citizens," Judge Coleman wrote. Judge Coleman also asserted that the company's contacts in Illinois were not "random, fortuitous or attenuated," and there is no legal requirement that a company exclusively target state residents or customers to satisfy jurisdictional requirements. A copy of Coleman's decision is available online at: https://files.lbr.cloud/public/2020-08/1300000-1300810-https-ecf-ilnd-uscourts-gov-doc1-067124516552.pdf?dJm2aRIJTfP-JQQRuCRZVD0LwIfrGCIAN.

In a separate order on August 12, Judge Coleman granted plaintiff Mutnick's request to consolidate the related cases of *Hall v. Clearview AI*, *Inc.*, and *Marron v. Clearview AI*, *Inc.*

Clearview, *continued on page 30*

Clearview, *continued from page 29*

Judge Coleman granted the *Mutnick* plaintiffs leave to file a consolidated complaint by no later than Aug. 31, 2020 and stated that Defendant Clearview's answer is due on Sept. 14, 2020. *Hall v. Clearview AI, Inc.*, No. 1:20-cv-00846 (N.D. Ill. Feb. 5, 2020); *Marron v. Clearview AI, Inc.*, No. 1:20-cv-02989 (N.D. Ill. May 20, 2020). *Marron v. Clearview AI, Inc.*, No. 1:20-cv-02989 (N.D. Ill. May 20, 2020).

On May 28, 2020, the ACLU, Chicago Alliance Against Sexual Exploitation, the Sex Workers Outreach Project, the Illinois State Public Interest Research Group, and Mujeres Latinas en Acción sued Clearview in Illinois state court claiming that the company had violated the biometric privacy rights of their members, program participants, and other Illinois residents on a "staggering scale." The complaint argues that vulnerable communities — including sex workers, sexual assault survivors, and undocumented immigrants — are especially harmed by facial recognition surveillance and alleges that Clearview's data-scraping practices captured faceprints from images without consent in violation of the BIPA. "In capturing these billions of faceprints and continuing to store them in a massive database, Clearview has failed, and continues to fail, to take the basic steps necessary to ensure that its conduct is lawful, including by obtaining the prior written consent of the individuals' who appear in the photos; informing those individuals of when their biometric data will be deleted; or even telling them to whom Clearview will be disclosing or selling their faceprints," the complaint states.

In response to the allegations, Clearview has argued that its practices — collecting and disseminating public information — are protected under the First Amendment. On August 11, *The New York Times* reported that Clearview had retained prominent First Amendment attorney Floyd Abrams. Litigation against Clearview "has the potential of leading to a major decision about the interrelationship between privacy claims and First Amendment defenses in the 21st century," Abrams told the *Times*. Abrams went on to explain that, in his view, although the technology used by Clearview is novel the underlying premise of the cases is a company's right to create and disseminate information. (Abrams delivered the 2005 Silha Lecture, titled "Confidential Sources of Journalists: Protection or Prohibition," on Oct. 24, 2005. For more on the lecture, see "2005 Silha Lecture Features First Amendment Attorney Floyd Abrams" in the Fall 2005 issue of the Silha *Bulletin*.)

Clearview is also represented by Tor Ekeland, an attorney known for representing hackers against charges of violating the Computer Fraud and Abuse Act (CFAA). On May 28, Ekeland told *Law360* that the lawsuit brought by the ACLU is an "opportunistic attempt" to censor a search engine that uses only publicly available images accessible on the internet. "It is absurd that the ACLU wants to censor which search engines people can use to access public information on the internet," Ekeland said. "The First Amendment forbids this." Ekeland's comments are available online at: https://www.law360.com/articles/1277681/advocacy-orgs-say-clearview-ai-broke-biometric-privacy-law.

> "[P]rivacy isn't always the enemy of the First Amendment, as companies eager for a deregulatory approach to their privacy-infringing activities would have you believe."
>
> **— University of Colorado Law School professors Margot E. Kaminski and Scott Skinner-Thompson**

However, other legal experts have pushed back against the argument that Clearview's practices are constitutionally protected. Albert Fox Cahn, attorney and executive director of the nonprofit Surveillance Technology Oversight Project, told *Law360* that "[n]o court has found there to a be a First Amendment right to harvest the public's biometric data to create a surveillance product."

In a March 9 essay for *Slate*, University of Colorado Law School professors Margot E. Kaminski and Scott Skinner-Thompson asserted that courts will probably consider whether the information collected and disseminated concerns matters of the public interest. "The information Clearview AI is gathering — biometric data of our faces from personal profiles on Facebook, LinkedIn, Twitter, and YouTube — usually isn't a 'matter of public interest.' It's the exact opposite — extremely personal and private information being used by the government (through Clearview AI) to track, police, and control the populace," wrote Kaminski and Skinner-Thompson. "[P]rivacy isn't always the enemy of the First Amendment, as companies eager for a deregulatory approach to their privacy-infringing activities would have you believe."

On August 16, Clearview challenged a motion for a preliminary injunction in *Mutnick*, arguing that an injunction requiring the company to stop collecting and selling biometric data is "flatly at odds with the First Amendment." In making the argument, Clearview highlighted the U.S. Supreme Court's 2011 decision in *Sorrell v. IMS Health Inc.*, which struck down a Vermont law that prevented pharmacies from selling prescription records. *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011). Vermont had passed the law in order to protect the privacy of doctors (patients' information was already anonymized), however the Court ruled that the law violated the First Amendment. "The creation and dissemination of information are speech within the meaning of the First Amendment," Justice Anthony Kennedy wrote in *Sorrell*.

(For more information about *Sorrell*, see "U.S. Supreme Court Invalidates Vermont Prescription Confidentiality Law" in the Summer 2011 issue of the Silha *Bulletin*.)

In its challenge to the preliminary injunction, Clearview also argued that its data-scraping code "matches information on the public internet to a specific user search query by running algorithms on public data." "Computer language is the language of the Internet, and it is protected by the First Amendment," Clearview wrote. As of August 2020, Judge Coleman had yet to rule on the preliminary injunction.

— Sarah Wiley
Silha Research Assistant

Twitter Hack Included Data Breach of User Accounts

On July 15, 2020, hackers breached Twitter's internal systems and compromised 130 user accounts, in some instances posting rogue tweets and downloading user data from the accounts. Dozens of high-profile users were targeted, including presidential nominee and former Vice President Joe Biden, Bill Gates, and Elon Musk. The rogue tweets posted to some users' accounts promised readers they could double an investment or contribution, but were in fact a financial scam.

PRIVACY

The incident began to emerge publicly around 4 p.m. Eastern when numerous prominent Twitter accounts tweeted a similar message offering to double people's money. "I am giving back to the community," one tweet read on Joe Biden's account. "All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes."

On its company blog, Twitter said it believed the hackers were able access the accounts by "target[ing] certain Twitter employees through a social engineering scheme," which entails "the intentional manipulation of people into performing certain actions and divulging confidential information." The blog post continued: "The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. As of now, we know that they accessed tools only available to our internal support teams to target 130 Twitter accounts. For 45 of those accounts, the attackers were able to initiate a password reset, login to the account, and send Tweets.. . . In addition, we believe they may have attempted to sell some of the usernames." In seven of the compromised accounts, the hackers also used the platform's "Your Twitter Data" feature and downloaded detailed account information and activity. "We are reaching out directly to any account owner where we know this to be true," Twitter said.

Among the actions that Twitter took in response to the breach was to restrict the ability of some accounts to post tweets or change passwords. "We did this to prevent the attackers from further spreading their scam as well as to prevent them from being able to take control of any additional accounts while we were investigating. We also locked accounts where a password had been recently changed out of an abundance of caution," Twitter said. Most accounts were restored to full functionality by the following day.

The company further said that it was investigating the incident, working with police, and evaluating how it could improve system security. Part of the investigation included determining precisely what information the hackers were able to view. Twitter said that for the compromised accounts, the hackers (1) could not access previous passwords; (2) could see email addresses, phone numbers, and other personal information; (3) accessed 36 users' direct messages, including one elected official from the Netherlands; and (4) "may have been able to view additional information" in accounts that were taken over by the hackers.

In a July 30 update to the blog post, the company described how it believed the attack unfolded. "A successful attack required the attackers to obtain access to both our internal network as well as specific employee credentials that granted them access to our internal support tools. Not all of the employees that were initially targeted had permissions to use account management tools, but the attackers used their credentials to access our internal systems and gain information about our processes. This knowledge then enabled them to target additional employees who did have access to our account support tools," Twitter said. The post continued: "This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems. This was a striking reminder of how important each person on our team is in protecting our service. We take that responsibility seriously and everyone at Twitter is committed to keeping your information safe."

Twitter's blog post ended by saying the company would work to improve security and bolster company-wide training to address social engineering attacks. "We're acutely aware of our responsibilities to the people who use our service and to society more generally. We're embarrassed, we're disappointed, and more than anything, we're sorry. We know that we must work to regain your trust, and we will support all efforts to bring the perpetrators to justice. We hope that our openness and transparency throughout this process, and the steps and work we will take to safeguard against other attacks in the future, will be the start of making this right," Twitter said.

That hackers exploited Twitter's internal operations was not a surprise to some observers. On July 27, 2020, *Bloomberg* reported that Twitter had "struggled for years to police the growing number of employees and contractors who have the ability to reset users' accounts and override their security settings." Chief Executive Officer Jack Dorsey and the company's board of directors had received multiple warnings in recent years about the issue, according to *Bloomberg*, citing former Twitter employees. Specifically, *Bloomberg* reported that "Twitter's oversight over the 1,500 workers who reset accounts, review user breaches and respond to potential content violations for the service's 186 million daily users have been a source of recurring concern." Twitter workers' access to user data is mostly limited to information like email addresses, phone numbers, and internet protocol addresses, but it can be enough information "to snoop on or even hack an account." *Bloomberg* reported that within the last several years, oversight of employees was so lax that "some contractors made a kind of game out of creating bogus help-desk inquiries that allowed them to peek into celebrity accounts, including Beyoncé's, to track the stars' personal data including their approximate locations gleaned from their devices' IP addresses." Twitter's security team at times "struggled to keep track" of account spying because of the prevalence of the practice, according to *Bloomberg*. "While some of the contractors were caught and fired, others started beating the formal logging system by creating fraudulent tickets that claimed something was wrong with a user account, only to grab that complaint themselves to resume their escapade, according to the employees," *Bloomberg* reported.

A Twitter spokesperson disagreed with how the former employees

Twitter, *continued on page 32*

Recent Minnesota Legal Disputes Involve Information Access and Defamation Liability

MINNESOTA

Two notable disputes involving information access and defamation liability were resolved in the summer of 2020 in Minnesota. In the first case, a judge granted a request from the news media to unseal the names of jurors in a high-profile murder trial from 2019. In the second case, a University of Minnesota law professor prevailed in a libel lawsuit against a former romantic partner and was awarded almost $1.2 million in damages.

On July 17, 2020, the Minneapolis *Star Tribune* reported that Fourth Judicial District Court Judge Kathryn L. Quaintance ordered the release of names of jurors in the 2019 trial of former Minneapolis police officer Mohamed Noor. The order came in response to a request from the *Star Tribune* and Hubbard Broadcasting seeking the names and other information. Quaintance had kept the names sealed because of concerns with how news organizations would use the information, the possibility that jurors might be asked about their deliberations, and the potential that jurors could be harassed.

Although Quaintance ordered release of the names on August 3, she declined to release additional information about the jurors, such as where they live, dates of birth, occupations, marital status, and education. The order also sought to require journalists to contact jurors through their lawyers if they are represented by one. Quaintance issued a letter to jurors informing them that they may obtain free legal representation.

Suki Dardarian, the *Star Tribune*'s senior managing editor and vice president, said the newspaper was considering whether to appeal Quaintance's denial of the additional juror information. "We are surprised that she would withhold basic juror information that is routinely public in every other trial in the state of Minnesota," Dardarian told the *Star Tribune* for the July 17, 2020, story. She added: "Now is not the time for secrecy in our criminal justice system," she said."

On April 30, 2019, a jury convicted Noor of third-degree murder and second-degree manslaughter in connection with the July 2017 shooting death of 40-year-old Justine Ruszczyk Damond. Quaintance withheld juror names after the conviction multiple times. She wrote in a May 2019 order that disclosure of the names would likely mean their publication and the possibility of "unwanted publicity

Twitter, *continued from page 31*

described the company's policing of user account access to *Bloomberg* and said the company had the ability to "stay ahead of threats as they evolve." The spokesperson also confirmed that Twitter has a staff of about 1,500 employees and contractors to handle user accounts, but said "we have no indication that the partners we work with on customer service and account management played a part here." Workers are given only as much access as they need to perform their job duties and participate in "extensive security training and managerial oversight," the spokesperson told *Bloomberg*.

On July 31, 2020, *The New York Times* reported that three people were believed to be responsible for the Twitter hack. Prosecutors alleged that 17-year-old Graham Ivan Clark of Tampa, Fla., was principally responsible for the breach and was assisted by 19-year-old Mason John Sheppard of the United Kingdom and 22-year-old Nima Fazeli of Orlando, Fla. Prosecutors alleged that Clark was able to talk a Twitter employee into believing that he was a co-worker who needed another employee's security credentials to access the company's internal systems. Investigators were able to find the hackers based on unspecified clues they left about their identities and how they sought to hide the money they collected through Bitcoin, according to the *Times*. As of August 2020, Clark was facing 30 felony charges, including fraud.

In an Aug. 11, 2020 blog post with *Infosecurity Magazine*, cybersecurity expert Karen Bowen said the Twitter hack illustrates the risk of allowing too much internal access to user data. Bowen asked: "[W]hy did so many employees have access to verified accounts? Who had back-end access to the administrative tool? How could anyone easily alter trusted accounts without any approval?" Bowen suggested that such broad access made Twitter and the security of user data vulnerable. To improve security, she suggested separating employee duties so that they require more than just one person. Another way to secure user data is to limit authority for tasks; some actions, such as resetting passwords, do not necessarily require complete access to user data or full authorization in a system. "Employees, contractors, service providers and other insiders are in an opportune position to compromise data," Bowen wrote. "Privileged users, such as managers with access to sensitive information, pose the biggest insider threat to organization."

On July 16, 2020, *HuffPost* reported that the incident raised questions about the potential for hackers to disrupt the November 2020 election by sowing disinformation. The outlet reported that hackers could cause confusion or suppress voting by tweeting out false information through real accounts, such as those belonging to governments and the media. Nina Jankowicz, author of the book *How To Lose The Information War* and a disinformation fellow at the Woodrow Wilson International Center for Scholars in Washington, D.C., told *HuffPost*: "The biggest concern for me isn't necessarily that an account like [President Donald] Trump's would be hacked, it's if people could gain access to really legitimate, non-partisan sources of information and post misleading information on those accounts." Investigative researcher Diara J. Townes of First Draft, a nonprofit seeking to combat misinformation, told *HuffPost* that hacks about the election could undermine trust in the voting process. "It would be a question of how many people still believe voting by mail is safe, rather than how much bitcoin did the scammers get," Townes said.

— Jonathan Anderson
Silha *Bulletin* Editor

and harassment," a rationale that she continually cited in subsequent orders keeping the information sealed. Quaintance also cited a pending appeal by Noor as another reason to prevent disclosure of juror names.

On Oct. 28, 2019, Quaintance attended the 2019 Silha Lecture, in which attorney Kelli L. Sager talked about the public's right of access to judicial records and proceedings. During the Q&A session moderated by Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley, Quaintance said "jurors have a right to be anonymous." She further said that in her experience, jurors want protection and do not want the press intruding into their private lives. "Those are very real, pragmatic concerns, and are about keeping the trials fair," Quaintance said. (For more information on the Silha Lecture and Quaintance's comments and questions, see "34th Annual Silha Lecture Tackles Public and Media Access to Court Proceedings and Records" in the Fall 2019 issue of the Silha *Bulletin*. For more information about the news media's pursuit of the juror names, see "Minneapolis Star Tribune and Hubbard Broadcasting Seek Juror Names and Information in Noor Trial" in the Winter/Spring 2020 issue of the Silha *Bulletin*.)

University of Minnesota Law Professor Wins Defamation Lawsuit

On May 18, 2020, Fourth Judicial District Court Judge Daniel C. Moreno ruled in a defamation lawsuit brought by University of Minnesota Professor of Law Francesco Parisi. The lawsuit, against Parisi's former girlfriend, Morgan Wright, was a bench trial awarding him almost $1.2 million in damages, including $100,000 in punitive damages. At issue in the suit were allegations by Wright that Parisi beat and raped her and attempted to run her down with his vehicle, that he raped his own daughter and underage girls, and that he was HIV positive. Wright made these claims to police, the Minnesota Department of Health, and to Parisi's employer, the University of Minnesota. The court found these statements false and defamatory.

Underlying the defamatory statements was a real estate deal that went sour between Parisi and Wright. The two had met in September 2014 and soon made plans to jointly purchase a condo above Parisi's unit. When Wright stopped paying contractors and withdrew her money for the project, Parisi attempted to evict her. She later sued Parisi for battery, claiming he attempted to run her down with his vehicle. After Wright lost her civil suit and a subsequent appeal, she alleged to police that Parisi raped her. The court found the timing of the allegations suspect as they came shortly after Wright incurred legal setbacks.

In analyzing the defamation allegations, the court first found that Wright's statements to police alleging that Parisi raped her were not protected by a qualified privilege because she did not act in good faith. "Wright fabricated the many accusations she made against Parisi in retaliation for a failed relationship and a real estate venture gone awry. Good faith cannot exist in this context," the court wrote in its ruling. "Although Wright professes to believe her own accusations, it cannot be the case that one acts in good faith by convincing oneself that false accusations regarding the experience of a crime are true. Reckless disregard for the truth precludes good faith — Wright acted in reckless disregard for the truth when she made a false police report claiming Parisi raped her." The court further found that Wright did not meet other elements of qualified privilege, namely that she lacked proper motive or reasonable or probable cause to make the rape allegations to police. "The Court has found that Wright's report to the police was based on her desire to retaliate against Parisi for their broken relationship, the failed real estate deal, and her litigation losses," the court wrote.

The court then found that Parisi had "demonstrated that Wright committed many acts of defamation against him. She caused false statements to be published, and the record is replete with Wright's varying false allegations, made to others, that tended to harm Parisi's reputation, and that were understood to refer to Parisi."

The court also found that Wright engaged in defamation *per se* because she "accused Parisi of crimes, sexual impropriety or misconduct, and unprofessional behavior outside of her false police report." Defamation *per se* "presumes reputational damages and personal losses" and can be actionable "without any proof of actual damages," the court wrote.

In evaluating damages, the court found that Parisi was entitled to $50,000 for the cost of hiring defense counsel after his arrest on the false rape accusation; $130,000 to cover "diminished salary raises" that Parisi could have received as a professor; $87,500 for lost speaking and secondary teaching opportunities; $250,000 for lost consulting revenue; $67,164 for losing the opportunity to serve as director of a law and economics program; $279,850 for lost income that would have come from serving on the board of directors of an Italian organization; $100,000 in general and emotional damages for being jailed as a result of the rape allegation, during which time his mother died; $25,000 in general and emotional damages for the toll on Parisi's personal life; and $100,000 for "general reputational damages." The court also awarded Parisi $100,000 in punitive damages and further awarded him recovery of his costs in pursuing the lawsuit.

John Braun, Parisi's attorney, told the Minneapolis *Star Tribune* that despite the financial award his client won, an internet search for his name "returns a mug shot and headlines about him being a rapist, and it will forever. So part of the court's message is that in the 21st century this is a greater harm than it might have been in the past, and an award needs to anticipate the long arc of future harm still to be endured by its victim."

A copy of the court's decision is available online at: https://docs.google.com/viewerng/viewer?url=https://abovethelaw.com/uploads/2020/05/FINAL-Order-for-jdt-18-5381.pdf&hl=en_US.

— Jonathan Anderson
Silha *Bulletin* Editor

FRONTLINE Counsel Dale Cohen to Deliver 35th Annual Silha Lecture, "Inconvenient Truths and Tiger Kings: The Vital Role of Documentaries Today" on Oct. 19, 2020

Documentary films are everywhere. There is an unlimited supply of streaming shelf space, an endless array of stories to be told, and dwindling resources at traditional media outlets to tell them.

As the George Floyd killing demonstrates, the power of video to convey news and other messages is unmatched. Yet, the law and our institutions do not always treat documentaries the same as other news media.

SILHA CENTER EVENTS

The 2020 Silha Lecture, "Inconvenient Truths and Tiger Kings: The Vital Role of Documentaries Today," will explore the unique legal and ethical issues relating to documentaries. Where have we been and where is the law headed as everyone carries a sophisticated video camera and partisan advocacy grows?

This year's Silha Lecturer is Dale Cohen, Special Counsel to FRONTLINE, the award-winning PBS documentary series. He advises and leads the news team and producers on legal issues and ethical standards. Cohen is also Director and founder of the UCLA Doc Film Legal Clinic.

In addition to the Clinic, Cohen teaches News Media Law in the Digital Age at UCLA. His other teaching experience includes media law courses at University of North Carolina's School of Law, Emory College, the Philip Merrill College of Journalism at the University of Maryland, and the Medill School of Journalism at Northwestern University. A frequent speaker at documentary film festivals and media law conferences, Cohen is also the co-author of the textbook, *Media and the Law* (2d ed., LexisNexis). A graduate of Syracuse University with degrees in American Political Thought and Journalism, Cohen's J.D. is from the Northwestern University Pritzker School of Law.

The 35th Annual Silha Lecture is sponsored by the Silha Center for the Study of Media Ethics and Law. Due to the coronavirus pandemic, it will take place virtually on Monday, Oct. 19, 2020 as a synchronous Zoom webinar, starting at 7:30 pm Central Time (US and Canada). This event is free and open to the public, but preregistration is required. To preregister, go to https://z.umn.edu/2020SilhaLecture.

The Silha Center for the Study of Media Ethics and Law is based at the Hubbard School of Journalism and Mass Communication at the University of Minnesota. 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.

The University of Minnesota is an equal-opportunity educator and employer. To request disability accommodations, please contact Disability Services at 612-626-1333 or drc@umn.edu at least two weeks before the event.

— Elaine Hargrove
Silha Center Staff

The Silha *Bulletin* is a publication of the Silha Center for the Study of Media Ethics and Law. It is published three times a year: late fall, late spring, and late summer. It is available online at: https://hsjmc.umn.edu/research-centers/centers/silha-center/silha-center-bulletin and the University of Minnesota Digital Conservancy at: http://conservancy.umn.edu/discover?query=Silha+Bulletin.

If you would like to be notified when a new issue of the Silha *Bulletin* has been published online, or receive an electronic copy of the *Bulletin*, please email us at silha@umn.edu. Please include "Silha Bulletin" in the subject line. You may also call the Silha Center at (612) 625-3421.

Inconvenient Truths and Tiger Kings: The Vital Role of Documentaries Today

DALE COHEN, SPECIAL COUNSEL TO PBS's 'FRONTLINE'

Documentary films are everywhere. There's an unlimited supply of streaming shelf space, an endless array of stories to be told, and dwindling resources at traditional media outlets to tell them.

35TH ANNUAL SILHA LECTURE

The George Floyd killing demonstrates the unmatched power of video to convey news and other messages. Yet, the law and our institutions don't always treat documentaries the same as other news media.

We will explore the unique legal and ethical issues relating to documentaries. Where have we been and where is the law headed as everyone carries a sophisticated video camera and partisan advocacy grows?

This year's Silha Lecturer is Dale Cohen, Special Counsel to *Frontline*, the award-winning PBS documentary series, where he advises and leads the news team and producers on legal issues and ethical standards. He is also Director and founder of the UCLA Doc Film Legal Clinic and an adjunct professor of law.

> MONDAY, OCT. 19, 2020
> 7:30PM CDT
> REMOTE PRESENTATION
> FREE & OPEN TO THE PUBLIC, BUT ADVANCE REGISTRATION IS REQUIRED
> TO REGISTER, VISIT https://z.UMN.edu/2020SilhaLecture

The University of Minnesota is an equal opportunity educator and employer. To request disability accommodations, please contact Disability Services at 612-626-133 or drc@umn.edu at least two weeks before the event.

SILHA CENTER FOR THE STUDY OF MEDIA ETHICS & LAW

HUBBARD SCHOOL OF JOURNALISM & MASS COMMUNICATION
UNIVERSITY OF MINNESOTA

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW

HUBBARD
SCHOOL OF JOURNALISM
& MASS COMMUNICATION

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