THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | FALL 2017

Federal Search Warrants and Nondisclosure Orders Lead to Legal Action; DOJ Changes Gag Order Practices

In 2017, broad federal search warrants, as well as nondisclosure orders preventing technology and social media companies from informing their customers that their information had been handed over to the government, led to legal action and raised concerns from observers. However, the U.S. Department of Justice (DOJ) also changed its rules on the gag orders, leading a large technology company to drop its lawsuit against the agency regarding the orders.

In 2017, the DOJ filed two search warrants seeking extensive information from web hosting company DreamHost and from Facebook in connection to violent protests in Washington, D.C. during President Donald Trump's January 20 inauguration festivities. On Aug. 24, 2017, District of Columbia Superior Court Chief Judge Robert Morin ordered DreamHost to comply with a DOJ search warrant seeking email addresses and other information on individuals who visited www.disruptj20.org, a website used to organize protests against President Donald Trump. In the order, Morin also emphasized that the government must provide details of a minimization plan to limit violations of innocent third parties' First and Fourth Amendment rights, which he reemphasized in a separate September 15 order. On October 10, Morin allowed DreamHost to redact some identifying information about visitors to www.disruptj20.org until the government could demonstrate that the information was related to criminal activity.

On Sept. 28, 2017, the American Civil Liberties Union (ACLU) filed a motion to quash or narrow three DOJ search warrants that were also tied to the inauguration day protests. The warrants requested information concerning three Facebook users' accounts, including the names and personal information of 6,000 users who "liked" an anti-Trump Facebook page operated by one of the users. The DOJ announced on October 13 that it was dropping its request for the names of 6,000 users, but was still pursuing other information under the search warrants. In a November 9 opinion, Morin required Facebook to redact personally identifying information of all third parties tied to the three accounts, as well as requiring the DOJ to follow several procedural safeguards to ensure the privacy and First Amendment rights of third parties related to the Facebook accounts. Facebook had previously fought a DOJ gag order preventing the company from alerting the users of the accounts that the DOJ was seeking their information, which the government later dropped.

In a July 17, 2017 ruling, the U.S. Court of Appeals of the Ninth Circuit upheld the constitutionality of 18 U.S.C. § 2709(a),(c), which authorizes the Federal Bureau of Investigation (FBI) to prevent the subject of an administrative subpoena or search warrant, usually an electronic communication service provider, from disclosing the fact that it had received such a request. On Oct. 12, 2017, the Floyd Abrams Institute for Freedom of Expression at Yale Law School and 20 First Amendment Scholars, including Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley, filed an *amici* brief in response to the ruling, explaining that National Security Letters (NSL) issued by the FBI are accompanied by a nondisclosure order, which "empowers the government to preemptively gag a wire or electronic communication service provider from speaking about the government's request for information about a subscriber." The brief contended that these orders constitute prior restraints in violation of the U.S. Constitution and U.S. Supreme Court precedent. On the same day, the Reporters Committee for Freedom of the Press (RCFP), along with 20 media organizations, filed a separate *amici* brief, in which they also contended that the nondisclosure orders constitute prior restraints.

Finally, on Oct. 19, 2017, the DOJ significantly limited the imposition of gag orders by DOJ attorneys and agents that barred companies from informing their customers that their electronic information was turned over to the government. Following the changes, Microsoft announced that it was dropping its lawsuit against the DOJ asking a federal judge to strike down the portions of the Stored Communications Act (SCA), a provision of the Electronic Communications Privacy Act (ECPA), allowing the protective orders. 18 U.S.C. § 2705(b).

D.C. Judge Orders DreamHost to comply with DOJ Warrant, Later Places Limitations on Warrant

On Aug. 24, 2017, District of Columbia Superior Court Chief Judge Robert Morin ordered Los Angeles-based web-hosting company DreamHost to comply with a U.S. Department of Justice (DOJ) search warrant seeking email addresses and other information on individuals who visited www.disruptj20.org, a website used to organize protests against President Donald Trump. On September 15, Morin wrote an additional order reiterating his requirement that the government "present a minimization plan by which its review of the data and information produced by DreamHost would not include, to the extent possible, data or information of lawful activity not within the scope of the [w]arrant." Finally, on October 10, Morin limited the information the DOJ could obtain through the warrant, allowing DreamHost to redact some identifying information about visitors to www.disruptj20.org, though still allowing the disclosure of other information in the warrant.

Search Warrants, *continued on page 3*

Inside This Issue

Fall 2017: Volume 23, No. 1

Silha Center Staff

Search Warrants, *continued from page 1*

On January 20, six police officers were injured in protests during President Trump's inauguration, according to *The Washington Post* on July 8. The riots caused tens of thousands of dollars of damage to vehicles and store windows. In April 2017, the federal government charged 234 people with felony rioting in connection with the protests. A 31-year-old Florida man was sentenced to four months in jail after pleading guilty to two felonies: assault on a police officer and inciting a riot. Multiple other individuals pled guilty to misdemeanor charges, while some charges were dropped. As the *Bulletin* went to press, other individuals remained on trial, including freelance photographer Alexei Wood, who live-streamed the "J20" protest.

COVER STORY

About one week after the inauguration day riots, the federal government, as part of its investigation, served DreamHost with a grand jury subpoena, which called for seven categories of information related to www.disruptj20.org. The categories included "information identifying the individual registrant of the website, the registrant's physical addresses and email addresses, information about the services the registrant obtained from DreamHost, the payment for those services, and information about the registrant's computer interactions with DreamHost's servers." Within three weeks, DreamHost produced the records, with the understanding that the government was requesting only information about the registrants of the website, not third-party visitors.

In an August 14 blog post, DreamHost announced that the DOJ had asked the company in a July search warrant to provide "*all* information available" about the visitors to www.disruptj20.org. The search warrant, signed by D.C. Superior Court Judge Ronald P. Wertheim on July 12, stated that "Detective Greggory Pemberton [of the Metropolitan Police Department] . . . ha[d] probable cause to believe that in the premises controlled by DreamHost Inc., there [was] now . . . concealed property, namely stored electronic communications including but not limited to digital files, records, messages, and photographs . . . in violation of D.C. Code § 22-1322."

One section of the warrant asked DreamHost to disclose "all information in [its] possession . . . that might identify the subscribers related to [www.disruptj20.org], including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service[,] . . . means and source of payment for services[,] . . . and information about domain name registration." According to DreamHost, the warrant covered 1.3 million visitor IP addresses, as well as personal information of "thousands of people." The warrant also requested "all records or other information pertaining to [www.disruptj20.org]." The warrant required that DreamHost deliver the information via mail, courier, or email to Assistant U.S. Attorney John W. Borchert.

The second section of the warrant stated that the government would seize any "[i]nformation . . . that constitutes fruits, evidence and instrumentalities of violations of D.C. Code § 22-1322 involving the individuals who participated, planed [*sic*], organized, or incited the January 20 riot." The information sought in this section included the data detailed in the "disclosure" section, as well as "programming code used to serve or process requests made via web browsers; HTML, CSS, JavaScript, image files, or other files; HTTP request and error logs; . . . connections related to the website and any other transactional information; . . . other databases related to the website; [and] email accounts and the contents thereof, associated with the [website.]" The "seizure" portion of the warrant also included "[s]ubscriber information related to the accounts established to host [www.disruptj20.com]," which included names and addresses, payment information, and domain registration details. The full warrant is available online at: https://www.dreamhost.com/blog/wp-content/uploads/2017/08/DH-Search-Warrant.pdf.

On July 28, 2017, U.S. Attorney for the District of Columbia Channing Phillips (the government), filed a motion in the D.C. Superior Court for DreamHost to "show cause why [it] should not be compelled to comply with [the] warrant." According to the motion, the government sent a copy of the search warrant to DreamHost on July 14 and 17 via email and served a copy to the company's location in California. On July 19 and 20, the government requested that DreamHost "begin an immediate production of materials in response" to the warrant. However, on July 21, Raymond Aghaian, an attorney representing DreamHost, sent an email to the government discussing several concerns, including "some uncertainty [in] the language" of the warrant and that the D.C. Code does not apply because DreamHost's servers containing the records are located in Portland, Ore., according to DreamHost's August 14 blog post. Aghaian also contended that "[s]ome of the requested information likely falls under . . . the Privacy Protection Act [(PPA)]" and that "[s]ome of the information requested appears overbroad, requesting what amounts to all data without any limitations or a specified timeframe, likely constituting an overseizure [*sic*]." 42 U.S.C. §§ 2000aa.

In its motion, the government made two arguments why DreamHost should be required to provide cause why it had not complied with the warrant. First, the government contended the search warrant was lawful under the Fourth Amendment because the D.C. Superior Court determined "there was probable cause" to issue the warrant and that it was supported "by the sworn affidavit" by Pemberton. Thus, the government concluded that "there should be no dispute that the . . . search warrant was properly issued and that DreamHost must comply." Additionally, the government refuted Aghaian's suggestion that the warrant "runs afoul of 'the Superior Court's jurisdictional limits,'" calling this claim "misguided" and citing several federal statutes, including the Stored Communications Act (SCA).

Second, the government contended that DreamHost's other concerns were "without merit," including Aghaian's claim about "uncertainty [of] the language," which the government contended was "wholly irrelevant." The government also explained that the PPA "does not as a factual matter preclude the government from searching and seizing electronic information — even 'protected' materials — pursuant to a search warrant." Finally, the government argued that DreamHost's claim about the warrant being "overbroad" was "not a sufficient basis for DreamHost to refuse to comply with the warrant." The government later amended the warrant to specifically request information from July 1, 2016 to Jan. 20, 2017.

On August 11, Aghaian, on behalf of DreamHost, filed a response in opposition to the government's motion. The web hosting company first argued that the search warrant violated the Fourth Amendment. Aghaian contended that because the warrant "endangers the First Amendment interests of third parties," the warrant must be scrutinized with "particular exactitude," citing *Zurcher v. Stanford Daily*, in which the U.S. Supreme Court found that courts must "apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search." 436 U.S. 547, 565 (1978). Aghaian wrote, "Courts have specifically held that the government oversteps its authority when it seeks to obtain customer identities and records of activity in connection with protected speech, such

Search Warrants, *continued on page 4*

Search Warrants, *continued from page 3*

as that involved here.. . . It is not difficult to anticipate the impact this disclosure will have on the willingness of third parties to investigate and engage with web sites of political organizations."

Therefore, the response contended that the warrant's "description of the things to be seized does not pass the 'particularity test,'" which the Supreme Court ruled in *Maryland v. Garrison* was established to "prevent general searches." 480 U.S. 79, 84 (1987). DreamHost argued that the warrant "lack[ed] the required specificity" and was "not reasonable under the Fourth Amendment" because it would "[allow] the government to obtain large amounts of information, including the content of email communications, initiated by innocent third parties, [it failed] to identify with sufficient specificity what will be seized, and [it did] not explain to DreamHost what will happen to the large quantities of un-seized information."

Second, Aghaian contended that the government's search warrant violated the PPA because much of the data requested by the government could qualify as a "work product," "documentary material," or both under the PPA. Aghaian added, "Without any specification from the government, particularly given the over-expansive language of the Search Warrant, the Court should not compel DreamHost to provide all material to the government without a determination whether such material is intended for publication and if such material qualifies either as 'work product' or 'documentary material.'"

The PPA defines "work product" as materials created "in anticipation of communicating such materials to the public," including conclusions, opinions, or theories. "Documentary materials" are those "upon which information is recorded," such as written materials, photographs, and electronically recorded tapes or discs. 42 U.S.C. § 2000aa-7(a). Under the PPA, it is "unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" unless there is probable cause that the individual in possession of the materials committed or is committing a criminal offense, or if there is reason to believe seizing the materials would save a life, the materials contain information "relating to the national defense, classified information, or restricted data," or the materials relate to child pornography or the sexual exploitation of children. The PPA provides more circumstances for government officials to search for documentary materials, including if "there is reason to believe that the giving of notice pursuant to a subpoena . . . would result in the destruction, alteration, or concealment of such materials" or if the materials had "not been produced in response to a court order directing compliance with a subpoena."

> "[The DOJ request for data] seems quite concerning and extremely overbroad — raising both First and Fourth Amendment concerns.. . . It's targeting anyone who visited a site used to organize a protest, in a way that seriously risks chilling speech and associational rights."
>
> **— Jennifer Daskal, American University law professor**

Finally, Aghaian contended that the search warrant was "extraterritorial" meaning it was "issued from the District of Columbia but directed at electronic data stored in Oregon." According to Aghaian, Washington, D.C. law "only provides for search warrants executed in the District of Columbia."

Civil liberties advocates and members of the technology community were also critical of the search warrant. In an August 14 interview with *The Washington Post*, Mark Rumold, staff attorney for the Electronic Frontier Foundation (EFF), said that no plausible explanation exists for a search warrant of such breadth, "other than to cast a digital dragnet as broadly as possible." He added that the government's investigation into the January riots was being handled "in a blunt manner that does not take into account the significant First Amendment interests."

Jennifer Daskal, an American University law professor, told *The Hill* on August 16 that the DOJ's request for data appeared questionable. "It seems quite concerning and extremely overbroad — raising both First and Fourth Amendment concerns," Daskal said. "It's targeting anyone who visited a site used to organize a protest, in a way that seriously risks chilling speech and associational rights." She noted that searches were supposed to be "particularized based on individualized suspicion."

In its August 14 blog post, DreamHost wrote, "Chris Ghazarian, our General Counsel, has taken issue with this particular search warrant for being a highly untargeted demand that chills free association and the right of free speech afforded by the Constitution.. . . [The] information could be used to identify any individuals who used this site to exercise and express political speech protected under the Constitution's First Amendment. That should be enough to set alarm bells off in anyone's mind."

In light of the growing criticism of the search warrant, prosecutors from the U.S. attorney's office in Washington, D.C. dropped the request for IP addresses on August 22, as reported by the *Los Angeles Times* on August 22. They also amended the original warrant to focus only on the 234 people charged with rioting on January 20. In a court filing, the prosecutors noted that they were continuing to seek email addresses associated with www.disruptj20.org, as well as email addresses of third parties associated with the website. They wrote that they had "no interest in records relating to the 1.3 million IP addresses," but would continue pursuing information on the planning, coordinating, and participation of the protests. The prosecutors added, "The government values and respects the First Amendment right of all Americans to participate in peaceful political protests and to read protected political expression online. This warrant has nothing to do with that right.. . . The government is focused on the criminal acts of defendants and their co-conspirators, and not their political views."

In an August 14 statement, DreamHost called the DOJ shift a "huge victory for Internet privacy" and a "step in the right direction." However, DreamHost also wrote, "This late-in-the-game re-scoping of the request for data by the DOJ . . . didn't go far enough."

On August 24, multiple news agencies reported that D.C. Superior Court Chief Judge Robert Morin ordered DreamHost to provide the information requested in the DOJ's revised warrant. DreamHost was required to turn over the information to the court, which would hold the data while the company decided whether it

wanted to appeal. If DreamHost decided not to appeal, or Morin's ruling was not overturned by a court of appeals, the D.C. Superior Court would turn over the data to prosecutors, according to an August 24 report by *Politico*.

During the hour-long hearing, DreamHost's attorneys continued to argue that the search warrant was too broad and would include information of innocent users who visited the site but were not part of the riots, *Politico* also reported. Conversely, prosecutors John Borchert and Jennifer Kerkhoff argued that the warrant had to be broad because the government did not know every individual who was associated with the January 20 riots until after the data was reviewed.

Morin said during the hearing that he recognized the tension between free speech rights and law enforcement's need to search digital records for evidence, according to *The Washington Post*. Reuters reported that Morin said he would put restrictions on how the government reviews the material in order to protect First Amendment rights and online political discourse. First, Morin said he would require prosecutors to tell him who would review the data and why the information was "critical" to the government's case. Furthermore, Morin required that the government describe the process it would use and to develop a plan to minimize the search of material unrelated to any criminal activity. Second, Morin ordered that the information obtained by the government not be shared with other federal agencies and that any information not relevant to the investigation be put under court seal. Finally, Morin shortened the timeframe of the warrant to between October 2016 and Jan. 20, 2017, as reported by Reuters.

Following the ruling, Aghaian reiterated his warning that turning over the requested information could cause a chilling effect. "Providing the information outright to the government for the government to review and identify who the individuals are and what they said in relation to political expression, speech and exercising their right of association is entirely problematic," Aghaian said in a statement following the hearing.

Paul Alan Levy of Public Citizen, a Washington, D.C. non-profit consumer rights advocacy group representing several people who visited the www.disruptj20.org, was also critical of the ruling. "The mere revealing of the identities to government agents, even under the strictures that [the judge] has provided for, is problematic," Levy told *Politico* on August 24. "This is a president who has shown he has no tolerance for dissent and is perfectly willing to allow extrajudicial means and extralegal means to be used to suppress dissent.. . . If you're somebody who is communicating in opposition to the president, I think you have to be worried about being disclosed to a government agency."

On Sept. 15, 2017, Morin wrote an additional order after DreamHost and the government failed to provide, in their proposed orders, "any explanation regarding how the government will conduct its search without reviewing identifying information of innocent parties associated with the website" *In Re DreamHost*, 2017 WL 4169713 (2017). Morin indicated that he had "anticipated the government would have included procedures, or at least a methodology, by which this minimization would occur" and, as a result, wrote the order to further explain his concerns, instructions, and recommendations to the government.

Morin first discussed the Fourth Amendment's requirement that the seizure of materials protected under the First Amendment must be applied with "scrupulous exactitude," citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). He explained that D.C. Superior Court has authorized a "two-step process" by which law enforcement may conduct 'a later [off-site] review of the media or information consistent with the warrant'" when dealing with the search and seizure of electronic evidence where evidence of a criminal offense is intermingled with unrelated data or information. Various courts, according to Morin, have ruled that "additional safeguards on electronic search warrants may be reasonable and appropriate to limit the possibility of abuse by the government." Therefore, Morin concluded that "[b]ecause of the potential breadth of the government's review, . . . it is appropriate to order additional protections based on the First Amendment considerations of innocent third-parties at issue in this case."

Consequently, Morin discussed minimization "options" that the government should consider, including first a "General Review . . . of the data and information [by the government] to determine the procedures it will employ to minimize the data and information not within the scope of the Warrant." Morin provided several factors the government must consider regarding the General Review, including "(i) limiting the review to metadata such as document dates, custodians, filenames, logs, and other non-content information; (ii) identifying the individuals who will be involved in or authorized to conduct this review . . .; (iii) the process for ensuring that the General Review guidelines are followed; and (iv) a general timeline for completion of the General Review."

After completing the General Review, the government was next required to "file a report with the Court explaining (i) the process the government will use to conduct a detailed review of the data and information, (ii) the procedures the government will implement to minimize the review of data and information not within the scope of the Warrant, and (iii) . . . the government's plan for removing from its possession all data and information not within the scope of the warrant." The purpose of this stage, according to Morin, is to ensure innocent third-parties' rights are not violated, especially "when core First Amendment rights are at issue."

Finally, Morin wrote that the government can then conduct its review of the data after the plan is approved by the court. Upon completing the search, the government must: "(i) file with the Court an itemized list of the data and information that the government believes falls within the scope of the Warrant and the specific reason(s) the government believes that each individual item(s) of data and information falls within the scope of the Warrant; (ii) permanently remove from its possession any data or information outside the scope of the Warrant; and (iii) not distribute, publicize, or otherwise make known to any other person or entity . . . the data and information that is outside the scope of the Warrant." Morin's full order is available online at: https://static.reuters.com/resources/media/editorial/20170929/In%20re%20DreamHost.pdf.

On October 10, Morin ordered DreamHost to redact identifying information of visitors to www.disruptj20.org, who "communicated through, or interacted with, the website," further limiting the DOJ's warrant. *In Re DreamHost*, No. 17 CSW 3438 (2017). According to the *Los Angeles Times* on the same day, the DOJ could not obtain information identifying individuals who interacted with the website until investigators, and the court, demonstrated that it was evidence of criminal activity. Additionally, Morin reiterated that the government must adhere to several safeguards, including filing a report with the court explaining the search protocol and review procedures.

Morin explained that the protection of First and Fourth Amendment rights requires additional safeguards. "Because of

Search Warrants, *continued on page 6*

Search Warrants, *continued from page 5*

the potential breadth of the government's review in this case, the Warrant in its execution may implicate otherwise innocuous and constitutionally protected activity," he wrote. "As the Court has previously stated, while the government has the right to execute its Warrant, it does not have the right to rummage through the information contained on DreamHost's website and discover the identity of, or access communications by, individuals not participating in alleged criminal activity, particularly those persons who were engaging in protected First Amendment activities."

Morin's ruling still compelled DreamHost to provide other information about www.disruptj20.org, as reported by *Politico* on October 10. Additionally, Morin indicated that he would not stay the ruling for a potential appeal. "Given the unprecedented level of participation by a service provider, DreamHost, in making suggestions to the Court to ensure that the identities of innocent visitors to the website are protected, the Court will deny any request to stay this order absent any additional showing," he wrote. The full order is available online at: http://www.politico.com/f/?id=0000015f-0808-d01e-a35f-ff4ee0bd0003.

In a statement following the ruling, DreamHost's general counsel Christopher Ghazarian said, "We're happy to see significant changes that will protect the constitutional rights of innocent internet users. Under this order, we can redact all identifying information and protect the identities of users who interacted with disruptj20.org.. . . The new order is a far cry from the original warrant we received in July. Absent a finding by the Court that probable cause of criminal activity exists, the government will not be able to uncover the identities of these users."

Levy also praised the ruling in an interview with *Politico*. "I'm pleased that the judge adopted our more expansive and protecting definition of what identifying information has to be withheld from disclosure. That's really very important," Levy said.

EFF's Andrew Crocker agreed. "We're pleased to see the court exercise appropriate caution before allowing the government access to information held by DreamHost," Crocker told *Politico*. "The court recognized the serious First Amendment interests raised by the government's attempts to identify communications belonging to ordinary users of disruptj20.org without any evidence that these users are connected to its investigation. Allowing DreamHost to redact this information and requiring the government to articulate its search protocols are excellent first steps to preserving these users' First Amendment rights."

In an October 10 blog post titled "The End of the Road," DreamHost announced, "We do not intend to appeal the court's ruling." DreamHost explained that there was "really no need" because "[a]ny sweeping requests for data that could personally identify website visitors not directly related to an ongoing criminal investigation are now off the table." DreamHost added, "The law makes it clear that the Department of Justice does have a right to request some customer information throughout the course of ongoing criminal investigations. We respect that right and appreciate the court's oversight in this case as a step to help protect users and reign in what we considered to be a problematic, overly-broad records request."

ACLU Files Motion Against "Manifestly Overbroad" DOJ Search Warrants Targeting Facebook; Judge Limits the Scope of the Warrants

On Sept. 28, 2017, the American Civil Liberties Union (ACLU) filed a motion in the Superior Court of the District of Columbia, Criminal Division seeking to quash or narrow three search warrants filed by the U.S. Department of Justice (DOJ) in February. The warrants requested information concerning three Facebook accounts linked to riots in Washington, D.C. during President Donald Trump's Jan. 20, 2017 inauguration. The warrants also sought the names and personal information of 6,000 users who "liked" DisruptJ20, an anti-Trump Facebook page operated by one of the users identified in the warrants. On October 13, the DOJ dropped its request for the names of those 6,000 users who had liked the page. Finally, in a November 9 opinion, District of Columbia Superior Court Chief Judge Robert Morin required the DOJ to follow several procedural safeguards to "ensure that the identities of innocent persons [and third parties were] not revealed." Morin also limited the warrants by requiring Facebook to redact the personally identifying information of all third parties tied to the three accounts.

On January 20, protests during President Trump's inauguration resulted in injuries of six police officers, according to *The Washington Post* on July 8. The riots caused tens of thousands of dollars of damage and led to charges against 234 people for felony rioting charges.

On Feb. 9, 2017, Superior Court of the District of Columbia Judge Ronald P. Wertheim signed three search warrants filed by the DOJ against three Facebook accounts: the Disruptj20 page owned by Emmelia Talarico, and personal accounts lacymacauley, owned by Lacy MacAuley, and legba.carrefour, owned by Legba Carrefour.

The DOJ asked Facebook to disclose "[a]ll contact and personal identifying information, including full name, birth date, gender, email addresses, passwords, security questions and answers, physical address (including state, and zip code), telephone numbers, screen name, hometown, occupation, and websites" tied to the Facebook accounts. The warrants also sought IP addresses and any "profile information; News Feed information; status updates; links to videos, photographs, or other web content; Notes; Wall postings; Comments; Friend lists . . . [and] electronic communications and messages." Additionally, the DOJ requested "basic subscriber records and login history . . . for any other Facebook account(s) that have ever been associated or linked to the [accounts]." Facebook was required to disclose the information from a 90-day period between Nov. 1, 2016 through February 2017.

The warrants also listed information to be seized by the DOJ, including "[a]ny message, photo, video, or other communication or recording which depicts, describes, or otherwise relates to the rioting or inciting to riot activity on January 20, 2017," as well as any information "to identify and locate the perpetrators" of the riots, among other information. The full warrants are available online at: https://www.acludc.org/sites/default/files/field_documents/facebook_search_warrant.pdf.

On September 28, the ACLU filed a motion to quash or narrow the search warrants, contending that they were overbroad and failed the Fourth Amendment's particularity requirement for three reasons. First, the ACLU explained that the Fourth Amendment requires "not only that a warrant describe the specific place to be searched and items to be seized but that the specifications are not so expansive and overly broad as to render the scope of the search akin to that permitted by a general warrant." The motion argued that the warrants constituted "government scrutiny of individuals' political speech and associations," creating a chilling effect of individuals' political speech and other First Amendment freedoms. Thus, the ACLU contended that the warrants

required a "special 'exactitude'" because they implicated the exercise of First Amendment rights."

Second, the motion stated that searches of electronic information raise "special privacy concerns given the breadth and quantity of personal and expressive/associative material individuals can store electronically." The ACLU argued that searching an individual's social media is "the 21st century equivalent of reading every letter the person ever sent, listening to every phone call the person ever made, and viewing every photograph the person ever took." Therefore, a warrant that "gives the government carte blanche to acquire the entire contents of an electronic device or digital account" creates a threat to privacy by exposing "deeply personal and expressive/associational material," as well as information outside the scope of the warrant.

Finally, the ACLU contended that the disclosure of the information requested by the DOJ "would paint a detailed picture both of intimate aspects of the Intervenors' lives and of their political and associational activities." Furthermore, the government would "[learn] something about the political predilections of approximately 6,000 people" who liked the anti-Trump Facebook page. The warrants, the motion argued, would therefore "obviously chill protected speech and associational activities, particularly activities associated with dissenting viewpoints." Thus, the ACLU argued that the warrants did not provide for a "particularized search," but instead a "classically overbroad fishing expedition or 'exploratory rummaging'" in violation of the First and Fourth Amendments.

Consequently, the ACLU proposed that if the court declined to quash the warrants, that it should limit the warrants by imposing procedural safeguards. The ACLU cited Morin's September 15 order regarding DreamHost in which he ruled that "additional safeguards on electronic search warrants may be reasonable and appropriate to limit the possibility of abuse by the government." *In Re DreamHost*, 2017 WL 4169713 (2017). Therefore, the ACLU proposed "the engagement of a special master to review and identify information that the government is authorized to seize under the warrants" because it would provide a neutral party that "would have no ancillary investigative incentive to linger over private material but instead could proceed directly and most efficiently to the identification of relevant material." The ACLU's full motion is available online at: https://www.acludc.org/sites/default/files/field_documents/facebook_targets_motion_to_quash.pdf.

In a statement, senior staff attorney at the ACLU for the District of Columbia Scott Michelman wrote, "Opening up the entire contents of a personal Facebook page for review by the government is a gross invasion of privacy.. . . Moreover, when law enforcement officers can comb through records concerning political organizing in opposition to the very administration for which those officers work, the result is the chilling of First Amendment-protected political activity."

On October 13, *Gizmodo* reported that the DOJ had dropped its request for the names of 6,000 users who liked the anti-Trump Facebook page. The DOJ also narrowed the warrants by excluding a list of friends of the individual accounts, as well as limiting the range of the photographs sought in the warrant to between January 20 and Feb. 9, 2017. "The best aspect of the hearing was the judge clearly seemed to understand that the government asked for more than it needed," ACLU's District of Columbia branch senior staff attorney Scott Michelman told *Gizmodo* after the hearing. "Ultimately, I think the question will be what kind of limits the judge orders."

> "[W]hen law enforcement officers can comb through records concerning political organizing in opposition to the very administration for which those officers work, the result is the chilling of First Amendment-protected political activity."
>
> **— Scott Michelman, ACLU for the District of Columbia senior staff attorney**

In a November 9 opinion, Judge Morin further limited the three search warrants. He contended that "[g]iven the potential breadth, the Warrants in their execution may intrude upon the lawful and otherwise innocuous online expression of innocent users," therefore "implicating the privacy and First Amendment rights of the account holders and other third parties who interacted or communicated with the targeted accounts." Morin wrote that the court "deem[ed] it appropriate in this case to implement procedural safeguards to preserve the First and Fourth Amendment freedoms at stake and ensure that only data containing potential incriminating evidence is disclosed to the government."

Morin consequently proposed several procedural safeguards, similar to those he outlined in the similar context of the DreamHost case. Regarding the DisruptJ20 Facebook page, Morin ruled that the DOJ must first file a report with the court "explaining the government's intended search protocols" in order to uncover only the data included in the warrant. Second, the government "may only conduct its search on a redacted data set that omits non-account holder identifying information." Third, the government must file an additional report after completion of the search, including an itemized list of materials "it believes evidences a violation of D.C. Code." Finally, the government may only obtain un-redacted information if the court finds that "the requested information is evidence of criminal activity."

Regarding the individual accounts named in the other two warrants, Morin found that the government had "established probable cause to believe that criminal activity [was] likely to be found in the individual accounts" of Lacymacauley and Legba.Carrefour, meaning the government was "entitled to review the material and determine [whether] . . . there is evidence of criminal activity." However, because the alleged evidence was likely "intermingled with unrelated information," Morin ordered Facebook to "redact any identifying information of persons whom Facebook Messenger communications are sent, persons who liked or friended a particular account holder, and other information not directly related to an account holder." Morin also ruled that Facebook redact the identities of the 6,000 users who liked the DisruptJ20 Facebook page, particularly because the DOJ dropped their request for the information. After the DOJ had reviewed the redacted information, it was required by Morin to file with the court any request for non-redacted identifying information. Morin further ruled that the government must "permanently delete from its possession any data that does not fall within the scope of the warrants" and that the government must not make known any data or information outside the warrants. Morin's full ruling is available online at: https://www.acludc.org/sites/default/files/field_documents/11-9-2017_dc_superior_ct_order.pdf.

According to *Gizmodo* on November 13, Morin rejected the ACLU's suggestion that a neutral third party review the

Search Warrants, *continued on page 8*

Search Warrants, *continued from page 7*

material prior to it being turned over to the government. Michelman said in a November 9 statement, "The court agreed to impose safeguards to protect political activity and third-party communications from government snooping, but was not equally careful to protect our clients' private and personal communications."

As the *Bulletin* went to press, no further legal actions had been announced.

When Facebook was initially served the search warrants in February 2017, they were accompanied by a gag order, which prevented the company from alerting the users of the accounts named in the warrants that the DOJ was seeking their information. However, *BuzzFeed News* and *Engadget* reported on September 13 that a court filing confirmed that the government had dropped the gag order.

In an October 2017 statement, a Facebook spokesperson wrote, "Last month, we successfully fought to be able to notify the three people whose broad account information was requested by the government. Now that they have exercised their rights to contest the government's warrants, we believe their arguments deserve a fair and full hearing."

Ninth Circuit Ruling Prompts Two *Amici* Briefs Opposing Gag Orders on Electronic Communication Service Providers

On July 17, 2017, the U.S. Court of Appeals of the Ninth Circuit upheld the constitutionality of 18 U.S.C. § 2709(a),(c), which authorizes the Federal Bureau of Investigation (FBI) "to prevent a recipient of a national security letter (NSL) from disclosing the fact that it has received such a request." An NSL is an "administrative subpoena issued by the FBI to a wire or electronic communication service provider which requires the provider to produce specified subscriber information that is relevant to an authorized national security investigation." The ruling led to two separate *amici* briefs by media advocates and experts on Oct. 12, 2017. The Floyd Abrams Institute for Freedom of Expression at the Yale Law School (Abrams Institute) and 20 First Amendment scholars, including Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley, filed an *amici* brief contending that NSL nondisclosure orders constitute prior restraints, which are "universally recognized to be 'the most serious and the least tolerable infringement on First Amendment rights,'" citing *Neb. Press Ass'n v. Stuart*, 427 U.S. 539 (1976). The Reporters Committee for Freedom of the Press (RCFP), along with 20 media organizations, filed a separate *amici* brief on the same day, in which they also contended that the nondisclosure orders constitute prior restraints, and further criticized the Ninth Circuit's ruling as "threaten[ing] to erode press freedom in reporting on government surveillance."

In its July 17 ruling, the Ninth Circuit held that "18 U.S.C. § 2709(c) is a content-based restriction on speech that is subject to strict scrutiny," which requires the government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest. However, the Ninth Circuit found that the nondisclosure requirement of the statute "withstands such scrutiny." *In re National Security Letter*, 863 F.3d 1110 (9th Cir. 2017). Judge Sandra Segal Ikuta wrote for the unanimous court, which concluded first that national security was a compelling government interest, citing *Holder v. Humanitarian Law Project*, in which the U.S. Supreme Court found that "[e]veryone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order." 561 U.S. 1, 28 (2010).

Next, the court concluded that the statute was narrowly tailored for two reasons. First, Ikuta contended that the statute "does not authorize the government to issue a nondisclosure requirement based on a mere possibility of harm." Instead, Ikuta found, the statute requires "a high ranking official [to] certify that disclosure 'may result' in one of four enumerated harms" provided by the statute, including "(i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person." Therefore, the statute "imposes narrow, objective, and definite standards on the government before it can issue a nondisclosure requirement."

Second, the statute requires the FBI "to reassess the necessity of nondisclosure on two occasions: three years after an investigation is begun and upon the closing of an investigation," according to Ikuta. Additionally, under the statute, a court "may require the government to justify the continued necessity of nondisclosure on a periodic, ongoing basis, or may terminate the nondisclosure requirement entirely if the government cannot certify that one of the four enumerated harms may occur." Ikuta found these considerations of the statute address "any constitutional concerns regarding the duration of the nondisclosure requirement."

Before concluding, Ikuta contended that "[r]ather than resembling a censorship or licensing scheme, the NSL law is more similar to governmental confidentiality requirements that have been upheld by the courts." She continued, "The NSL law does not resemble these government censorship and licensing schemes. It neither requires a speaker to submit proposed speech for review and approval, nor does it require a speaker to obtain a license before engaging in business. Rather, the NSL law prohibits the disclosure of a single, specific piece of information that was generated by the government: the fact that the government has requested information to assist in an investigation addressing sensitive national security concerns."

In an Oct. 12, 2017 *amici* brief in support of a petition for rehearing and rehearing *en banc*, the Abrams Institute and the First Amendment scholars contended that the Ninth Circuit had "erred in concluding that the NSL gag scheme more closely resembles a 'governmental confidentiality requirement' than a 'government censorship and licensing scheme.'" *Under Seal v. Sessions*, No. 16-16067 (9th Cir. 2017).

The brief primarily argued that the NSL gag orders "exhibit all of the chief traits of prior restraints," including first that "they constitute a 'previous restraint upon publication' rather than post hoc penalty" as outlined in *Near v. Minnesota*, 283 U.S. 697, 713-14 (1931). The Floyd Abrams Institute and the First Amendment scholars explained that communications companies, including Facebook, Google, and others, "are the major media organizations of the 21st century, but the NSLs they receive forbid them to 'say what they wanted to say' in public."

Second, the brief contended that the NSL gag orders are "overly broad" and "content-based" because companies "cannot explain to their customers and fellow citizens how NSLs are being used or what kinds of records the FBI is sweeping up with its NSL authority—and cannot describe the kinds of information the FBI considers subject to warrantless search using an NSL." Furthermore, the NSL gag orders "also suppress discussion about the policy and legal rationales supporting or undermining the gag order scheme itself." Therefore, the brief concluded that the Ninth Circuit had properly ruled that 18 U.S.C. § 2709(c) is a content-based restriction on speech, making it subject to the strict scrutiny standard.

Third, the Abrams Institute and First Amendment scholars argued that the

gag orders "vest significant discretion to suppress speech in the executive branch" because the statute "grants officials broad discretion to suppress speech prior to any judicial review, heightening the risk of 'government censorship.'" Finally, the brief noted that the NSL gag orders "still appear to be permanent or indefinite," which, according to the brief, are "classic aspects of prior restraints."

Also on October 12, RCFP and 20 media organizations, including the First Amendment Coalition, *The New York Times*, and *The Washington Post*, filed an *amici* brief supporting a petition for rehearing and rehearing *en banc* challenging the constitutionality of 18 U.S.C. § 2709(a),(c), specifically that it "empowers the government to preemptively gag a wire or electronic communication service provider from speaking about the government's request for information about a subscriber under its "nondisclosure requirement."

The brief first provided a detailed explanation of "First Amendment law's 'demanding standard for prior restraint.'" The brief emphasized *New York Times v. United States*, also known as "The Pentagon Papers Case," in which the U.S. Supreme Court held that the government could not issue a prior restraint against newspapers that sought to publish classified documents after they received the information from someone who illegally photocopied the documents. 403 U.S. 713 (1971). According to the brief, in prior restraint cases, courts apply "exacting review to any prior restraint that inhibits core First Amendment activity, such as speech and news reporting on matters of public concern."

Second, the RCFP and media organizations' brief was critical of Ninth Circuit's July 2017 ruling, including that the court did not apply "exacting scrutiny" but instead concluded that "narrow tailoring is not perfect tailoring."

The brief also contended that the ruling would have "detrimental effects for the free press and public debate." The brief argued that the court's approach of characterized speech about NSLs "not as speech of significant public concern, but rather as 'a single, specific piece of information'" was problematic because it "fail[ed] to consider the importance of robust public debate about national security and threaten[ed] to erode press freedom in reporting on government surveillance, one of the key controversies of our time." Furthermore, the nondisclosure requirement "restricts public discourse by silencing NSL recipients who wish to inform the press and the public about government surveillance" and does not allow individuals and companies to "engage in meaningful debate about the subject." Therefore, according to the brief, "as long as NSL recipients are prevented from disclosing the existence of NSLs, the press is unable to fulfill its constitutionally-recognized role of keeping the public informed about government activities." The full *amici* brief is available online at: http://www.newsguild.org/mediaguild3/wp-content/uploads/2017/10/Amicus-Brief-101217-.pdf.

As the *Bulletin* went to press, no further legal proceedings had been announced.

DOJ Limits Gag Orders on Companies Required to Hand Over Customer Data

On Oct. 19, 2017, Deputy Attorney General Rod J. Rosenstein approved a U.S. Department of Justice (DOJ) memorandum that significantly limited the imposition of gag orders by the federal government barring technology companies from informing their customers that their electronic information, such as emails and other records, were turned over to the government pursuant to a subpoena. The memorandum "provide[d] guidance and direction for [DOJ] attorneys and agents seeking protective orders pursuant to 18 U.S.C. § 2705(b) of the Stored Communications Act (SCA)." Following the changes to the gag order policy, Microsoft announced in an October 23 blog post that it was dropping its lawsuit against the DOJ in which it had asked a federal judge to strike down the portions of the SCA, a provision of the Electronic Communications Privacy Act (ECPA), allowing the protective orders.

On October 19, multiple news agencies reported that Rosenstein had approved new guidelines limiting the use of gag orders by the DOJ against technology companies. The memorandum included three key provisions, including first that the guidance "applies prospectively to all applications seeking protective orders, including both new orders and renewals, filed on or after 30 days of the date this memorandum is issued." Second, the memorandum stated that technology companies will only be "prohibited from voluntarily notifying their users of the receipt of legal process under the [Stored Communications Act (SCA)] . . . if the government obtains a protective order under [Section 2705(b)]" of the SCA. Finally, any gag orders under Section 2705(b) must "have an appropriate factual basis and . . . should extend only as long as necessary to satisfy the government's interest."

Next, the memorandum listed several steps that government prosecutors must follow when applying the gag orders. First, the new guidelines required that prosecutors "conduct an individualized and meaningful assessment regarding the need for protection from disclosure . . . and only seek an order when circumstances require."

Second, prosecutors were required to identify "factors justifying the protection from disclosure." For example, prosecutors could identify "the risk of flight or harm to public safety" or that the "data sought by the government related to the investigation may be destroyed or made inaccessible" in order to justify preventing technology companies from disclosing to its consumers that their information was being requested and/or transferred.

Third, the new guidance allowed prosecutors to seek a single protective order that would cover multiple grand jury subpoenas issued as part of the same investigation. However, an order for multiple items "[could] be sought only if the facts justifying protection from disclosure are the same for all items of process covered by the order."

Finally, the memorandum required that prosecutors filing Section 2705(b) applications "only seek to delay notice for one year or less," except in exceptional circumstances. In those cases, extensions of equal or less duration may be requested, provided prosecutors detail "additional, specific facts" regarding the investigation. The memorandum also noted that the DOJ "recognizes that judges may direct shorter or longer periods for orders," as allowed by the SCA. The full document is available online at: https://assets.documentcloud.org/documents/4116326/Protective-Orders.pdf.

In an October 23 statement, DOJ spokeswoman Lauren Ehrsam explained the reasoning behind the changes to DOJ policies. "This update further ensures that the department can protect the rights of citizens we serve, while allowing companies to maintain relationships with their customers by notifying those suspected of crimes, or believed to have information relevant to a crime, in a timely manner that information was obtained relating to their user accounts," she wrote.

In a blog post the same day, Microsoft president and chief legal officer Brad Smith praised the changes. "This is an important step for both privacy and free expression," Smith wrote. "It is an unequivocal win for our customers, and we're pleased the DOJ has taken these

Search Warrants, *continued on page 10*

Search Warrants, *continued from page 9*

steps to protect the constitutional rights of all Americans."

On April 14, 2016, Microsoft had filed a complaint seeking a declaratory judgment in the U.S. District Court of the Western District of Washington after federal courts had "issued nearly 2,600 secrecy orders silencing Microsoft from speaking about warrants and other legal process seeking Microsoft customers' data; of those, more than two-thirds contained no fixed end date" in the previous 18 months. The complaint indicated that Microsoft brought the case "because its customers have a right to know when the government obtains a warrant to read their emails, and because Microsoft has a right to tell them."

In the complaint, Microsoft first criticized the ECPA, specifically Section 2705(b) of the SCA allowing gag orders, because the statute "allows courts to order Microsoft to keep its customers in the dark when the government seeks their email content or other private information, based solely on a 'reason to believe' that disclosure might hinder an investigation." The complaint continued, "Nothing in the statute requires that the 'reason to believe' be grounded in the facts of the particular investigation, and the statute contains no limit on the length of time such secrecy orders may be kept in place."

Second, Microsoft argued that Section 2705(b) was overbroad and violated the First Amendment because it "allow[ed] courts to impose prior restraints on speech about government conduct—the very core of expressive activity the First Amendment is intended to protect— even if other approaches could achieve the government's objectives without burdening the right to speak freely." The complaint noted that the statute "sets no limits on the duration of secrecy orders, and it permits prior restraints any time a court has 'reason to believe' adverse consequences would occur if the government were not allowed to operate in secret." Additionally, application for the orders are based "purely [on] subjective criteria, such as a finding that notice would 'jeopardiz[e] an investigation' in unspecified ways or 'unduly delay a trial.'"

Finally, Microsoft contended that the statute violated the Fourth Amendment because individuals have "a right . . . to know when the government searches or seizes their property," as explained in the Supreme Court case *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995). The complaint included the example of the government entering an individual's home to seize his or her letters from a desk drawer or computer hard drive. In that instance, an individual, "in almost all circumstances, has a right the right to notice of the government's intrusion." However, the complaint argued that Section 2705(b) "subjects Microsoft's cloud customers to a different standard merely because of how they store their communications and data." Microsoft's full complaint is available online at: https://assets.documentcloud.org/documents/2803275/Microsoft-challenges-constitutionality-of-gag.pdf.

> "This is an important step for both privacy and free expression.. . . It is an unequivocal win for our customers, and we're pleased the DOJ has taken these steps to protect the constitutional rights of all Americans."
>
> **— Brad Smith, Microsoft president and chief legal officer**

On Feb. 8, 2017, U.S. District Court Judge James L. Robart granted in part and denied in part a DOJ motion to dismiss Microsoft's lawsuit. Robart found that Microsoft had "adequately support[ed its] claim that Section 2705(b) is unconstitutionally overbroad" under the First Amendment. Specifically, Robart agreed with Microsoft's contentions that Section 2705(b) was overbroad "(1) by permitting nondisclosure orders 'for such period as the court deems appropriate'; (2) by permitting a court to issue a nondisclosure order when the court has 'reason to believe' notification would result in one of five outcomes listed in Section 2705(b); and (3) by allowing a court to issue a nondisclosure order when notification to the target would 'otherwise seriously jeopardiz[e] an investigation or unduly delay[ ] a trial.'" Robart also found that Microsoft had adequately stated a claim that Section 2705(b) orders constitute prior restraints because the statute "allows for indefinite nondisclosure orders, which restrain Microsoft from speaking about government investigations without any time limit on that restraint."

Furthermore, Robart concluded that Microsoft had "alleged sufficient facts that when taken as true state a claim that certain provisions of Section 2705(b) fail strict scrutiny review," which requires the government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest. Robart added that "even if a lesser standard of review [than strict scrutiny] applies to Microsoft's First Amendment claim, Microsoft's allegations support the reasonable inference that indefinite nondisclosure orders impermissibly burden Microsoft's First Amendment rights."

However, Robart ruled against Microsoft regarding its Fourth Amendment claim, concluding that the company "may not bring a claim to vindicate its customers' Fourth Amendment rights." However, Robart seemed to leave the issue open to an appeal. "The source of the court's conclusion is thus the product of established and binding precedent, which precludes the court from allowing Microsoft to vindicate Fourth Amendment rights that belong to its customers," he wrote. "This court cannot faithfully reconcile the broad language of those cases and Microsoft's theory of Fourth Amendment standing on the facts of this case; that task is more properly left to higher courts."

According to *Ars Technica* and *The Verge* on Feb. 9, 2017, Robart's ruling allowed Microsoft's lawsuit to move forward. In a statement, Smith wrote, "We're pleased this ruling enables our case to move forward toward a reasonable solution that works for law enforcement and ensures secrecy is used only when necessary."

However, according to *The Washington Post* on October 24, Smith announced that Microsoft was dropping its lawsuit following the changes to DOJ gag orders against technology companies. In addition to dropping its lawsuit, Microsoft also called on Congress to pass legislation that would limit secrecy orders to 90 days, unless the government seeks renewal, according to *The Washington Post* and the *ABA Journal* on Oct. 24, 2017.

Scott Memmel
Silha *Bulletin* Editor

Federal Judge Blocks Canadian Supreme Court Order Requiring Google to Delist Search Results

On Nov. 2, 2017, Judge Edward J. Davila of the U.S. District Court for the Northern District of California, San Jose Division, granted a motion brought by Google asking that the court prevent enforcement of an order by the Supreme Court of Canada requiring the search engine to delist certain search results that allegedly infringed the intellectual property rights of a British Columbia-based technology company. *Google Inc. v. Equustek Solutions Inc.* No. 5:17-cv-04207-EJD (N.D. Cal. 2017). In a June 28, 2017 ruling, the Supreme Court of Canada had held that Canadian courts have the right to force Google to remove links throughout the world, upholding a lower court ruling that required Google to de-index a small technology distributor globally. *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34 (2017).

PRIOR RESTRAINTS

Google's complaint was not the first attempt by a U.S. search engine to ask a U.S. court to block a foreign court order requiring a search engine to delist or limit some search results. In 2001, a district court judge granted a motion brought by Yahoo! seeking to block a French court's order requiring Yahoo! to filter search results for Nazi-related goods on its auction website. However, the U.S. Court of Appeals for the Ninth Circuit reversed that ruling because neither of the parties bringing the appeal had attempted to enforce the French court's ruling.

The case related to Google arose in 2011 after Equustek Solutions, a small technology company in British Columbia, filed a complaint against Datalink, which acted as a distributor for Equustek's products, for relabeling one of Equustek's products and marketing it as Datalink's own. Despite court orders prohibiting the sale of inventory and the use of Equustek's intellectual property, Datalink left British Columbia, but continued to sell the product from an undisclosed location. Equustek asked Google to "de-index [Datalink]'s websites," which Google refused to do, leading Equustek to seek an order requiring Google to do so.

Google later reported to Equustek that it had de-indexed 345 specific webpages associated with Datalink, but not all of their websites. According to the majority opinion written by Canadian Supreme Court Justice Rosalie Abella, de-indexing the pages, rather than the entire websites, "proved to be ineffective since Datalink simply moved the objectionable content to new pages within its websites, circumventing the court orders. Moreover, Google had limited the de-indexing to searches conducted on google.ca." As a result, on June 13, 2014, Equustek obtained an interlocutory injunction from a Canadian trial court to enjoin Google from displaying any part of Datalink's websites on any of its search results worldwide. The Court of Appeals for British Columbia dismissed Google's appeal.

In October 2016, several U.S. and international organizations intervened in the case, including the Reporters Committee for Freedom of the Press (RCFP), the First Amendment Coalition, the Associated Press (AP), and the Electronic Frontier Foundation (EFF), among others. The organizations proposed a "principled test, with specific requirements, as guidance for Canadian courts when considering the granting of mandatory worldwide injunctions affecting non-parties in foreign jurisdictions, particularly where such orders restrain free expression on the Internet." The brief also invoked the preliminary injunction test in the United States, which requires that "(1) it is likely to succeed on the merits of its claims, (2) it is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities weighs in its favor, and (4) an injunction is in the public interest." Additionally, the brief cited the First Amendment and potential prior restraints in the United States as "tipp[ing] sharply [the scales] in favour of judicial restraint." The full brief is available online at: https://www.eff.org/document/eff-equustek-briefsupreme-court-canada.

In her June 2017 ruling, Justice Abella concluded that a test "determining whether the court should exercise its discretion to grant an interlocutory injunction against Google" had been "met in this case: there is a serious issue to be tried; [Equustek] is suffering irreparable harm as a result of [Datalink]'s ongoing sale of its competing product through the Internet; and the balance of convenience is in favour of granting the order sought."

Abella added that a Canadian court "can grant an injunction enjoining conduct anywhere in the world" when it is necessary to ensure the effectiveness of the injunction. She continued, "The problem in this case is occurring online and globally. The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally. If the injunction were restricted to Canada alone or to google.ca, the remedy would be deprived of its intended ability to prevent irreparable harm, since purchasers outside Canada could easily continue purchasing from [Datalink]'s websites, and Canadian purchasers could find D's websites even if those websites were de-indexed on google.ca." Therefore, the Court concluded that the world-wide injunction was the "only effective way to mitigate the harm to Equustek pending trial." Thus, the Court ordered Google to delist search results related to Datalink worldwide, affirming the lower court's order.

However, Abella noted that the order was not meant "to remove speech that, on its face, engages freedom of expression values, it is an order to de-index websites that are in violation of several court orders.. . . We have not, to date, accepted that freedom of expression requires the facilitation of the unlawful sale of goods."

In a dissenting opinion, Justice Suanne Côté, joined by Justice Malcolm Rowe, listed several factors that "strongly favour judicial restraint in this case," including that the order "has not been effective in making Datalink cease its activities. Although the order may seem to 'reduce the harm to Equustek,' it has been not been effective in doing so." The dissenting opinion contended that there were alternative remedies available to Equustek, such as a world-wide injunction to freeze Datalink's assets in France.

On June 28, 2017, EFF published a statement, which contended that the Canadian Supreme Court's decision "will likely embolden other countries to try to enforce their own speech-restricting laws on the Internet, to the detriment of all users. As others have pointed out, it's not difficult to see repressive regimes such as China or Iran use the ruling to order Google to de-index sites they object to, creating a worldwide heckler's veto." The statement continued,

Google, *continued on page 12*

Google, *continued from page 11*

"The *Equustek* decision is part of a troubling trend around the world of courts and other governmental bodies ordering that content be removed from the entirety of the Internet, not just in that country's locale."

In a June 28 interview with *ZDNet*, University of Ottawa Law Professor Michael Geist provided hypotheticals based on EFF's argument. "[W]hat happens if a Chinese court orders it to remove Taiwanese sites from the index? Or if an Iranian court orders it to remove gay and lesbian sites from the index? Since local content laws differ from country to country, there is a great likelihood of conflicts. That leaves two possible problematic outcomes: local courts deciding what others can access online or companies such as Google selectively deciding which rules they wish to follow," he said.

On July 24, 2017, Google filed a complaint in the Northern District of California asking the court enjoin enforcement of the Canadian order. In its complaint, Google explained that because the Canadian order is an "enforcement order" requiring Google to take actions in the United States, a U.S. Court is "the next venue in [this] battle." Google noted that Equustek's counsel argued before the Canadian Supreme Court that "the enforceability of the Canadian Order 'in the United States is a question for U.S. courts.'" Furthermore, Google alleged that absent a declaration from a U.S. court that the Canadian order is unlawful in the United States, Equustek would "continue to pursue enforcement of the Canadian Order and seek to hold Google in contempt if Google stops complying with it."

Google first contended that enforcement of the Canadian order in the United States would violate the First Amendment. The complaint argued that the order "furthers no compelling interest (nor a substantial interest), and is not narrowly tailored to achieve one." Further, according to the complaint, Equustek could not "show that it has no alternatives available." For example, Equustek had not sought similar injunctions against other search engines, such as Bing or Yahoo!.

Second, Google contended that the Canadian order violated Section 230 of the Communications Decency Act, which states,"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The complaint argued that Google qualified for immunity under Section 230 because Google is as an "interactive computer service." Additionally, Datalink is the information content provider, whereas Google aggregates "snippets from third-party websites such as Datalink's," according to the complaint. However, under the Canadian order, Google is treated as the publisher of the contents of the Datalink websites and is required to "exclude material that third parties have posted online."

> "[The Canadian Supreme Court's decision] will likely embolden other countries to try to enforce their own speech-restricting laws on the Internet, to the detriment of all users. As others have pointed out, it's not difficult to see repressive regimes such as China or Iran use the ruling to order Google to de-index sites they object to, creating a worldwide heckler's veto."
>
> **— June 28, 2017 Electronic Frontier Foundation statement**

Finally, Google contended that enforcement of the Canadian order "trespasses on comity." The complaint explained that "a foundational principle of jurisprudence that each country is the master of its own territory." The complaint continued, "Foreign courts therefore ordinarily refrain from issuing worldwide injunctions because they only have jurisdiction to prescribe conduct that, wholly or in substantial part, takes place within or affects their own territories." Google argued that the Canadian order "is repugnant to United States public policy surrounding the First Amendment and the immunity against imposing liability on interactive computer service providers." Google further argued that the Canadian order is "repugnant to United States public policy because it issued an injunction against Google, an innocent non-party, merely for the sake of 'convenience' . . . [and] did not come close to satisfying well-settled United States law for imposing injunctions." Therefore, according to Google, the order "purports to place the Canadian court in the position of supervising the law enforcement activities of a foreign sovereign nation (the United States) against the United States' own citizens on American soil," requiring "corrective action" by a U.S. court.

Under each cause of action, Google contended that it had "suffered and, if Defendants' conduct is not stopped, will continue to suffer, irreparable injury absent injunctive relief." Google also noted that it was complying with the Canadian order "until such time as this Court affords relief."

On Nov. 2, 2017, Judge Davila granted Google's motion seeking preliminary injunctive relief that would prevent enforcement of the Supreme Court of Canada's order. Davila explained that the party seeking a preliminary injunction must establish that "(1) it is likely to succeed on the merits of its claims, (2) it is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities weighs in its favor, and (4) an injunction is in the public interest."

Davila first addressed the likelihood that the injunction would succeed on its merits. He found that Google had qualified for immunity under Section 230 of the Communications Decency Act. Davila cited three reasons, including that the search engine is an "interactive computer service [provider]," that Datalink provided the information at issue, rather than Google which indexed the information, and that the Canadian order held Google "liable as the 'publisher or speaker' of that information."

Second, Davila held that Google was harmed "because the Canadian order restricts activity that Section 230 protects." Third, Davila found that "the balance of equities favors Google because the injunction would deprive it of the benefits of U.S. federal law," though he did not elaborate further on his reasoning.

Finally, Davila found that the injunction would serve the public interest because "Congress recognized that free speech on the internet would be severely restricted if websites were to face tort liability for hosting user-generated content." Congress' response was to enact Section 230 of the

Communications Decency Act, which states, "The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity . . . It is the policy of the United States . . . to promote the continued development of the Internet and other interactive computer services and other interactive media [and] to preserve the vibrant and competitive free market that presently exists for the Internet." Therefore, Davila argued that the Canadian order "threaten[ed] free speech on the global internet" and "would eliminate Section 230 immunity for service providers that link to third-party websites." Davila's full ruling can be found online at: https://www.eff.org/files/2017/11/02/2017-11-02_order_granting_dckt_47_0.pdf.

In a November 3 statement, EFF legal director Corynne McSherry and staff attorney Vera Ranieri quoted the Canadian Supreme Court's ruling, which stated that "[i]f Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly." McSherry and Ranieri contended that Davila's order provides Google that evidence. Thus, according to the statement, Google could next "seek a permanent injunction and take Judge Davila's order back to British Columbia and ask the court to modify the original order."

McSherry and Ranieri added, "The California ruling is a ray of hope on the horizon after years of litigation, but it is far from a satisfying outcome. While we're glad to see the court in California recognize the rights afforded by Section 230 of the Communications Decency Act, most companies will not have the resources to mount this kind of international fight. If the current trend continues, many overbroad and unlawful orders will go unchallenged. Courts presented with a request for such an order must step up and require plaintiffs to meet a high burden – including proving that the requested order doesn't run contrary to the rights of everyone it will affect."

As the *Bulletin* went to press, no further legal proceedings had been announced.

Google's complaint was not the first attempt by a U.S. search engine to have a U.S. court block a foreign court order requiring a search engine to delist or limit some search results. In November 2000, a French court ruled that Yahoo! had to put a filtering system in place to prevent French users of its search engine from gaining access to Nazi-related goods on its auction site. The ruling upheld a May 2000 ruling that found Yahoo! had violated French anti-racism laws, including Section R645-2 of the French Criminal Code. Free speech and internet experts contended that the case set a dangerous precedent because it allowed a country to impose an order on another nation.

"The California ruling is a ray of hope on the horizon after years of litigation, but it is far from a satisfying outcome. While we're glad to see the court in California recognize the rights afforded by . . . the Communications Decency Act, most companies will not have the resources to mount this kind of international fight. If the current trend continues, many overbroad and unlawful orders will go unchallenged."

— Electronic Frontier Foundation legal director Corynne McSherry and staff attorney Vera Ranieri

Yahoo! sought a declaratory judgement in the District Court of Northern California, the same court as Google's 2017 complaint, blocking the French order, claiming it was not enforceable in the United States. The search engine contended that it could not fully comply with the French order without banning Nazi material from its website and search results altogether, thereby barring U.S. users from seeing it, infringing on their First Amendment rights.

On Nov. 7, 2001, Judge Jeremy Fogel granted Yahoo!'s motion, finding that the French order was not enforceable in the United States. *Yahoo! Inc. v. La Ligue Contre Le Racisme et L 'Antisemetisme*, *169 F. Supp. 2d 1181* (N.D. Cal. 2001). Fogel wrote that although "France clearly has the right to enact and enforce laws such as those relied upon by the French Court here," the French order could not be enforced in the United States consistent with the First Amendment. He wrote, "Internet users in the United States routinely engage in speech that violates, for example, China's laws against religious expression, the laws of various nations against advocacy of gender equality or homosexuality, or even the United Kingdom's restrictions on freedom of the press." The League Against Racism and Anti-Semitism (Ligue Internationale Contre le Racisme et l'Antisemitisme — LICRA) and the Union of Jewish Students (UEJF) filed an appeal with the Ninth Circuit Court of Appeals.

On Aug. 23, 2004, the U.S. Court of Appeals for the Ninth Circuit reversed Fogel's ruling. *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 379 F.3d 1120 (9th Cir. 2004). Judge Warren J. Ferguson, joined by Judge A. Wallace Tashima, found that "no U.S. court can review the decision of the French court in this case because neither LICRA nor UEJF has as yet asked any U.S. court to enforce the French court's ruling."

Judge Melvin Brunetti filed a dissenting opinion, in which he contended that it was not necessary for LICRA and UEJF to attempt to enforce the fines imposed upon Yahoo! by the French court, but that the order to pay the fines itself was enough to establish jurisdiction. He added that because the court did not resolve the present case, the fines against Yahoo! would continue to mount. "The threat to Yahoo! is concrete and growing daily," he wrote. (For more information on *Yahoo! Inc. v. La Ligue Contre Le Racisme et L 'Antisemetisme*, see "Yahoo! Inc. v. LICRA and UEJF" in the Summer 2004 issue of the Silha *Bulletin*, "French Court's Against Yahoo! Not Enforceable in the United States" in the Winter 2002 issue, and "Yahoo! Bans Sales of Nazi Memorabilia After French Ruling" in the Spring 2001 issue.)

Scott Memmel
Silha *Bulletin* Editor

News Organizations and Journalists Face High-Profile Defamation Lawsuits

In the summer and fall of 2017, freelance journalist Yashar Ali, *The New York Times*, *Rolling Stone* magazine, and the mayor of Minneapolis each faced notable defamation lawsuits. Additionally, American Broadcasting Company (ABC) continued to face litigation related to the "pink slime" trial.

DEFAMATION

On August 9, then-Fox News Channel host Eric Bolling filed a $50 million defamation suit against Ali for a story published in *The Huffington Post* regarding sexual harassment allegations. On August 15, the U.S. Court of Appeals for the Fifth Circuit revived a defamation claim by an economics professor against *The New York Times* regarding his quoted statements about slavery. On Aug. 29, 2017, a district court judge ruled in favor of the *Times* in a defamation suit brought by former Alaska Gov. Sarah Palin. On Sept. 19, 2017, the U.S. Court of Appeals for the Second Circuit ruled that two former members of the University of Virginia (UVA) chapter of the Phi Kappa Psi fraternity had adequately shown that defamatory statements in a 2014 retracted *Rolling Stone* magazine story were "of and concerning" the two men, reviving a lawsuit against *Rolling Stone*. On Oct. 11, 2017, Minneapolis Police Lt. John Delmonico filed a complaint against Minneapolis, Minn. Mayor Betsy Hodges, accusing her of defaming him in a text message exchange with then-Minneapolis Police Chief Janeé Harteau. Finally, on Oct. 26, 2017, insurance provider AIG filed a lawsuit against Walt Disney Company (Disney) regarding an insurance policy connected to the August 2017 confidential settlement in the "pink slime" case between American Broadcasting Company (ABC), which is owned by Disney, and Beef Products Inc. (BPI). Disney contended that the settlement should be covered by its $25 million insurance policy while AIG contended that the policy required ABC to obtain written approval from outside counsel before broadcasting its report.

Eric Bolling Files $50 Million Defamation Lawsuit Against Journalist

On Aug. 10, 2017, *The Washington Post* reported that then-Fox News host Eric Bolling had filed a $50 million defamation lawsuit against journalist Yashar Ali, accusing the freelance writer of publishing false and misleading statements about his character in an August 4 article for *The Huffington Post*. Ali's attorney responded that the lawsuit was without merit because it "d[id] not identify which purportedly 'false and misleading' statements could possibly support a $50 million damages award" and defended his client's reporting as uncovering the truth.

While contracted under *The Huffington Post*, Ali wrote an article on August 4 alleging that Bolling sent lewd text messages – including an unsolicited photo of male genitalia – to at least two co-workers at Fox Business and one at Fox News. In the article, Ali reported that he spoke to 14 anonymous sources for the story, and attempted to contact Bolling for information.

Ali also quoted Bolling's attorney Michael J. Bowe, who denied the allegations. "Mr. Bolling recalls no such inappropriate communications, does not believe he sent any such communications, and will vigorously pursue his legal remedies for any false and defamatory accusations that are made," Bowe said.

Adding to the claims against Bolling, in an August 5 Facebook post, Caroline Heldman, an associate professor of politics at Occidental College in Los Angeles, who appeared on the network frequently between 2008 and 2011, accused Bolling of sexual harassment. Heldman alleged that Bolling was one of three Fox News and Fox Business employees who sexually harassed her. Heldman wrote, "My only surprise is that it took this long for people to come forward about Bolling's behavior, which has been wildly inappropriate for years."

The day after Ali's article was published, Fox News Channel released a statement saying that it had suspended Bolling "pending the results of an investigation, which is currently underway."

On August 9, Bolling filed a "summons with notice" in the Supreme Court of New York, County of New York, a trial court, against Ali, seeking $50 million in damages for defamation, as reported by *Politico*. Ali had 20 days to respond and demand that Bolling file a complaint. Bolling would then have 20 days to file his response, according to Politico. The summons read, "The nature of this action is for damages and injunctive relief based on defamation arising from the defendant's efforts to injure the plaintiff's reputation through the intentional and/or highly reckless publication of actionable false and misleading statements about the plaintiff's conduct and character. As a result of the defendant's actions, the plaintiff has been substantially harmed." The full summons with notice is available online at: https://pmcdeadline2.files.wordpress.com/2017/08/bolling-summons-aug-9_redacted-wm_redacted-2.pdf.

After receiving the summons, Ali posted on Twitter that "[i]t's important to note that Bolling's summons does not include *HuffPost* - he is coming after me personally." In a second tweet, Ali wrote, "Not going to stop reporting on Eric Bolling or anyone else. I've had family members killed/jailed in Iran, a lawsuit isn't going to scare me."

In an August 11 letter to Bowe and Fox News executive vice president of legal and business affairs Dianne Brandi, Ali's lawyer Patricia Glaser contended that the lawsuit was without merit because it "does not identify which purportedly 'false and misleading' statements could possibly support a $50 million damages award." She added, "Mr. Ali conducted a thorough investigation and verified his information with 14 independent sources.. . . [T]ruth is always a defense to defamation." Additionally, Glaser called Bolling's suit "a calculated effort to harass and intimidate Mr. Ali personally.. . . Continuing litigation will only reveal that Mr. Bolling's lawsuit was filed for public relations purposes and to retaliate against Mr. Ali for uncovering the truth. Already, Mr. Bolling's suit has tarnished Mr. Ali's reputation and incited Mr. Bolling's supporters to post racist tirades against Mr. Ali on his Facebook Page." The full letter is available online at: http://www.hollywoodreporter.com/thr-esq/eric-bolling-lawsuit-yashar-ali-enlists-power-lawyer-patty-glaser-defamation-fight-1028959.

On Sept. 7, 2017, *Variety* reported that Fox News Channel had cancelled Bolling's show "The Specialist," after the allegations of harassment persisted. The network issued a statement saying that Fox and Bolling agreed to part ways amicably. "We thank Eric for his ten years of service to our loyal viewers and wish him the best of luck," a network spokesperson said in the statement. On Sept. 8, 2017, WPXI News reported that according to Bowe, Fox News' decision to part ways with Bolling would have no effect on the pending defamation suit.

In an August 14 interview with *Salon*, Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley said she was not surprised that Bolling brought the suit. "In this litigious time, where we're

seeing a variety of public figures bring lawsuits against the news media," she said. "I can't say I was really surprised because the revelations were pretty explosive and led to Bolling being suspended. It is not unusual for people in that situation to lash back." Kirtley continued, "It is not unusual for the plaintiff to sue just the writer, frankly as an intimidation move, unless you are talking about a multi-million dollar freelancer. It is not likely that the writer will have resources that a news organization would have, so they are seen as more vulnerable and prepared to settled."

Kirtley added that Bolling, being himself a member of the news media, added a unique twist to the case. "Anybody who is in the media ought to be making a calculation that even if they prevail in a lawsuit like this, there is a possibility that they will result in making really bad legal precedent. It could come back to have an effect on them in the future," she said.

Fifth Circuit Revives Defamation Lawsuit Against *The New York Times*

On Aug. 15, 2017, the U.S. Court of Appeals for the Fifth Circuit revived a professor's defamation lawsuit against *The New York Times* over his quoted statements regarding slavery. *Block v. Tanenhaus*, 867 F.3d 585 (5th Cir. 2017). The court reversed a district court ruling to dismiss the case after the *Times* filed a special motion under Louisiana's anti-strategic litigation against public participation (SLAPP) statute, which allows courts to dismiss defamation suits against defendants who speak out on free speech issues. LSA-C.C.P. Art. 971.

The case arose in January 2014 when *The New York Times* published a front page article about libertarianism and the potential presidential candidacy of Senator Rand Paul (R-Ky.). The story quoted Walter Block, an economics professor at Loyola University and an adjunct scholar at the Mises Institute. According to the Fifth Circuit's *per curiam* opinion, *The New York Times*' article quoted Block twice. The first quote cited him as "one economist" in the context of the statement that some Mises Institute scholars "have championed the Confederacy." The quote read, "one economist, while faulting slavery because it was involuntary, suggested in an interview that the daily life of the enslaved was 'not so bad — you pick cotton and sing songs.'"

The second quote included Block's name and position as a Loyola University economics professor and claimed that he described slavery as "not so bad" and was highly critical of the Civil Rights Act. "Woolworth's had lunchroom counters, and no blacks were allowed," Block was quoted. "Did they have a right to do that? Yes, they did. No one is compelled to associate with people against their will."

Block sued *The New York Times* for defamation in the U.S. District Court for the Eastern District of Louisiana, asserting claims for defamation and false light invasion of privacy, alleging that the *Times* "misrepresented his statements in an article that attributed racist views to libertarian scholars and discussed how ties with libertarian thinkers would impact Senator Rand Paul's potential presidential candidacy." *Block v. New York Times Company*, 200 F.Supp.3d 637 (E.D. La. 2016).

> "In this litigious time, where we're seeing a variety of public figures bring lawsuits against the news media, I can't say I was really surprised [by the lawsuit] because the revelations were pretty explosive and led to Bolling being suspended. It is not unusual for the plaintiff in that situation to lash back."
>
> **— Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley**

The New York Times responded by filing a special motion to strike the lawsuit under Article 971, Louisiana's anti-SLAPP statute. The statute allows a party to bring a special motion to strike "[a] cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States or Louisiana Constitution in connection with a public issue . . . unless the court determines that the plaintiff has established a probability of success on the claim." (For more information on anti-SLAPP statutes, see "Several State Courts and Legislatures Grapple with Anti-SLAPP Laws" in the Summer 2017 issue of the Silha *Bulletin*.)

The trial court granted *The New York Times*' motion, dismissing Block's claims on the ground that he failed to create a genuine issue of fact as to the falsity, fault and defamatory meaning of the statements. Block then appealed the decision to the Fifth Circuit, arguing that there was a genuine issue of fact and that the anti-SLAPP law "is not applicable in federal court because it is procedural and because, even if it is substantive, it is in direct collision with the Federal Rules of Civil Procedure."

On Aug. 15, 2017, the three-judge panel reversed the lower court's dismissal of Block's complaint. The Fifth Circuit first noted that Block had to demonstrate "that there is a genuine issue of material fact as to falsity, fault, and defamatory meaning in order to show that the district court should not have granted the [*Times*'] motion to dismiss under Article 971." Additionally, the court noted that "the applicability of state anti-SLAPP statutes in federal court is an important and unresolved issue in this circuit."

The court agreed with Block's argument that "there is a genuine issue of material fact as to whether [*Times*] distorted the meaning of his statements by omitting crucial context." Block contended that his statements "underscored the importance of free association and condemned chattel slavery precisely because it was involuntary, but that the [*Times*] quoted him out of context to make it appear that he considered chattel slavery 'not so bad.'" The court ruled that omitting context "can distort the meaning of a direct quotation" and, as a result, "there is a genuine fact issue as to whether the article misrepresented Block's statements."

The court also rejected three arguments made by the *Times*. First, the *Times* contended that it was correct in reporting that Block described chattel slavery as "not so bad" because his reference to picking cotton and singing songs "leaves no room for doubt" that he was describing chattel slavery. However, the court found that those statements were not the same as calling chattel slavery "not so bad." Second, the *Times* argued that it had communicated Block's objection to coercion elsewhere in the same story. However, because his name was not used, the court found that "a reasonable reader would not associate the two passages and would not infer that Block . . . is the same person as the unnamed economist." Finally, the court rejected the *Times*' claim that Block's pleading truth "would have had the same 'effect on the mind of the reader' as the message that the article conveyed." The court held that "effect on the mind of the reader" referred to the meaning of the statement conveyed to a reader, not the emotions it incites.

Next, the court found that because Block is a public figure, "the fault element

Defamation, *continued on page 16*

Defamation, *continued from page 15*

of his claims requires proof of actual malice," which requires the journalist acted with knowledge of falsity or reckless disregard of the truth, as defined by the 1964 Supreme Court case *New York Times v. Sullivan*, 376 U.S. 254 (1964). However, the court ruled that because "there is a genuine issue of material fact as to whether [*The New York Times*] altered the meaning of the quotation . . . [the] dismissal for failure to create a fact issue as to actual malice was premature."

Finally, the court discussed defamation under Louisiana law, which states that a "statement is defamatory if it 'ends to harm the reputation of another so as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.'" *The New York Times* did not argue that its description of Block would not harm his reputation, but instead contended that its article "made no such accusation" that Block viewed slavery as "not so bad." However, the court concluded that such a description of Block would negatively affect his reputation and would be defamatory, meaning "dismissal for failure to create a genuine fact issue as to whether the article had a defamatory meaning was premature." Thus, the court reversed the lower court's dismissal under Article 971 and remanded the case for further proceedings.

Danielle Rhoades Ha, a spokesperson for *The New York Times*, said in a statement that the newspaper was "disappointed in the court's ruling but remain[s] convinced that our story was accurate and we will proceed to prove our case before the district court."

Following the ruling, several media lawyers were particularly concerned that the court called the applicability of anti-SLAPP statutes in federal court an unresolved issue in the Fifth Circuit. An Aug. 16, 2017 *Law360* commentary quoted several media attorneys who argued that the circuit had previously recognized Louisiana's anti-SLAPP law and that the ruling opened the door to the possibility that similar state laws, including the defendant-friendly Texas Citizens Participation Act, would not apply in federal court.

Chip Babcock of Jackson Walker LLP told *Law360* that "[t]here are a lot of cases that in the past would have resulted in millions of dollars of legal fees and expenses to speakers, but which have been saved by the anti-SLAPP statute." Babcock added, "In the old days, it used to be that defendants would do anything they could to get to federal court. If the Fifth Circuit doesn't apply the anti-SLAPP statutes, the worm will turn and plaintiffs will try to get into federal court."

Paul Watler of Jackson Walker LLP said he was surprised by the court's comment because the Fifth Circuit had previously applied the Louisiana anti-SLAPP statute in two cases, *Henry v. Lake Charles American Press L.L.C.*, 566 F.3d 164 (5th Cir. 2009) and *Brown v. Wimberly*, 477 Fed.Appx. 214 (5th Cir. 2012). "The outcome of a suit against a media defendant should not turn on whether it's filed in state or federal court. It should turn on the merits of the claim," Watler told *Law360*.

Laura Prather of Haynes and Boone LLP agreed. "I think the Block decision is particularly troubling because it calls into question whether or not the Fifth Circuit has actually applied the Louisiana SLAPP statute in a diversity case," Prather said. "It calls into question something that had been established law and doesn't provide insight into why."

In an August 21 Trademark & Copyright Law commentary, Foley Hoag LLP partner David A. Kluft argued that Block "recklessly decontextualized the suffering of millions to make an intentionally controversial academic point" making it "ironic that he is now suing over four words allegedly taken out of context by someone else." Nevertheless, Kluft wrote that Block "has a triable claim," though he must show that *The New York Times* acted with actual malice.

District Court Judge Dismisses Sarah Palin's Lawsuit Against *The New York Times*

On June 27, 2017, *The New York Times* reported that former vice-presidential candidate Sarah Palin had filed a defamation lawsuit against the *Times*, claiming the newspaper had published a statement about her in a recent editorial that it "knew to be false." On August 29, U.S. District Court for the Southern District of New York Judge Jed S. Rakoff dismissed Palin's lawsuit, finding that her complaint failed to show that the *Times* published inaccurate statements maliciously. *Palin v. The New York Times Company*, No. 17-cv-4853 (S.D.N.Y. 2017).

On June 14, 2017, *The New York Times* published an editorial shortly after left-wing activist James Hodgkinson opened fire on an early morning baseball practice for Republican members of Congress in Alexandria, Va. The editorial connected the 2011 mass shooting by Jared Lee Loughner in Tucson, Az. that killed six people and severely wounded then-Congresswoman Gabrielle Giffords with a map distributed by Palin's political action committee (SarahPAC) in 2010. The editorial said that the map "put Ms. Giffords and 19 other Democrats under stylized cross hairs."

The *Times* later issued a correction, saying that there was no established link between political statements and the shooting. *The New York Times* Opinion Twitter account also sent out the correction, apologizing and saying that it appreciated that readers had pointed out the mistake. Nevertheless, Palin wrote in her lawsuit that the *Times*' response "did not approach the degree of the retraction and apology necessary and warranted by [the *Times*'] false assertion that Mrs. Palin incited murder."

On Aug. 16, 2017, *The New York Times* reported that Editorial Page Editor James Bennet had testified at a hearing that he did not intend to blame Sarah Palin for the 2011 mass shooting, but was trying to make a point about the heated political environment. "I did not intend and was not thinking of it as a causal link to the crime," Bennet said.

On Aug. 31, 2017, Rakoff dismissed Palin's complaint. He first explained that because Palin is a public figure, she had the burden of "establish[ing] by clear and convincing evidence that the *Times* acted with 'actual malice,'" a standard established by the U.S. Supreme Court in *New York Times v. Sullivan* that public officials have to show that news organizations had knowingly published false information or acted with reckless disregard for the truth. 376 U.S. 254 (1964).

Next, Rakoff had to determine whether the editorial statements were "of and concerning" Palin, requiring that "'the allegedly defamatory content refer[s] to the plaintiff' such that those knowing the plaintiff 'understand that [she] was the person meant.'" The *Times* argued that Palin's claim of defamation was directed at SarahPAC, not Palin herself, applying the "group libel doctrine" which provides that a "plaintiff's claim is insufficient if the allegedly defamatory statement referenced the plaintiff solely as a member of the group." However, Rakoff ruled that because the statements referenced a particular member of SarahPAC — Palin herself — the doctrine did not apply and that the statements were "of and concerning" Palin. Third, Rakoff addressed whether the statements were provably false. He noted that "a statement of opinion relating to matters of public concern which does not contain a provably false factual connotation will receive full constitutional protection," citing *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 20 (1990). Rakoff found that "although

the offending paragraphs . . . contain[ed] various assertions of opinion, a reasonable reader could well view them as a factual statement asserting that there was a 'direct link'" between the SarahPAC Map and the Loughner shooting. Rakoff added that Bennet ordered corrections be made after readers complained about the assertions in the editorial, suggesting that readers were "reasonably reading" that, as a factual matter, the map was causally linked to the shooting. Therefore, Rakoff concluded, the link is a factual statement that can be proven false, such as if there is no evidence that Loughner ever saw the map.

Finally, Rakoff considered whether the complaint had adequately alleged actual malice. He concluded that because the complaint "fail[ed] to identify any individual who possessed the requisite knowledge and intent and, instead, attributes it to the *Times* in general," the complaint "fail[ed] on its face" to adequately allege actual malice. He added that because the actual malice standard is "grounded in 'a profound national commitment to the principle that debate on public issues be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials,'" citing *Sullivan*, and that Palin failed to allege specific facts demonstrating actual malice, it is "plain that plaintiff has not and cannot meet this standard."

Additionally, Rakoff conceded that although the *Times* published "a few factual inaccuracies somewhat pertaining to Mrs. Palin," a defamation suit requires much more than publishing a falsehood. "Negligence this may be; but defamation of a public figure it plainly is not," Rakoff wrote. As a result, Rakoff granted the *Times*' motion to dismiss with prejudice.

In an Aug. 29, 2017 statement, *The New York Times* wrote, "We were delighted to see today's decision. Judge Rakoff's opinion is an important reminder of the country's deep commitment to a free press and the important role that journalism plays in our democracy. We regret the errors we made in the editorial. But we were pleased to see that the court acknowledged the importance of the prompt correction we made, once we learned of the mistakes."

Second Circuit Revives Lawsuit against *Rolling Stone*

On Sept. 19, 2017, the U.S. Court of Appeals for the Second Circuit ruled that a district court judge had erred in dismissing a defamation suit brought by three former members of the University of Virginia (UVA) chapter of the Phi Kappa Psi fraternity. *Elias v. Rolling Stone*, No. 16-2465-cv (2nd Cir. 2017). The court ruled that two of the individuals, George Elias IV and Ross Fowler, had adequately shown that defamatory statements in a 2014 retracted *Rolling Stone* magazine story were "of and concerning" the two men. Judge Raymond Lohier filed an opinion concurring in part and dissenting in part, in which he agreed with the majority's ruling regarding Elias and Fowler, but disagreed with the majority's conclusion that the district court erred in dismissing the plaintiffs' small group defamation claim. Just two days before the Second Circuit decision, Jann S. Wenner put his Wenner Media's controlling stake in *Rolling Stone* up for sale, citing "financial pressures."

> "Judge Rakoff's opinion is an important reminder of the country's deep commitment to a free press and the important role that journalism plays in our democracy. We regret the errors we made in the editorial. But we were pleased to see that the court acknowledged the importance of the prompt correction we made, once we learned of the mistakes."
>
> **— Aug. 29, 2017 *New York Times* statement**

Elias, Fowler, and Stephen Hadford's lawsuit followed the controversial 2014 story "A Rape On Campus," written by Sabrina Rubin Erdely, in which she reported on the alleged gang rape of UVA student "Jackie" during a Psi Kappa Psi fraternity party in 2012. On April 5, 2015, the Columbia School of Journalism published a study conducted at the request of *Rolling Stone*. The study found that the magazine had failed to follow ethical and journalistic principles. The magazine summarily retracted the article the same day the study was published. (For more information on "A Rape On Campus" and the Columbia School of Journalism's study, see Rolling Stone *Reaches Settlements in Two Defamation Lawsuits related to 2014 Campus Rape Story* in "*Rolling Stone*, *Daily Mail*, & ABC Reach Settlements in High-Profile Defamation Lawsuits" in the Summer 2017 issue of the Silha *Bulletin*, *Legal Challenges*, *Ethical Questions Linger for* Rolling Stone *over Retracted Campus Rape Story* in "*Rolling Stone* Faces New Reporting Controversy, Continues to Face Questions over Retracted Story" in the Winter/Spring 2016 issue and "News Organizations Backpedal after Failures to Fact Check, Anchor's False Stories" in the Winter/Spring 2015 issue.)

In the spring and early summer of 2017, *Rolling Stone* reached settlements in two additional lawsuits stemming from "A Rape On Campus," including with former UVA Associate Dean of Students Nicole Eramo and the Phi Kappa Psi fraternity itself. (For more information on the settlements, see Rolling Stone *Reaches Settlements in Two Defamation Lawsuits related to 2014 Campus Rape Story* in "*Rolling Stone*, *Daily Mail*, & ABC Reach Settlements in High-Profile Defamation Lawsuits" in the Summer 2017 issue of the Silha *Bulletin*.)

On July 29, 2015, Elias, Fowler, and Hadford filed a separate lawsuit against *Rolling Stone*, Erdely, and Wenner Media for defamation. The plaintiffs alleged that the article and an online podcast appearance by Erdely defamed them by identifying them individually as participants in the alleged rape and identifying them collectively as members of the fraternity at the time the rape allegedly occurred. The defendants filed a motion to dismiss the lawsuit, contending that the plaintiffs had failed to state a claim.

On June 28, 2016, U.S. District Court for the Southern District of New York Judge Kevin P. Castel granted the defendants' motion and dismissed Elias, Fowler, and Hadford's defamation claims. *Elias v. Rolling Stone*, 192 F.Supp.3d 383 (S.D.N.Y. 2016). The plaintiffs appealed the case to the Second Circuit.

On Sept. 19, 2017, Judge Katherine B. Forrest wrote the majority opinion, ruling that Castel had erred in dismissing Elias and Fowler's claims. Forrest wrote that in New York, "[d]efamation is 'the making of a false statement which tends to expose the plaintiff to public contempt, ridicule, aversion or disgrace, or induce an evil opinion of him in the minds of right-thinking persons, and to deprive him of their friendly intercourse in society,'" citing *Foster v. Churchill*, 87 N.Y.2d 774, 751 (1996). In order to state a claim for defamation, a plaintiff must allege "(1) a false statement that is (2) published

Defamation, *continued on page 18*

Defamation, *continued from page 17*

to a third party (3) without privilege or authorization, and that (4) causes harm, unless the statement is one of the types of publications actionable regardless of harm." Significantly, a defamation plaintiff must also allege that the purportedly defamatory statement was "of and concerning" him or her, meaning "'the reading public acquainted with the parties and the subject' would recognize the plaintiff as a person to whom the statement refers."

The court first addressed the dismissal of the plaintiffs' claims regarding the article written by Erdely. Elias, Fowler, and Hadford argued that "they have plausibly alleged that the defamatory statements in the Article were 'of and concerning' them individually." Forrest ruled that "while it is a close call . . . on balance that the complaint plausibly alleged that the purportedly defamatory statements in the Article were 'of and concerning' Elias and Fowler individually." Forrest found that because Elias was a member of the fraternity, graduated in 2013 when the alleged perpetrators graduated, "lived in the fraternity house in the only bedroom on the second floor that was both large enough to fit the description of the alleged location of the rape and easily accessible by non-residents," and was "identified by others as one of the alleged attackers," he had sufficiently pled that the article was "of and concerning" him. Similarly, Forrest ruled that Fowler had alleged the article was "of and concerning" him because he too was a member of Phi Kappa Psi in the class of 2013 and had a prominent role with the fraternity, meaning he would have been part of the initiation ritual alleged by Erdely to be related to Jackie's gang rape.

However, Forrest upheld the dismissal of Hadford's claim because it rested primarily on the fact that he rode his bike through campus, which the court determined was "too speculative" to withstand a motion to dismiss.

The plaintiffs also contended that the defamatory statements in "A Rape On Campus" "were directed at all Phi Kappa Psi members at the time of the alleged rape such that [the] Plaintiffs can maintain a claim for small group defamation." Forrest wrote that in order to evaluate a small group defamation claim, a court must consider "the size of the group, whether the statement impugns the character of all or only some of the group's members, and 'the prominence of the group and its individual members' in the community," citing *Brady v. Ottaway Newspapers, Inc.*, 84 A.D.2d 226 (N.Y. App. Div. 1981). Regarding the size of the fraternity, Forrest concluded that New York court had allowed defamation claims to move forward where "plaintiffs 'numbered at least 53,' the number of members of Phi Kappa Psi at the time of the alleged rape. Next, Forrest concluded that based on the article as a whole, "a reader could plausibly conclude that many or all fraternity members participated in alleged gang rape as an initiation ritual and all members knowingly turned a blind eye to the brutal crimes." At the very least, according to Forrest, "a reader of the article could also plausibly conclude that . . . they all knew that their fraternity brothers had [commited the rape]." Finally, the court concluded that "the size of the university community and the prominence of Phi Kappa Psi on campus support Plaintiffs' theory of small group defamation," which allows members of a group to bring a claim of defamation for statements directed at that group, according to the Digital Media Law Project hosted by the Berkman Klein Center for Internet & Society. Thus, the court ruled that the district court erred in dismissing the former fraternity members' small group defamation claim.

The court next addressed the plaintiffs' appeal of the dismissal of their defamation claim based on the online podcast done by Erdely. Specifically, Forrest focused on two statements: Erdely's claim that the article "seem[ed] to indicate that [Jackie's rape] is some kind of initiation ritual" and her statement that "it seems impossible to imagine that people didn't know about this." Forrest wrote that under New York law, "statements that do not purport to convey facts about the plaintiff, but rather express certain kinds of opinions of the speaker, do not constitute defamation." She concluded that Erdely's podcast statements, although "matters that could be proven or disproven" were "readily identifiable as speculation and hypothesis." Thus, the court upheld the district court's dismissal of the plaintiffs' claims stemming from the podcast. The court remanded the case back to the district court for further proceedings.

Judge Lohier filed an opinion concurring in part and dissenting in part. He agreed with the majority that Elias and Fowler had plausibly alleged that the article could be interpreted as being "of and concerning" them, and also agreed with the majority's dismissal of Hadford's defamation claim.

However, Lohier disagreed with the majority regarding the plaintiffs' small group defamation claim for two reasons. First, Lohier found that the complaint failed to allege that the article referred to "*all* of the fraternity members as complicit either in committing gang rapes or in the knowledge that they routinely occurred" (emphasis in original). Additionally, Lohier found it problematic that the majority accepted the claim that "all the men who were Phi Kappa Psi members at the time the rape purportedly occurred were defamed."

Second, Lohier "[was] not persuaded" by the majority's finding that university campuses are "intimate communities" and that Phi Kappa Psi was sufficiently prominent "on the UVA campus" to support the plaintiffs' group defamation claim. Further, he wrote that he was not convinced that "the [New York] Court of Appeals would adopt the factors set forth in *Brady* . . . rather than some other factors (or even an altogether new test) yet to be devised."

Therefore, Lohier wrote that he had proposed to the other judges that the court "certify the question of small group defamation to the New York Court of Appeals, rather than rely on one New York Appellate Division case, [*Brady*]." He added, "Whether New York defamation law protects them is a policy issue for the New York State courts or legislature to decide, not us."

In a Sept. 19, 2017 statement, *Rolling Stone* wrote, "We are disappointed with the Second Circuit's ruling today, but are confident that this case has no merit." As the *Bulletin* went to press, no further legal action or decisions had been announced.

According to *The Hollywood Reporter* on September 19, the Second Circuit's decision was "unfortunate timing for Jann Wenner," who had put *Rolling Stone* up for sale two days earlier. *The New York Times* reported that Wenner had put his company's controlling stake of the magazine up for sale in response to financial pressures on the magazine's parent company, Wenner Media. The *Times* also reported that the Wenners had recently sold the company's other two magazines, *Us Weekly* and *Men's Journal*. Wenner had also previously sold a 49 percent stake in *Rolling Stone* to BandLab Technologies, a music technology company based in Singapore, according to the *Times*.

Minneapolis Police Lieutenant Files Defamation Lawsuit against Mayor

On Oct. 13, 2017, the Minneapolis *Star Tribune* and the St. Paul Pioneer Press reported that Minneapolis Police Lt. John Delmonico had filed a lawsuit two days earlier against then-Minneapolis Mayor Betsy Hodges, accusing her of portraying him as untrustworthy and racist in a text message exchange with then-Police Chief Janeé Harteau.

The case arose in April 2017 when Hodges and Harteau exchanged a series

of text messages on city-issued cellphones regarding whether to appoint Delmonico as Fourth Precinct inspector. Harteau contended that she had followed the normal appointment process. Conversely, Hodges told Harteau that she should have had more notice regarding to the appointment of Delmonico.

In the text messages, Hodges mentioned that the community around the Fourth Precinct "remembers [Delmonico was] the one who commented on pointergate, and in [the] 4th precinct especially to have that person [be] inspector wont [*sic*] be doing a lot of good for community relationships." "Pointergate" began on Nov. 6, 2014, when KSTP-TV, the local ABC affiliate in Minneapolis, aired a report that showed a picture of Hodges with an African-American man, whose face was blurred, smiling and pointing at each other, a gesture which KSTP reporter Jay Kolls described as "a known gang sign." Kolls did not identify the man in the picture by name, but described him as a "twice-convicted felon for drug selling and possession and illegal possession of a firearm." Critics of the KSTP report argued that Hodges and Navell Gordon, the man in the photo, were simply pointing at each other, and accused KSTP of taking the picture out of context. The KSTP report included an interview with Delmonico in which he said "when you have the mayor of a major city with a known criminal, throwing up gang signs, that's terrible." He added, "As critical as she can be with the cops, is she going to support gangs in the city or cops?" (In December 2014, the Silha Center for the Study of Media Ethics and Law co-sponsored a forum that discussed the ethics behind the KSTP news story regarding "Pointergate." For more information on the event and "Pointergate," see "Silha Center Co-Sponsors Forum on Ethics of 'Pointergate' Broadcast" in the Fall 2014 issue of the Silha *Bulletin*.)

Additionally, Hodges texted Harteau that the community "remember[s] lots of racist stuff [Delmonico] has done" and that his appointment would be "very bad for . . . community trust building." Hodges also sent a text message stating "we can't trust John." The text messages were released after *Star Tribune* and KSTP records requests under the Minnesota Government Data Practices Act (MGDPA), which classified the text messages as "public records." Minn. Stat. § 13.01 *et seq.* The full text message conversation is available online at: http://www.startribune.com/text-messages-show-argument-between-hodges-harteau-over-delmonico-appointment/434298333/.

On April 26, Minnesota Public Radio (MPR) reported that Hodges had blocked Delmonico's appointment and had instead appointed Lt. Aaron Biard to be Fourth Precinct inspector. On July 22, Harteau had resigned after a woman was fatally shot by a Minneapolis Police officer, as reported by multiple news agencies.

On October 11, Delmonico filed a defamation lawsuit in the Fourth Judicial District Court in Hennepin County against Hodges and the City of Minneapolis regarding the text messages depicting Delmonico as being racist and untrustworthy.

The complaint first contended that Delmonico was a private Minnesota resident and "not a public figure," meaning he would not need to prove actual malice, which requires that Hodges acted with knowledge of falsity or reckless disregard of the truth, as defined by the 1964 Supreme Court case *New York Times v. Sullivan*. 376 U.S. 254 (1964).

Nevertheless, in an interview with the *Star Tribune* on October 13, Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley contended that Hodges' comments were likely covered by *New York Times v. Sullivan*. Kirtley explained that if a court found that Delmonico was a public figure, he "would have to prove that whatever Mayor Hodges said was based on actual malice." She added, "If her factual basis is verifiable and she makes her own comments, that is opinion, and that is protected."

The complaint next argued that the statements made by Hodges were "false, libelous, and defamatory, per se" and that they "exposed Delmonico to hatred, contempt, ridicule, and obloquy." The complaint added that Hodges "intentionally or recklessly made [the statements] with malice, hatred, and ill-will toward Delmonico and with a desire to injure him."

Finally, the lawsuit alleged that the defamatory statements "harmed Delmonico's reputation and lowered him in the estimation of his profession and the community in general." The complaint continued, "As a direct and proximate result of the [defamatory statements], Delmonico has suffered damage to his career, reputation, shame, embarrassment, mortification, and mental anguish." Delmonico sought over $50,000 in damages "to be established by proof at trial." The full complaint is available online at: http://www.documentcloud.org/documents/4108064-Read-John-Delmonico-s-lawsuit.html?embed=true&responsive=false&sidebar=false.

As the *Bulletin* went to press, the Hennepin County court had not announced any proceedings stemming from the lawsuit.

In an October 13 statement, Hodges responded to the lawsuit. "As mayor, I have been doing tough, transformational work to earn and build trust between the Police Department and community, especially in the 4th Precinct in North Minneapolis," she wrote. "This is why in April, I overruled then-Chief Harteau when she appointed Lt. John Delmonico to lead the 4th Precinct. I said at the time that while I appreciated Lt. Delmonico's many years of service, and believed that there were many leadership roles for which he could be a good fit, he was not the right fit for the 4th Precinct." She added, Leadership requires making choices and standing by them: I stand by mine."

On the same day, Harteau tweeted, "Not surprised!" In an interview with the *Star Tribune*, Harteau criticized Hodges. "I think the things that she said about Delmonico, not only on the text messages but in other meetings and public forums — about his leadership abilities and relationship with the community — were not only defaming, but inaccurate," Harteau said.

AIG Sues Disney, Denies Insurance Coverage Following Settlement in "Pink Slime" Trial

On Oct. 26, 2017, insurance provider AIG filed a lawsuit against Walt Disney Company (Disney) regarding an insurance policy connected to the August 2017 confidential settlement in the "pink slime" case between American Broadcasting Company (ABC), which is owned by Disney, and Beef Products Inc. (BPI) in which ABC news reports called BPI's Lean Finely Textured Beef (LFTB) product "pink slime." Disney contended that the settlement should be covered by Disney's $25 million insurance policy, and had previously filed a motion in federal court seeking to go before an arbitration panel after AIG denied coverage of the settlement. Conversely, AIG contended that the policy required ABC to obtain written approval from outside counsel before broadcasting its report, despite ABC's claims that such a requirement was outside normal industry practices.

In September 2012, BPI, as well as BPI Technology Inc. and Freezing Machines, Inc., brought a civil action in the Circuit Court of Union County in South Dakota against ABC following a series of broadcast and online stories, as well as several tweets, in March 2012 about BPI's LFTB product, which ABC News repeatedly referred to as "pink slime." BPI claimed that ABC's reporting, as well as reporter

Defamation, *continued on page 20*

Defamation, *continued from page 19*

Jim Avila's tweets related to LFTP, had defamed the company. On June 28, the *Sioux City Journal* reported that ABC had reached a confidential settlement with BPI, raising concerns from media experts that the settlement could embolden potential plaintiffs to file a defamation lawsuit. (For more information on the pink slime trial, the settlement, and concerns from media experts, see *ABC Reaches Settlement with Beef Products Inc. in "Pink Slime" Lawsuit* in "*Rolling Stone*, *Daily Mail*, and ABC Settle High-Profile Defamation Lawsuits" in the Summer 2017 issue of the Silha *Bulletin*.)

In an August 2017 quarterly earnings report, Disney reported a $177 million expense related to the settlement of litigation, according to *The Hollywood Reporter* on August 8. Although the earnings report did not specifically attribute the $177 million expense with the pink slime trial, Disney had reported no other lawsuit in 10-Q reports to shareholders filed with the Securities & Exchange Commission (SEC), as reported by *The Hollywood Reporter*. According to *The Wall Street Journal*'s August 9 interview with a BPI spokesperson, $177 million was not the total settlement amount, but instead what Disney was funding, with insurers reportedly paying the rest. According to *The Hollywood Reporter* on October 27, Disney had insurance policies with Swizz Re, Illinois Union Insurance Company, and Beazley that provided up to $50 million in coverage. The insurance provided by AIG was $25 million "in excess coverage," according to *The Hollywood Reporter*, meaning it provides up to $25 million of insurance for covered claims in excess of the first $50 million in payments.

On October 17, *Variety* magazine reported that Disney had filed a motion in the U.S. District Court for the Central District of California asking AIG to submit to an arbitration panel after AIG denied coverage of the settlement. *Walt Disney Co. v. AIG*, No. 17-07598 (C.D. Cal. 2017). On October 6, Disney's attorney, Marty Myers of Covington & Burling LLP, had written a letter to AIG's lawyers, which read, "It is regrettable that Disney and AIG were not able to come to agreement on further aspects of the arbitration(s)." Myers also warned that litigation would be "frivolous," according to *Variety* magazine.

Michael J. Bowe, AIG's counsel, of the firm Kasowitz Benson Torres LLP responded in an email, "What is regrettable is that you are obviously an untrustworthy liar. Your letter . . . completely misrepresents our discussions. I do thank you though for showing your true colors so that I can proceed accordingly for the remainder of these litigations. See you in court, as they say." According to *Law360*, on November 17, the federal court granted Disney's request to arbitrate. As the *Bulletin* went to press, no further legal proceedings had been announced regarding Disney's motion.

On October 26, multiple news agencies reported that AIG had sued Disney in the Supreme Court of the State of New York, County of New York, seeking a declaration that it did not have to pay the $25 million insurance claim. *AIG v. American Broadcasting Companies*, No. 656581/2017 (2017). In its lawsuit, AIG explained that its policy provides insurance for a "Multimedia Act," which includes "defamation or harm to the character or reputation of any person or entity" during the course of "Media Activities," including "news gathering, news programming, and news distribution of informational content, programming or materials."

However, the complaint explained that the policy includes a "Defamation Carve-Out," which states that "[t]he Insurer shall not be liable for Damages, Claims Expenses, or Data Breach Expenses on account of any Claim . . . based upon . . . any dishonest, fraudulent, criminal, malicious, or intentional act, error or omission, or any intentional or knowing violation of the law by an Insured." The Carve-out does not apply "if and only if two requirements are met. First, the insured party's claim must "[allege] actual malice, as defined by the law, in conjunction with allegations of defamation, libel or slander of a public person, as defined by law."

Second, the policy requires that "prior to the date the Insured engaged in such excluded conduct, the Insured had received from its outside legal counsel a written opinion and authorization stating that based on counsel's good faith and reasonable legal evaluation and analysis of the existing law, counsel has concluded that such conduct was legal under and protected by the First Amendment . . . or any similar provision of a State Constitution protecting freedom of speech or freedom of the press." Thus, in order to receive potential coverage for claims regarding defamation, an insured party, before engaging in the potential defamation of a public person, must "first [receive] a written opinion from outside counsel opining that the insured's conduct is appropriate . . . and lawful." The complaint contended that Disney had not met the second requirement, but still "demanded that [AIG] pay . . . the full limits of the [policy] . . . notwithstanding the clear contractual language that excludes the BPI Settlement from coverage under the [policy]."

The complaint added that the reason behind the requirement to obtain an advance written opinion from outside counsel "is obvious." "If [the] insured [party] consults outside counsel concerning potentially defamatory statements prior to making them, the insured will be less likely to engage in conduct that gives rise to liability," the complaint read. "In order to incentivize insureds to consult with counsel, the [policy] provides coverage to an insured that consults with counsel even if the counsel's advice ultimately proves incorrect." The complaint continued, "On the other hand, if an insured publishes defamatory content about a public person with actual malice without having consulted outside counsel (or against the advice of outside counsel), then the insured bears the responsibility for his reckless conduct."

Although portions of the complaint were blacked out, *Variety* magazine reported on October 26 that Disney's counter-argument seemed to be that it was not "commercially reasonable" or normal industry practice to be required to obtain written permission from an outside attorney. The complaint countered that "[n]ews organizations regularly obtain written opinions and authorization from outside counsel before investigating and reporting a news story."

The complaint asked the court to declare that the pink slime settlement "is not covered by the [AIG] policy." The full complaint is available online at: https://www.scribd.com/document/362722968/AIG-Pink-Slime#from_embed.

In an October 26 statement, a Disney spokesperson said, "Rather than honor the terms of the insurance policy it sold us, AIG has chosen instead to evade those terms and attack its customer. We will vigorously pursue our right to recover."

As the *Bulletin* went to press, no further legal proceedings had been announced regarding AIG's complaint.

Ashley Turacek
Silha Research Assistant

Scott Memmel
Silha *Bulletin* Editor

Attorney Charles Harder Continues Attacks on News Websites by Filing Defamation Suits

In 2017, attorney Charles J. Harder, best known for his victorious lawsuit against media gossip website *Gawker* on behalf of former-professional wrestler Hulk Hogan, continued his legal attacks on media websites. On Jan. 4, 2017, Harder filed a defamation lawsuit against technology news website *TechDirt* on behalf of Shiva Ayyadurai, a scientist and candidate for the U.S. Senate who has drawn criticism from *TechDirt* regarding his claims that he invented email in the late 1970's. On September 6, a district court judge dismissed the defamation suit, finding that the allegedly defamatory statements were not capable of being proven false and that the complaint did not provide adequate facts to demonstrate actual malice, a standard created by the U.S. Supreme Court in *New York Times v. Sullivan*, 376 U.S. 254 (1964), requiring knowledge that defamatory statements are false or made with reckless disregard of the truth. On Sept. 7, 2017, Harder filed a defamation lawsuit against women's website *Jezebel*, contending that a 2016 article defamed his client, Oregon-based life coach Gregory Scherick, by likening his therapy group to a cult and calling Scherick a "snakeoil salesman."

DEFAMATION

Meanwhile, on October 15, *The Hollywood Reporter* reported that Harder had left his position as part of Harvey Weinstein's legal team as more allegations continued to surface against Weinstein, an American film producer who co-founded The Weinstein Company and Miramax Films. Harder had previously hinted at a multi-million-dollar action against *The New York Times*, which, along with *The New Yorker*, had reported that over a dozen women had accused Weinstein of sexual harassment and assault. Two days later, Harder joined the legal team of Jared Kushner, President Donald Trump's adviser and son-in-law who faced allegations related to an investigation into possible collusion by the Trump administration with Russia's meddling during the 2016 presidential election.

Harder previously represented Hogan in his suit against *Gawker*. That case arose in October 2012 when *Gawker* published a story titled "Even for a Minute, Watching Hulk Hogan Have Sex in a Canopy Bed is Not Safe For Work but Watch It Anyway," written by then-editor-in-chief A.J. Daulerio. The story contained a one-and-a half-minute excerpt from a 30-minute video recording from 2007 of Hogan engaging in various sexual acts with Heather Cole, then-wife of radio host and Hogan friend "Bubba the Love Sponge" Clem. Hogan sued Gawker for $100 million in damages claiming invasion of privacy, infringement of personality rights, and intentional infliction of emotion distress. In March 2016, a jury awarded Hogan $55 million for economic injuries and $60 million for emotional distress. The jury later awarded Hogan $25 million in punitive damages. On May 25, 2016, the *Tampa Bay Times* reported Florida Circuit Court Judge Pamela Campbell denied Gawker's motion asking her to overturn the jury's verdict or reduce the $140 million in damages awarded to Hogan. On Aug. 16, 2016, *Forbes* reported that Univision Communications, Inc. had agreed to purchase Gawker Media's assets, and then ended *Gawker*'s operations in August. (For more on the background of the legal dispute between Gawker and Hogan, see "*Gawker* Shuts Down After Losing Its Initial Appeal of $140 Million Judgment in Privacy Case" in the Summer 2016 issue of the Silha *Bulletin* and "*Gawker* Faces $140 Million Judgment after Losing Privacy Case to Hulk Hogan" in the Winter/Spring 2016 issue.)

District Court Judges Dismisses Harder's Lawsuit Against *TechDirt*

On Sept. 6, 2017, U.S. District Court for the District of Massachusetts Judge F. Dennis Saylor IV dismissed a defamation lawsuit filed by attorney Charles Harder on behalf of Shiva Ayyadurai, a scientist who frequently claimed that he invented email in the late 1970s. *Ayyadurai v. Floor64, Inc.*, No. 17-10011-FDS (D. Mass. 2017). Ayyadurai contended that technology news website *TechDirt* published 84 allegedly defamatory statements contained within the 14 articles critical of his claims that he invented the internet. Media advocates praised the decision as defending the First Amendment protections for the press.

The case arose between September 2014 and November 2016 when *TechDirt*, which is owned and operated by California corporation Floor64, Inc., published 14 articles about Ayyadurai, who claimed that he "created email" while working as a research fellow at the University of Medicine and Dentistry of New Jersey. Multiple academic and media publications have recognized Ayyadurai as the inventor of email, including *Time* magazine, *Wired* magazine, and CBS News.

Ayyadurai's Jan. 4, 2017 complaint identified 84 allegedly defamatory statements contained within the 14 articles, of which the majority said Ayyadurai's claim to have invented e-mail is false. One such statement read, "Ayyadurai's claim that he invented email is complete bullshit. It's not true. Not even remotely." Other statements suggested that Ayyadurai has "misrepresents what a copyright registration means" and that "the 'US government officially recognized Ayyadurai as the inventor of email' in 1982." Thirteen of the articles were written by *TechDirt* insider Michael David Masnick and one was written by Leigh Beadon, another *TechDirt* insider.

On February 17, defendants Floor64 and Masnick, filed a special motion to dismiss the complaint, citing California's anti-strategic litigation against public participation (SLAPP) statute, which allows a special motion to strike "[a] cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue," unless a plaintiff "has established a probability that he or she will prevail on the claim." Cal. Civ. Proc. Code § 425.16. (For more information on anti-SLAPP statutes, see "Several State Courts and Legislatures Grapple with Anti-SLAPP Laws" in the Summer 2017 issue of the Silha *Bulletin*.) Floor64 and Masnick also moved to dismiss the libel claims against them for failure to state a claim on which relief can be granted. Beadon filed separate motions to strike and to dismiss.

Saylor first addressed whether the California anti-SLAPP law applies in the case. He found that "there is a presumption that the law of Massachusetts will apply" for three reasons, including "defendants published allegedly defamatory statements in a form of aggregate communication, a website," "plaintiff was domiciled in Massachusetts at the time," and finally, that "the website, which is accessible by anyone anywhere with an Internet connection, was published in Massachusetts." Thus, Saylor denied the motion to strike and applied Massachusetts law to the remaining claims.

Next, Saylor addressed the defendants' claims that "the complaint fails to make plausible allegations that the statements at issue are false; that the statements are protected under the First Amendment; and that the complaint fails to plausibly allege that the statements were made with actual malice." First, he determined whether Ayyadurai is a public figure, which would require that he prove the statements made by *TechDirt* were made with actual malice, knowledge that it was false or with reckless disregard of whether it was false or not. *New York Times v. Sullivan*, 376 U.S. 254 (1964). Saylor concluded that Ayyadurai constitutes a "limited-purpose" public figure because,

Harder, *continued on page 22*

Harder, *continued from page 21*

by publishing books, doing interviews, and posting on his website, he "thrust [himself] to the forefront" of the controversy "in order to influence the resolution of the issues involved" in it.

Second, Saylor determined whether the statements related to matters "of public concern," which would require the plaintiff to show that the comments were false. Saylor concluded that the statements were "clearly" matters of public concern because the complaint referred to numerous articles discussing Ayyadurai's claim that he invented email, that a number of the statements were made in response to other articles discussing the claim, and that readers posted numerous comments on the *TechDirt* articles.

Accordingly, Saylor sought to determine whether the complaint plausibly alleged falsity. He found that the *TechDirt* articles "do not dispute that plaintiff created *an* e-mail system," but rather that the plaintiff "should properly be characterized as *the inventor* of e-mail based on that creation" (emphasis in original). Thus, according to Saylor, "it is not clear that the allegations in the complaint are sufficient to show that the statements at issue are false."

Next, Saylor turned to whether the alleged defamatory statements are protected by the First Amendment. Regarding the majority of statements that claimed that Ayyadurai did not invent email, Saylor concluded that the statements were not capable of being proven wrong. He cited *Pan Am Systems, Inc. v. Atlantic Northeast Rails and Ports, Inc.* in which the U.S. Court of Appeals for the First Circuit concluded that "defamatory statements are not punishable unless they are capable of being proved true or false." 804 F.3d 59 (1st Cir. 2015).

Furthermore, Saylor cited the First Circuit's conclusion that "even a provably false statement is not actionable if it 'is plain that the speaker is expressing a subjective view, an interpretation, a theory, conjecture, or surmise, rather than claiming to be in possession of objectively verifiable facts.'" Saylor found that the statements were not actionable because they "disclose the non-defamatory facts on which they rely [and] make clear that the conclusions drawn from those facts are simply an interpretation of them." Further, the statements did not "rely on other, undisclosed and potentially defamatory facts that are not available to others." He added that the statements often constituted hyperbole, meaning the articles "simply [used] colorful and figurative language and are not making any fact-based accusation that plaintiff has actually committed a fraud."

Finally, Saylor determined that because the complaint did not provide any specific factual allegations to support the conclusion that *TechDirt* acted "with the knowledge that [the statements] were false," the complaint failed to provide adequate facts to demonstrate malice.

Additionally, Saylor considered Ayyadurai's claim that the defendants "made the allegedly defamatory statements despite knowing that another website, [*Gawker*], had settled a defamation claim brought by plaintiff concerning similar statements." Saylor concluded that this argument was not adequate to demonstrate actual malice because it did not demonstrate that the defendants knew the statements were false.

Thus, although Saylor denied the anti-SLAPP motion, he granted the defendants' motion to dismiss for failure to state a claim.

Following the ruling, in an interview with *The Daily Beast*, media attorney David Bodney praised the decision. "It is positively heartening to see the First Amendment protections recognized," Bodney said. "It is encouraging to see the First Amendment protections applied to keep the cost of 'free speech' as minimal as possible."

In a September 6 *TechDirt* story, Masnick praised the ruling. "We are certainly pleased with the decision and his analysis, which notes over and over again that everything that we stated was clearly protected speech, and the defamation (and other claims) had no merit," he wrote. "This is, clearly, a big win for the First Amendment and free speech – especially the right to call out and criticize a public figure such as Shiva Ayyadurai."

However, Masnick expressed concern that the anti-SLAPP motion was denied. "We are disappointed, however, that the judge denied our separate motion to strike under California's anti-SLAPP law," he wrote. "For years, we've discussed the importance of strong anti-SLAPP laws that protect individuals and sites from going through costly legal battles. Good anti-SLAPP laws do two things: they stop lawsuits early and they make those who bring SLAPP suits – that is, lawsuits clearly designed to silence protected speech -- pay the legal fees." He continued, "However, that just reinforces the argument we've been making for years: we need stronger anti-SLAPP laws in many states (including Massachusetts) and, even more importantly, we need a strong *federal* anti-SLAPP law to protect against frivolous lawsuits designed to silence protected speech. The results of this case have only strengthened our resolve to do everything possible to continue to fight hard for protecting freedom of expression and to push for stronger anti-SLAPP laws that make free speech possible, and not burdensome and expensive" (emphasis in original).

In a statement, Harder defended the lawsuit and indicated Ayyadurai's desire to appeal. "Dr. Ayyadurai has a long history of standing up for free speech. As a strong proponent of free speech, he also believes intruthful speech," Harder said. "False speech is not protected by the Constitution, and *TechDirt*'s false and malicious speech about Dr. Ayyadurai should receive no legal protection." He continued, "False speech does harm to readers, who are misled by it; it does harm to journalism, which is weakened by it; and it does harm to the subjects of the speech, whose reputations and careers are damaged by it. The public, and the courts, should not tolerate false speech, particularly when it causes people harm, and irresponsible media companies should stop using the Constitution as an excuse for their reckless dissemination of false information."

As the *Bulletin* went to press, Ayyadurai had not appealed the decision.

Harder Files Defamation Suit Against *Jezebel*

On Sept. 7, 2017, Charles Harder filed a defamation lawsuit against *Gawker*'s sister website *Jezebel* and its parent company Gizmodo Media Group, LLC on behalf of Oregon-based life coach Gregory Scherick, the founder of International Scherick, LLC, a New York a therapy group also known as Superstar Machine. Several media law experts and advocates said it was unlikely that Scherick would win the case.

In a May 10, 2016 exposé, *Jezebel* called Scherick a "snakeoil salesman" and called Superstar Machine a "cult that preys on its members' insecurities, exploits them financially, and isolates them," citing interviews with several former Superstar Machine members. The story added that Scherick "cultivated a group of women who served as his seconds-in-command, and whose role is to praise him, back up his decisions, and remind everyone coming into the group that they needed to give him 'a good experience.'" The full article is available online at: https://jezebel.com/inside-superstar-machine-which-ex-members-say-is-a-cul-1775494367.

According to *Rolling Stone* magazine on Sept. 7, 2017, Scherick filed a 26-page lawsuit in the New York State Supreme Court, County of New York against Gizmodo Media Group, which owns *Jezebel*, as well as the author of the article, Anna Merlan, and former editor-in-chief Emma Carmichael. He claimed that he and his company were defamed by the *Jezebel* article and that he lost 70 percent of his clientele after the article was published. The complaint read, "Superstar Machine is not a cult by any stretch of the imagination.. . . Among other things, there is no religious component to the group. It encourages its members to become stronger individuals through certain guidance and advice. It does not attempt to

instill Mr. Scherick's opinions on its members nor does it use rewards or punishments to force members to act in a certain manner." The complaint continued, "The existence of the Article . . . causes tremendous damage to Plaintiff's professional reputations, and Mr. Scherick's personal reputation as well."

Furthermore, the complaint alleged that *Jezebel* published the article despite several former Superstar Machine members writing in the comments section that the article's allegations were questionable and that it relied on sources with "extreme biases against Superstar Machine." Additionally, the complaint pointed out that UniModa and parent company Univision, which had acquired the assets of Gawker Media after the organization filed for bankruptcy, had transferred the assets, including *Jezebel*, to Gizmodo Media Group. The complaint alleged that Gizmodo Media Group published the *Jezebel* story "[d]espite being aware that Gawker Media has questionable, if not outright unethical 'journalistic' practices" and despite an earlier letter from Harder to Gizmodo Media Group to remove the defamatory statements in the article.

In the complaint, Scherick sought the removal of the *Jezebel* article, as well as compensation for the harm caused by the alleged defamatory statements. The plaintiffs also demanded a jury trial. The full complaint is available online at: https://www.documentcloud.org/documents/3988608-Scherick-Gizmodo-Complaint.html.

In a September 2017 statement, a spokesperson for Gizmodo Media Group wrote, "This case is nothing more than another obvious attempt by Charles Harder to intimidate journalists. The story in question was published on May 10, 2016 – months before our acquisition of certain Gawker Media assets, including *Jezebel*. Any litigation over the story should have been brought against Gawker Media in bankruptcy court – not against Gizmodo Media Group or the individual writers. We believe this suit is meritless and we plan to contest it vigorously."

Several media law experts argued that Harder faces significant obstacles in the lawsuit. Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley told *TheWrap* on September 10 that "[p]utting aside the general merits of this suit, it's just tougher to win a libel suit rather than a privacy suit." If Scherick is found to be a public figure, he will have to show that *Jezebel* published the defamatory statements with actual malice, which requires the journalist acted with knowledge of falsity or reckless disregard of the truth, as defined by the 1964 Supreme Court case *New York Times v. Sullivan*. 376 U.S. 254 (1964).

Kirtley also noted that unlike the Gawker Media case, which was filed in Florida, Scherick sued in New York, where judges have proved to be far more likely to dismiss libel lawsuits. "All things considered, if I'm libel media defendant, and if I could be sued anywhere, I'd prefer to be sued in New York."

University of Maryland Philip Merrill College of Journalism school dean Lucy Dalglish agreed. "There's no question it has been historically easier to get a dismissal or summary judgment on libel cases in New York," she told *TheWrap*. "New York judges generally follow established law and are accustomed to dealing with cases involving media of all types."

Harder Leaves Harvey Weinstein's Legal Team Amid Growing Sexual Assault Allegations; Joins Jared Kushner's Legal Team

On Oct. 15, 2017, *The Hollywood Reporter* and other news outlets reported that attorney Charles Harder had left his position as part of Harvey Weinstein's legal team as more allegations surfaced against the co-founder of The Weinstein Company and Miramax Films. Harder had previously hinted at a multi-million-dollar action against *The New York Times*, which, along with *The New Yorker*, reported that over a dozen women had accused Weinstein of sexual harassment, assault, and rape over several decades. Two days after Harder reportedly left Weinstein's legal team, *Vanity Fair* reported that the attorney became part of Jared Kushner's legal team.

On October 5, *The New York Times* published a story titled "Harvey Weinstein Paid Off Sexual Harassment Accusers for Decades," written by correspondent Jodi Kantor and investigative reporter Megan Twohey. The report explained that an investigation by the *Times* revealed "previously undisclosed allegations against Mr. Weinstein stretching over nearly three decades, documented through interviews with current and former employees and film industry workers, as well as legal records, emails and internal documents from the businesses he has run, Miramax and the Weinstein Company." The *Times* story also noted that Weinstein had "reached at least eight settlements with women, according to two company officials speaking on the condition of anonymity."

The New Yorker reported five days later that in his own ten-month investigation, reporter Ronan Farrow "was told by thirteen women that, between the nineteen-nineties and 2015, Weinstein sexually harassed or assaulted them." According to the story titled "From Aggressive Overtures to Sexual Assault: Harvey Weinstein's Accusers Tell Their Stories," three women told Farrow that Weinstein had raped them.

On October 5, *Variety* reported that Harder had threatened to sue *The New York Times* over its story, calling it "saturated with false and defamatory statements about Harvey Weinstein" in a statement. Harder added, "It relies on mostly hearsay accounts and a faulty report, apparently stolen from an employee personnel file, which has been debunked by 9 different eyewitnesses.. . . We sent the *Times* the facts and evidence, but they ignored it and rushed to publish. We are preparing the lawsuit now. All proceeds will be donated to women's organizations."

In a separate statement, a *Times* spokesperson defended the story. "We are confident in the accuracy of our reporting. Mr. Weinstein was aware and able to respond to specific allegations in our story before publication. In fact, we published his response in full."

On October 8, Weinstein was fired as an employee by the Weinstein Company board and was expelled from the Academy of Motion Picture Arts and Sciences, according to *The Hill*. On October 16, during a meeting to affirm his dismissal, Weinstein resigned from the Weinstein Company board, as reported by *The New York Times* the following day.

On October 15, Harder left Weinstein's legal team due to additional allegations of sexual assault and harassment against Weinstein, according to a tweet by *The Hollywood Reporter* editor Janice Min. *The Hollywood Reporter* also noted that this probably meant that there would be no lawsuit against *The New York Times*.

Vanity Fair reported on October 17 that Harder had joined the legal team of Jared Kushner, President Donald Trump's adviser and son-in-law who faces allegations related to an investigation into possible collusion by the Trump administration with Russia's meddling during the 2016 presidential election. CNN reported on July 14, 2017 that Kushner was part of a controversial meeting with a Russian lawyer, Donald Trump Jr., and then-Trump campaign chairman Paul Manafort during the 2016 campaign. Kushner was also among President Trump's advisers advocating for the president to fire then-Federal Bureau of Investigation director James Comey, who was leading the investigation into Russian election interference before being fired on May 9 by President Trump, according to *The New York Times* the same day.

Ashley Turacek
Silha Research Assistant
Scott Memmel
Silha *Bulletin* Editor

EPA Targets Journalist for "Misleading Story"; Ohio Photographer Shot by Police; Charge Dropped Against West Virginia Photographer

In the fall of 2017, several journalists faced professional attacks or physical harm while engaged in reporting. On September 3, the Environmental Protection Agency (EPA) published a news release criticizing reporter Michael Biesecker of the Associated Press (AP), prompting pushback from media advocates and experts. On September 4, photojournalist Andy Grimm was shot by a New Carlisle, Ohio sheriff's deputy who thought Grimm was pulling a gun from his car, although the body camera footage showed that Grimm was actually getting his camera and a tripod to record a traffic stop. Finally, on September 6, charges were dropped against West Virginia reporter Dan Heyman following a May 2017 incident in which Heyman was arrested after attempting to question then-Health and Human Services Secretary Tom Price and senior Trump advisor Kellyanne Conway in a West Virginia statehouse hallway.

ENDANGERED JOURNALISTS

Environmental Protection Agency slings personal attack at Associated Press Reporter

On Sept. 3, 2017, an U.S. Environmental Protection Agency (EPA) news release singled out an Associated Press (AP) reporter for writing an "incredibly misleading story" and "cherry-picking facts," among other allegations. The news release targeted a report by AP reporters Michael Biesecker and Jason Dearen criticizing the EPA for not being on the scene of toxic waste sites during flooding in the wake of Hurricane Harvey. Several news organizations spoke out in defense of Biesecker, criticizing the agency for singling out a specific reporter.

On September 2, Biesecker and Dearen posted an article, titled "AP EXCLUSIVE: Toxic waste sites flooded, EPA not on scene." The reporting team opted to focus its investigative efforts on Superfund sites, polluted locations requiring long-term clean up, in the path of Hurricane Harvey prior to the storm making landfall in Texas. On August 17, days before Harvey's landfall, the AP requested a copy of the agency's analysis of Superfund sites near floodplains or in danger of sea-level rise. After Harvey passed from Texas to Louisiana, the reporting team visited seven flooded Superfund sites by foot and by boat. One such site was the Highlands Acid Pit site in Highlands, Texas, which in the 1950s was filled with toxic sludge and sulfuric acid from oil and gas operations and "is still considered a potential threat to groundwater, and the EPA maintains monitoring wells there," according to the article. The article argued that in the wake of Hurricane Harvey and the resulting flooding, the EPA was "not on the scene."

According to *The Washington Post*'s "Eric Wemple" blog, the EPA responded with a statement indicating that it had seen aerial imagery showing that 13 of 41 sites were flooded and were "experiencing possible damage." The statement also criticized the AP's reporting as "misleading and inaccurate" and noted that regulatory officials were in place to investigate the scenes after they were able to safely access the sites. Biesecker and Dearen adjusted the article and published an update the following day, which read, in part, "The statement confirmed the AP's reporting that the EPA had not yet been able to physically visit the Houston-area sites, saying the sites had "not been accessible by response personnel.. . . EPA staff had checked on two Superfund sites in Corpus Christi on Thursday and found no significant damage."

On September 3, the EPA published a news release titled "EPA's Response to the AP's Misleading Story." The first line singled out Biesecker for writing "an incredibly misleading story about toxic land sites that are under water." The release continued, "Despite reporting from the comfort of Washington, Biesecker had the audacity to imply that agencies aren't being responsive to the devastating effects of Hurricane Harvey. Not only is this inaccurate, but it creates panic and politicizes the hard work of first responders who are actually in the affected area." The release also criticized the AP for "cherry-picking facts" and being an instance of "yellow journalism." The release did not mention Dearen.

The statement also cited an earlier report by Biesecker claiming that, "Unfortunately, the Associated Press' Michael Biesecker has a history of not letting the facts get in the way of his story. Earlier this summer, he made-up a meeting that Administrator Pruitt had, and then deliberately discarded information that refuted his inaccurate story – ultimately prompting a nationwide correction."

Biesecker had reported that Pruitt "met privately with the chief executive of Dow Chemical shortly before reversing his agency's push to ban a widely used pesticide after health studies showed it can harm children's brains, according to records obtained by The Associated Press." In fact, the private meeting did not take place due to scheduling conflicts, though it remained listed on an EPA schedule obtained by the AP. According to an "Erik Wemple" blog post on September 7, an EPA official insisted the agency responded before the story was published, but the same error appeared in a *New York Times* article. The AP ran a correction, which said, in part, "A spokeswoman for the EPA says the meeting listed on the schedule was canceled, though Pruitt and [Dow Chemical CEO Andrew] Liveris did have a 'brief introduction in passing.'" The AP also ran a new story with more information about the non-meeting.

Following the EPA's news release, fellow AP reporters, as well as other news organizations and reporters, criticized the EPA's condemnation of the report and singling out Biesecker. Chris Hayes, host of "All In with Chris Hayes" on MSNBC, on his September 5 show called the EPA's response "bizarre" and "unusually nasty" while defending the "correct" reporting of the AP team. Hayes also noted that the release did not indicate any inaccuracies of the reporting, but rather used personal criticism of Biesecker to disregard and attempt to discredit the report as a whole.

GQ's Luke Darby also criticized the EPA release. "[The EPA] basically confirmed the AP's reporting here: more than a dozen sites have been flooded and the EPA has not investigated them in person," he wrote in a September 5 *GQ* story. "And again, despite the EPA trying to single out Biesecker, the AP did have someone on the ground, proving if nothing else that the sites are accessible."

AP Executive Editor Sally Buzbee also responded to the EPA statement to rebut the criticisms lobbed at Biesecker and the AP team's reporting. "AP's exclusive story was the result of on-the-ground reporting at Superfund sites in and around Houston, as well as AP's strong knowledge of these sites and EPA practices," Buzbee said in September 4 statement. "We object to the EPA's attempts to discredit that reporting by suggesting it was completed solely from 'the comforts of Washington' and stand by the work of both journalists who jointly reported and wrote the story."

Despite prompting backlash from members of the media, an anonymous source told Wemple that it boosted morale within the agency. "I was with 20 to 30 career folks who were appalled by the story and they nearly teared up when press release went out. . . This administration was defending their hard work and dedication," said the official.

Ohio Photojournalist Shot by Sheriff's Deputy

On Sept. 4, 2017, Andy Grimm, a photojournalist for the *New Carlisle News* in Ohio, was shot by Clark County Sheriff's Deputy Jake Shaw while attempting to photograph a traffic stop. The Labor Day incident was captured on Shaw's body camera, producing footage that has led to criticism of both the officer and photographer.

Grimm told Ohio's FOX 45 television station he had gone out the night of September 4 to shoot a lightning storm, but stopped to catch the sheriff's deputy's traffic stop for the *New Carlisle News*. According to Grimm, Shaw mistook the photographer's camera and tripod for a firearm when Grimm began to pull the gear from the trunk of his Jeep across the road from the deputy. Grimm told FOX 45, "My camera was already on the tripod and I grabbed it like this [reaching motion] and turned and I just hear 'pop, pop.'" Additionally, Grimm said he never heard a warning from Shaw nor did he hear the deputy identify himself or make any demands of Grimm prior to shooting.

The body camera video begins seconds before Shaw fired the two shots at Grimm. The footage did not indicate Shaw made any attempt to identify himself or warn the photographer prior to firing. After the shots were fired, Grimm could be heard screaming in pain. Between expletives Grimm shouted, "Jake, you just shot me," as the officer ran to his aide. Shaw's first words on the video are a call into dispatch for medical assistance. Shaw's body camera captured Grimm's blood-stained shirt and glimpses of the wound on Grimm's right side. The first shot grazed Grimm's right shoulder but the second hit near his rib cage on the right side, narrowly avoiding major organs.

Throughout the footage, it became clear that Shaw and Grimm knew each other. Shaw repeated "Andy" multiple times and throughout the recording, the two referred to each other as "dude." At one point, Shaw said, "Andy, I thought it was a friggin' gun, dude.. . . Stay strong with me. I love you, brother." In an interview with the *New Carlisle News*, Grimm later noted that his father, Dale Grimm, owns the newspaper in the community of just over 5,000 and that the staff is well-acquainted with first responders.

In the footage, Grimm also emphasized that this was not the first instance that he pulled over to record a traffic stop by a sheriff's deputy. "I have done this exact same thing hundreds of times to hundreds of different officers, Grimm said. "Of course caution is exercised. Never approach law enforcement from behind at night. I always approach from the side so I can be visible to the officer and the perp. I try to make myself noticeable to ease the officer's concerns." In the body camera video, Grimm told Shaw that he flashed his lights and waved before getting his gear ready. "I thought you saw me wave, dude," Grimm said. Grimm is also heard asking to call his wife, as well as pleading with the officer to keep his camera safe from the rain and asking if it can come with him in the ambulance.

In a Q&A with *New Carlisle News* reporter Maggie Yowler, Grimm emphasized he did not feel anger toward Shaw. "I instantly felt bad for him. I knew the mess he would have to go through with the investigation and such," Grimm said. "I can still have compassion for someone even after they just shot me." The body camera footage is available online at: https://petapixel.com/2017/09/07/heres-body-camera-footage-cop-shooting-photographer/.

Shaw was placed on administrative leave pending further investigation by the Ohio Bureau of Criminal Investigations. On October 27, the *Springfield News Sun* reported that Shaw had returned to work on October 21. However, as the *Bulletin* went to press, the Ohio Attorney General's Office investigation remained ongoing. Grimm told the *Springfield News Sun*, "It's hard to believe that he's back to work but I'm just waiting on due process."

Following the shooting, residents of New Carlisle discussed the incident on a community Facebook group, according to a September 16 FOX 45 report. Some residents argued that Grimm was responsible and did not exercise enough caution in approaching the traffic stop at night. One commenter wrote, "Andy . . . [we] are up praying for you right now. Shaw – your [sic] a good person and a good cop. Your job is not easy . . . Your [*sic*] both in my prayers tonight." Other residents contended that the officer was responsible and should have given a warning and/or otherwise identified himself to Grimm. "Cops need to wake up!" wrote one commenter. "I call for Shaw's Badge," said another, according to September 5 story by *The Huffington Post*.

Charge Dropped Against West Virginia Journalist

On Sept. 6, 2017, *Public News Service* in West Virginia released a joint statement with the Kanawha County Prosecuting Attorney announcing that the State had dropped the "willfully disrupting a State governmental process or meeting" charge against Dan Heyman, a reporter for *Public News Service*. In May 2017, Heyman was arrested while attempting to pose questions to then-Health and Human Services Secretary Tom Price and senior Trump advisor Kellyanne Conway in the hallway of the West Virginia State Capitol. On September 29, Price resigned his position following a separate controversy that he extensively used taxpayer-funded charter flights, according to a White House announcement.

The event leading to the arrest and charge against Heyman occurred on May 9, 2017 when Heyman attempted to ask questions of Price and Conway in the hallway of the West Virginia statehouse following a press conference. *The New York Times* reported Heyman persistently shouted questions at Price and Conway regarding the since-failed American Health Care Act (AHCA) which, at the time, was under consideration in the U.S. House of Representatives.

Heyman was arrested shortly thereafter and charged with one misdemeanor count of "willful disruption of governmental processes" according to the criminal complaint. The full complaint is available online at: https://www.documentcloud.org/documents/3711449-Daniel-Heyman-Criminal-Complaint.html. (For more information on the events leading to Price's arrest and the charges against the reporter, see *West Virginia Journalist Arrested* in "Journalists Face Physical Restraints and Arrests; Trump Video Raises Further Concerns about Violence Against the Media" in the Summer 2017 issue of the Silha *Bulletin*.)

Lawrence Messina, director of communications for the Reporters Committee for Freedom of the Press (RCFP), previously wrote in a May 16 letter to West Virginia Capitol Police that the actions of the arresting officers were not in accordance with the statute under which Heyman was charged. W.Va. Code § 61-6-19, titled "Willful disruption of governmental processes; offenses occurring at State Capitol Complex; penalties" imposes a penalty if an individual "willfully interrupts or molests the orderly and peaceful process" of a government office. However, the statute also acknowledges the importance of respecting First Amendment rights by

Journalists, *continued on page 26*

The United States, the European Union, and the Irish High Court Wrangle Data Privacy Concerns

SPECIAL REPORT

On Oct. 18, 2017, the European Commission released a report on the annual review of the EU-U.S. 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]." On Sept. 20, 2017, U.S. Secretary of Commerce Wilbur Ross and EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová had released a joint statement praising the annual review, which took place on September 18 and 19. Ross and Jourová called the review an "important milestone for the Framework and for U.S.-EU cooperation on data protection issues."

However, throughout 2017, individuals in the United States and the EU, as well as a digital rights group and two human rights organizations, had questioned the future of the Privacy Shield under the leadership of President Donald Trump.

Meanwhile, on Oct. 3, 2017, the High Court in Ireland issued a judgement on Facebook's use of "standard contractual clauses" (SCC) in data transfers between the EU and United States, referring the case to the European Court of Justice (ECJ). In February and March 2017, the Irish High Court had heard expert testimony in the case (*Schrems II*) brought by Austrian data privacy activist Maximillian Schrems concerning Facebook's use of SCCs, language widely adopted in EU data transfer written agreements used by companies to transfer personal data. Schrems contended that the use of SCCs for transferring personal data does not adequately protect his, and other individuals', personal data.

Also in 2017, the United Kingdom (UK) and Germany, as well as the Article 29 Working Party, which provides the European Commission with independent advice on data protection matters and helps develop data protection policies in the EU Member States, took steps related to the implementation of the General Data Protection Regulation (GDPR). The GDPR was adopted by the EU in Spring 2016 to harmonize data privacy laws across Europe and to protect EU citizen's data privacy rights, and will become effective in May 2018.

In *Schrems I*, on Oct. 6, 2015, the Court of Justice of the European Union (CJEU) invalidated the U.S.-EU Safe Harbor, the previous framework governing data protection regulations of personal data transfers between the EU and United States. The case arose after Schrems claimed that United States law and national security practices, particularly the widespread surveillance practices of U.S. intelligence agencies revealed by Edward Snowden, failed to ensure adequate protection of personal data under the European Union's Data Protection Directive for European citizens. The court ruled that the Safe Harbor framework did not ensure that the U.S. provided the level of protection required by Article 25(6) of the Data Protection Directive. *Schrems v. Data Protection Comm'r*. Case C-362/14, Schrems v. Data Prot. Comm'r., 2015 E.C.R. I-650 (Oct. 6, 2015).

On Feb. 24, 2016, President Obama signed the Judicial Redress Act, Pub. L. No. 114-126, 130 Stat. 282 (2016), which authorized the U.S. Department of Justice (DOJ) to designate "covered countries" whose citizens are permitted to bring civil actions against government agencies in U.S. courts under the U.S. Privacy Act, according to a February 27 Keller and Heckman LLP commentary. The Judicial Redress Act granted EU citizens the ability to seek remedies under the Privacy Act against United States agencies for the improper disclosure of personal information.

On July 12, 2016, the European Commission officially adopted an amended version of the Privacy Shield, which included several additional commitments by U.S. government agencies concerning surveillance of individuals in the United States, according to a July 18,

Journalists, *continued from page 25*

adding that "any assembly in a peaceable, lawful and orderly manner for a redress of grievances shall not be a violation of this section."

Messina's letter read, "When it is clear that someone is engaged in newsgathering, Capitol Police officers must recognize the First Amendment rights at stake, as the West Virginia statute does, as well as the public interest in the important work that reporters like Mr. Heyman do." The full letter is available online at: https://www.rcfp.org/sites/default/files/2017-05-16-letter-to-wv-capitol-police.pdf.

On September 6, *Public News Service* released a joint statement with the Kanawha County Prosecuting Attorney announcing the State was dropping the charge against Heyman. The statement read, "The State has determined, after a careful review of the facts, that Mr. Heyman's conduct, while it may have been aggressive journalism, was not unlawful and did not violate the law with which he was charged, that is, willfully disrupting a State governmental process or meeting." The full statement is available online at: https://twitter.com/PNS_News/status/905479972797652992.

Heyman's attorney J. Timothy DiPiero said in a September 6 conference call with the Associated Press (AP) that his client's cell phone recording of the incident was helpful in getting the charges dismissed. "Dan really saved himself by having that phone on because the truth came out," DiPiero said.

Jamie Lynn Crofts, legal director of the American Civil Liberties Union (ACLU) of West Virginia, said dropping the charge "was a win for the First Amendment and all of us who rely on it." Additionally, Heyman received financial support for legal fees from the Society of Professional Journalists (SPJ) and *pro bono* assistance from the law firm Wilmer Hale, according to *The Washington Post*'s "Erik Wemple" blog.

On September 29, multiple news agencies reported that Price had resigned his role as Health and Human Services Secretary on September 29 following mounting criticism of his use of taxpayer dollars for private airfare. "I'm not happy, I can tell you that. I'm not happy," President Donald Trump said as prepared to leave the White House en route to his private golf club in Bedminster, N.J., as reported by *The Washington Post*.

Brittany Robb
Silha Research Assistant

2016 *Bloomberg BNA* commentary. In addition to Privacy Shield, the European Commission also sought an "Umbrella Agreement" between the EU and U.S., establishing standards on international transfers of personal data for law enforcement purposes. The agreement was approved by the European Parliament on Dec. 2, 2016.

Following the adoption of the Privacy Shield, several critics argued that it was not a significant enough departure from the Safe Harbor framework. The Article 29 Working Party, which provides the European Commission with independent advice on data protection matters and helps develop data protection policies in the EU Member States, had several concerns, including a lack of specific rules on automated decisions; the lack of a general right to object; and the lack of assurance that mass, indiscriminate collection of personal data would not take place. (For more information on the U.S.-EU Safe Harbor framework, *Schrems I*, and the adoption of the Privacy Shield, see *Trump Executive Order Eliminates Privacy Act Protections for Certain Non-Citizens; Threatens Privacy Shield Laws* in "Federal Government, Minnesota Court of Appeals Address Data Privacy Issues" in the Winter/Spring 2017 issue of the Silha *Bulletin* and "Judicial Redress Act the Next Step in a Replacement of EU-US Safe Harbor Framework; Controversial Cybersecurity Information Security Act Passes the Senate" in the Fall 2015 issue.)

United States and European Union Officials Hold Review of the Privacy Shield

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]." The report provided the findings of the Commission, as well as several recommendations for improvement on the framework. Observers generally praised the positive review of the Privacy Shield, though some observers noted that the framework could still be improved, including through the recommendations proposed by the European Commission.

Following a March 2017 meeting with U.S. Secretary of Commerce Wilbur Ross in Washington, D.C., EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová confirmed that the annual review of the Privacy Shield would take place in September 2017, as reported by DAC Beachcroft, an international law firm, in a June 22 commentary. According to Jourová, the review would help ensure that the United States was deleting EU personal data where it was no longer necessary for the purpose for which it was collected, and that the Shield continued to reflect the GDPR. Jourová said during the announcement that the review "will be an important milestone where we need to check that everything is in place and working well."

> "This first annual review marks an important milestone for the Framework and for U.S.-EU cooperation on data protection issues.. . . Officials noted that this input [from Privacy Shield participants and independent organizations] greatly informed the review process and will lead to continued improvements to the functioning of the program."
>
> **— U.S. Secretary of Commerce Wilbur Ross and EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová**

In a Sept. 20, 2017 commentary for TLT, a UK law firm, partner Alison Deighton outlined three areas of concern that would likely be addressed by the review, including the "[c]ollection of bulk data for law enforcement purposes," "[a]utomated decision-making," and the Privacy Shield's Ombudsperson mechanism, including how the individual is appointed, as well as calls for stricter assurances regarding the independence and powers of the Ombudsperson. The Privacy Shield Ombudsperson is a position "dedicated to facilitating the processing of requests from EU individuals relating to national security access to data transmitted from the European Union to the United States." On Jan. 18, 2017, Acting Assistant Secretary Judith G. Garber was delegated the authorities of the Under Secretary for Economic Growth, Energy and the Environment, which includes the Ombudsperson, according to the U.S. Department of State's website.

Prior to the review, the White House expressed optimism about the Privacy Shield. "The White House applauds the preparation efforts in advance of the first annual joint review of the EU – U.S. Privacy Shield. We firmly believe that the upcoming review will demonstrate the strength of the American promise to protect the personal data of citizens on both sides of the Atlantic," the White House wrote in a September 15 statement. "Programs like the Privacy Shield . . . enable the free flow of information, which sustains the nearly $1 trillion dollars in goods and services trade across the Atlantic, and even more around the globe."

On September 21, Ross and Jourová released a joint statement praising the review, which had taken place on September 18 and 19. "This first annual review marks an important for the Framework and for U.S.-EU cooperation on data protection issues," they wrote. "The review examined all aspects of the administration and enforcement of the Privacy Shield, including commercial and national-security related matters, as well as broader U.S. legal developments. Participants also discussed their respective work to implement the Privacy Shield program during its inaugural year, recognizing the value of regular communication between U.S. and EU authorities."

Ross and Jourová added that the review was largely a success. "Since the program's inception, over 2,400 organizations have joined the Privacy Shield. U.S. and EU officials welcomed the information shared by Privacy Shield participants on Framework compliance, and by civil society and independent recourse mechanism providers," they wrote. "Officials noted that this input greatly informed the review process and will lead to continued improvements to the functioning of the program."

However, according to a September 25 *VPNCompare* commentary, the Privacy Shield review "duck[ed] the big issues in an attempt to keep things sweet between the EU and the USA." The commentary added that it was "a little surprising just how positive the joint statement . . . was."

Privacy, *continued on page 28*

Privacy, *continued from page 27*

On October 18, the European Commission published a report detailing its findings and recommendations following the review of the Privacy Shield. The Commission found that U.S. authorities had "put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield," including "enforcement" and "complaint handling" mechanisms meant to safeguard the individual rights of EU citizens, such as the Ombudsperson mechanism.

The report also concluded that the certification process of the framework had also "been handled in an overall satisfactory manner and [that] more than 2,400 companies [had] been certified so far." Additionally, the report noted that safeguards in the United States remained in place regarding "access to personal data by public authorities for national security purposes." The report cited Presidential Policy Directive 28 (PPD-28), which was ordered by President Barack Obama in 2014 to extend privacy safeguards to foreign nationals and to U.S. individuals' privacy rights against overreaching government surveillance.

Next, the report provided several recommendations for improvement of the Privacy Shield. First, the European Commission contended that companies "should not be able to publicly refer to their Privacy Shield certification before the certification is finalized" in order to avoid a "discrepancy between information that is publicly available, and the [U.S. Department of Commerce's (DOC)] Privacy Shield list." Furthermore, the Commission recommended that the DOC "[conduct], proactively and on a regular basis, searches for false claims of participation in the Privacy Shield" and conduct regular compliance checks to identify possible compliance issues that warrant "further follow-up action." In September 2017, the Federal Trade Commission (FTC) had entered consent agreements with three U.S. companies who had allegedly misrepresenting their participation in the Privacy Shield, according to a *National Law Review* report on Sept. 23, 2017. Md7, LLC; True Communication Inc.; and Decusoft, LLC each represented that they were participants in the Privacy Shield while their applications to the DOC were not finalized.

Second, the report asked that the DOC and data protection authorities of EU Member States (DPAs) continue to increase awareness of individuals' rights under the Privacy Shield, especially the ability to lodge complaints. The European Commission noted that the DOC had begun awareness efforts through its website by answering frequently asked questions tailored to four audiences: U.S. Businesses, EU Businesses, EU Individuals, and the DPAs. The DPAs, according to the European Commission, had published information on their respective websites as well, including documents developed by the Article 29 Working Party. However, the European Commission urged the DOC and Member States to "intensif[y] actions . . . to better inform individuals about their rights under the framework," but did not provide or recommend any specific means of doing so.

> "The Commission's general view is that the American authorities are living up to their commitments and that the system works.. . . The US side have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield."
>
> **— EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová**

Additionally, the European Commission recommended that the DOC and DPAs should "develop guidance on the interpretation of certain concepts in the Privacy Shield that need further clarification," such as the "principle of accountability for onward transfers and the definition of human resources data," which had emerged from the review as concepts that would "benefit from additional clarification," according to the European Commission.

Third, the report called on Congress to "favourably enshrine" PPD-28 in order to ensure "the stability and continuity of these protections." Fourth, the European Commission stated that it would "commission a study to collect factual evidence and further assess the relevance of automated decision-making" regarding transfers carried out under the Privacy Shield. Fifth, the report called on President Donald Trump's administration to swiftly appoint the Privacy Shield Ombudsperson and the members of the Privacy and Civil Liberties Oversight Board (PCLOB), which is tasked with protecting "privacy and civil liberties in the field of counterterrorism policies and their implementation." As the *Bulletin* went to press, President Trump had not named a permanent ombudsperson or the members of the PCLOB.

Finally, the European Commission called on U.S. authorities to "proactively fulfil their commitment to provide . . . timely and comprehensive information about any developments that could be of relevance for the Privacy Shield, including on developments that are liable to raise questions about the protections afforded under the framework." A full version of the report is available online at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

In addition to the report, the European Commission issued a press release which stated that the review showed that the Privacy Shield "works[,] but implementation can be improved." The press release also noted that the next step was for the report to be sent to the European Parliament, the Council, the Article 29 Working Party of Data Protection Authorities, and to the U.S. authorities and that the European Commission would "work with the U.S. authorities on the follow-up of its recommendations," as well as "closely monitor the functioning of [the] Privacy Shield." The full press release is available at: http://europa.eu/rapid/press-release_IP-17-3966_en.htm. The European Commission also published an infographic and Q&A document, as well as a "working document" detailing more fully the findings of the review. All the documents are available online at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

In a statement following the release of the report, Jourová said, "The Commission's general view is that the American authorities are living up to their commitments and that the system works.. . . The US side have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. Such as new redress possibilities for EU individuals and co-operation channels with European data protection authorities."

Jourová added that the European Commission was lobbying the Trump Administration and Congress to reform Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), 50 U.S.C.A. § 1881a, which provides authority for the United States government's "downstream" and "upstream" surveillance programs. The National Security Agency (NSA) defines "downstream" surveillance, previously referred to as PRISM, as "acquir[ing] communications 'to or from' a Section 702 selector (such as an email address)," according to an April 28, 2017 NSA statement. "Upstream" surveillance is defined as "acquir[ing] communications 'to, from, or about' a Section 702 selector." An example is the acquisition of an email that has a targeted email address in its text, even though it is between two individuals or organizations who are not targets. In the April 28 statement, the NSA announced that it was ending "upstream" surveillance, meaning surveillance would now be limited to communication that is directly to or from a foreign intelligence target.

In a statement, then-FTC Chairwoman Maureen Ohlhausen wrote, "We welcome the positive outcome of the [review].. . . Enforcing international privacy frameworks . . . is an integral part of our Privacy and Data Security program." She added, "We look forward to continuing to work with our European counterparts to ensure that the Privacy Shield remains a robust mechanism for protecting privacy and enabling transatlantic data flows."

Morgan Reed, president of ACT | The App Association, which represents more than 5,000 app companies and information technology firms, also praised the positive review of the Privacy Shield. "We support the EU-U.S. Privacy Shield as a model framework to foster cross-border data flows and secure privacy protections. Our small business members are among the 2,400 businesses that depend on Privacy Shield certification to engage with and access customers throughout the EU," he wrote. "Their growth and success hinges on the ability to protect consumer privacy, and maintain consumer trust. We will continue to work with U.S. government entities to ensure the Privacy Shield and its commitments are upheld."

In an October 18 commentary for *TechCrunch*, reporter Natasha Lomas noted some of the limitations of the European Commission's report. "[The European Commission] asks but does not comprehensively answer the question: 'How many access requests from surveillance authorities were received by companies under the Privacy Shield?' — instead it just pulls out a few figures disclosed by Privacy Shield-certified companies that already publish transparency reports, claiming they are 'illustrative' of the fact that 'as a percentage of total user accounts' the number of accounts affected by requests for government access to personal data 'remains limited,'" she wrote. "So it very much remains to be seen how red the EU's line will be if US intelligence agencies get their way and knock back any sympathetic reform of FISA's Section 702."

European Union Leaders Differ on Future of Privacy Shield Under Trump

In March 2017, two European commissioners met with President Donald Trump's administration to emphasize the importance of the EU-U.S. Privacy Shield (Privacy Shield), as well as to better understand the Trump administration's thoughts on the agreement. Both commissioners left the meetings feeling "reassured" and "positive," according to sources close to both leaders and in interviews with the media. Conversely, Members of the European Parliament (MEPs), as well as the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) expressed several concerns with the Privacy Shield, including questions about U.S. government surveillance, as well as vacant positions in the Federal Trade Commission (FTC) and the Privacy and Civil Liberties Oversight Board.

Previously, in January 2017, President Trump signed an executive order requiring that executive agencies strengthen enforcement of federal immigration laws, drawing concern from some observers who contended that the order would have a significant effect on the, while others were not convinced there would be any changes.

On Jan. 25, 2017, NBC News reported that President Trump had signed an executive order directing federal departments and agencies to "exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information." The Privacy Act of 1974, 5 U.S.C. § 552a, broadly limits the ability of federal agencies to collect and disclose records of U.S. citizens or legal permanent residents (LPRs) of the United States.

The executive order's application to the Privacy Act brought greater scrutiny to the Privacy Shield. Shortly after President Trump issued his executive order, Jan Philipp Albrecht, rapporteur of the European Parliament for the EU-U.S. data protection framework, posted on Twitter that the European Commission should suspend the Privacy Shield and sanction the U.S. for breaking the umbrella agreement.

However, other observers contended that the executive order would not affect the Privacy Shield. On Jan. 26, 2017, *TechCrunch* reported that a spokeswoman for the European Commission quelled concerns about the future of Privacy Shield, noting that it "does not rely on the protections under the U.S. Privacy Act." In a Jan. 27, 2017 commentary on the International Association of Privacy Professionals (IAPP) website, IAPP Westin Fellow Cobun Keegan wrote, "[c]itizens of the EU members states, unlike those of other countries, retain privacy protections under the Privacy Act even after implementation of this executive order, however. This is due to special protections negotiated under the EU-U.S. Data Protection and Privacy Agreement (known as the 'Umbrella Agreement'), as implemented in the U.S. by the Judicial Redress Act."

In a January 30 Hogan Lovells commentary, former FTC Commissioner Julie Brill contended that President Trump's executive order "does not impact any of the U.S. commitments under the Privacy Shield, nor does it revoke protections for EU citizens under the Privacy Act provided pursuant to the Judicial Redress Act." Brill and co-writer Bret Cohen, a Hogan Lovells attorney, explained that "while the [Executive Order] permits the President to direct U.S. federal agencies to refrain from offering Privacy Act protections to citizens of foreign countries, it cannot (and does not) revoke coverage from jurisdictions already designated as covered under the Judicial Redress Act or countries that could receive such designation in the future from the Department of Justice pursuant to the Judicial Redress Act."

Furthermore, Brill and Cohen noted that "even if coverage under the Privacy Act were affected by this [Executive Order] — which it is not — it would not impact any explicit commitments

Privacy, *continued on page 30*

Privacy, *continued from page 29*

made by the U.S. under Privacy Shield. This is for a simple reason: the Privacy Shield Framework and the European Commission's official Adequacy Decision approving Privacy Shield did not rely on the Privacy Act's protections." The commentary added, "the Privacy Act addresses the right to obtain redress with respect to government databases, whereas Privacy Shield addresses privacy rights with respect to private company databases. The EO will not affect EU citizens' right to redress against Privacy Shield organizations through their independent recourse mechanisms, as well as through binding arbitration."

In the months following the executive order and throughout 2017, observers continued to note that there had been no changes related to the Privacy Shield under the Trump Administration, though concerns still remained. In an April 6 *TechCrunch* story, reporter Natasha Lomas wrote that the Privacy Shield "appear[ed] to be weathering the storm of a Trump presidency." However, Lomas also noted that "it could take just a single stroke of Trump's pen to bring the entire arrangement toppling down." She added, "a [U.S.] president apparently intent on rolling back Obama era reforms — including privacy-related ones — European lawmakers are more visibly concerned than ever."

Cameron F. Kerry, a Distinguished Visiting Fellow in Governance Studies at the Brookings Institution, wrote in a June 12 commentary that President Trump has "affirmed support for the framework [of the Privacy Shield] and its essential pillars." However, he also expressed concern with President Trump's relationship with the EU as perhaps affecting the Privacy Shield in the future. "The trouble is, the administration keeps doing other things that jeopardize support for the Privacy Shield," Kerry wrote. (For more information on President Trump's Executive Order, see *Trump Executive Order Eliminates Privacy Act Protections for Certain Non-Citizens; Threatens Privacy Shield Laws* in "Federal Government, Minnesota Court of Appeals Address Data Privacy Issues in the Winter/Spring 2017 issue of the Silha *Bulletin*.)

On March 10, 2017, Reuters reported that the European Commission Vice-President Andrus Ansip was "reassured" after U.S. Secretary of Commerce Wilbur Ross "gave no indication of any plans to change U.S. privacy protections underpinning" the Privacy Shield. Ross had met with Ansip in Washington, D.C. on March 9, where he reportedly "confirmed his support of the data transfer pact," according to a source who spoke with Reuters. Ross also indicated that the Trump Administration had no plans to change Presidential Policy Directive 28, which was ordered by President Barack Obama in 2014 and extended privacy safeguards to foreign nationals while also protecting the U.S. individuals' privacy rights against overreaching government surveillance.

A few weeks later, European Commissioner for Justice, Consumers, and Gender Equality Vera Jourová visited Washington, D.C. to further underscore the importance of the Privacy Shield, according to a March 30 *Bloomberg BNA* commentary. Prior to the meeting, in an interview with *Handelsblatt*, a media startup headquartered in Berlin, Jourová had warned the Trump administration against weakening the Privacy Shield. Nevertheless, Jourová found the late-March meeting "satisfactory" and was optimistic the Privacy Shield would remain in place. In an interview with *Bloomberg* on March 30, Jourová said, "I have to come back to Europe with such assurances and to continue working on keeping the privacy shield running." She added, "I can say I have positive feelings. I spoke to Mr. Ross, I spoke to the American Chamber of Commerce and representations of various businesses and I had a very good feeling."

> "[President Trump] has affirmed the framework [of the Privacy Shield] and its essential pillars.. . . The trouble is, the administration keeps doing other things that jeopardize support for the Privacy Shield."
>
> **— Cameron F. Kerry, Brookings Institution Distinguished Visiting Fellow in Governance Studies**

However, some EU officials remained concerned over the status of the Privacy Shield, despite the visits by Ansip and Jourová. According to a June 4, 2017 European Parliament press release, Members of the European Parliament (MEPs) adopted a resolution calling on the EU Commission to conduct "a proper assessment and ensure that the [Privacy Shield] for data transferred for commercial purposes provides enough personal data protection for EU citizens to comply with the EU Charter of Fundamental Rights and new EU data protection rules." Specifically, officials feared that deficiencies in the Privacy Shield might create an uncertain legal environment for businesses conducting trans-Atlantic data transfers. "This resolution aims to ensure that the Privacy Shield stands the test of time and that it does not suffer from critical weaknesses," said Civil Liberties Committee Chair Claude Moraes (S&D, UK) in the press release. "We acknowledge the significant improvements made compared to the former EU-U.S. Safe Harbour, but there are clearly deficiencies that remain to be urgently resolved to provide legal certainty for the citizens and businesses that depend on this agreement."

In the press release, the MEPs listed several issues they were "particularly worried about." First, the MEPs listed the recent revelations about surveillance activities conducted by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) during 2015. *Circa* first reported in May 2017 that the NSA under President Obama "routinely violated American privacy protections while scouring through overseas intercepts and failed to disclose the extent of the problems until the final days before Donald Trump was elected president last fall, according to once top-secret documents that chronicle some of the most serious constitutional abuses to date by the U.S. intelligence community."

The MEPs also listed new rules passed in 2017 "allow[ing] the NSA to share vast amounts of private data, gathered without warrant, court orders or congressional authorisation, with 16 other agencies, including the FBI." On Jan. 13, 2017, *The Intercept* reported that the Obama administration had announced these new rules as an amendment to Section 2.3 of Executive Order 12333 ("EO 12333"), which "imposes certain broad restrictions concerning the surveillance of US persons' communications under it." Signed by President Reagan in 1981, EO

12333 was initially intended to authorize foreign surveillance. The National Security Agency (NSA) stated in internal documents that EO 12333 "is the primary source of NSA's foreign intelligence-gathering authority."

Second, the MEPs expressed concern regarding the U.S. Congress "[rejecting] rules to protect the privacy of broadband customers . . . [including those] 'that would have required internet service providers to get consumers' explicit consent before selling or sharing web browsing data and other private information with advertisers.'" Third, the press release listed "vacancies on the Privacy and Civil Liberties Oversight Board" and the FTC, which is the primary data privacy regulator in the United States, as well as "insufficient independence of the Ombudsperson mechanism set up by the US Department of State" as concerns moving forward with the Privacy Shield under the Trump administration. According to the State Department, the Under Secretary of State for Economic Growth, Energy, and the Environment serves as the Privacy Shield Ombudsperson, a position "dedicated to facilitating the processing of requests from EU individuals relating to national security access to data transmitted from the European Union to the United States." Finally, the MEPs expressed concern that EU individuals, whose data is transferred to the U.S., do not have effective redress rights, despite Judicial Redress Act signed by President Obama on Feb. 24, 2016.

During a visit to Washington, D.C. between July 17 and July 21, the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) also expressed several concerns with the Privacy Shield, although LIBE and the Trump administration had both reiterated their commitment to the framework during the meeting, according to *JD Supra* on Aug. 10, 2017. Particularly, Moraes identified several positions that needed to be filled by the Trump administration, including in "the Privacy and Civil Liberties Oversight Board that [was] currently lacking four of its five commissioners and the ombudsperson." LIBE also noted that three open FTC seats remained vacant. Additionally, similar to the MEPs, Moraes raised concerns with the state of government surveillance in the United States.

In an Aug. 10, 2017 commentary, Ropes & Gray LLP partner Rohan Massey discussed the possible implications of the meeting. "LIBE's visit appears to have fulfilled its objective, which was 'to obtain up-to-date information on the state of play in the US on major topics which fall within the remit of the LIBE Committee' such as the protection of personal data and the implementation of the EU-U.S. Privacy Shield," Massey wrote. "Unfortunately, it transpires that, in Claude Moraes' words, 'Deficiencies still remain and must be urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses.'" He added, "The EU Data Protection Commissioners are due to issue their assessment of how the agreement is working by the end of the year. Sceptics might say that, in the light of the shortcomings identified by LIBE and the increasingly dysfunctional political landscape in the US, that assessment is unlikely to be entirely positive."

> "[European Parliament's Civil Liberties, Justice and Home Affairs Committee's] visit appears to have fulfilled its objective, which was 'to obtain up-to-date information on the state of play in the US on major topics' . . . such as the protection of personal data.. . . Unfortunately, it transpires that . . . 'Deficiencies still remain and must be urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses.'"
>
> **— Rohan Massey, Ropes & Gray LLP partner**

Digital Rights and Human Rights Organizations Express Concern Regarding the Privacy Shield

In July 2017, digital rights organization Access Now and two human rights organizations, Amnesty International and Human Rights Watch, expressed concern with the Privacy Shield, citing U.S. government surveillance and insufficient redress mechanisms under the Privacy Shield framework, among other criticisms. On July 5, 2017, Access Now, an international organization that defends and extends digital rights of users at risk, sent a letter to Bruno Gencarelli, Head of Unit for International Data Flows and Protection for the European Commission, in response to a Privacy Shield Review questionnaire. On July 26, 2017, Amnesty International and Human Rights Watch wrote a separate letter to the European Commission contending that "the U.S. surveillance regime renders the [EU-U.S.] Privacy Shield invalid."

On Feb. 8, 2017, Access Now had sent a letter to EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová and European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) Chair Claude Moraes asking for the suspension of the Privacy Shield. The letter contended that "U.S. law, including representations made by officials in annexes to the Privacy Shield, is . . . insufficient to protect Europeans' data under the legal criteria set out by these laws and the Court of Justice of the European Union." The letter also listed several "significant changes have been introduced to U.S. law and policy that even further degrade the protections for Europeans' data," which Access Now would elaborate on in its July letter to Gencarelli.

In a February 8 press release discussing the letter, Amie Stepanovich, U.S. Policy Manager at Access Now, wrote, "[The Trump] administration has made it clear that it has little regard for the rights of many classes of people, including anyone who lives outside of the United States.. . . As the operator of the largest and most well-funded surveillance apparatus in the world, the US owes a specific duty to respect human rights." She continued, "President Obama had taken small steps in that direction, but this White House is not only moving to erase that progress, but to move us even further backward and subvert any semblance of international leadership this country once had."

However, in the July 5 letter to Gencarelli, rather than call for the suspension of the Privacy Shield, Access Now instead called for reforms because the framework is "highly important to

Privacy, *continued on page 32*

Privacy, *continued from page 31*

providing a rights-respecting internet infrastructure." Specifically, Access Now argued that the Privacy Shield "must comply with international and European human rights law, including on data protection. In order to ensure that this is the case, the European Commission should subject the Privacy Shield and U.S. practices implicating the rights of people in the EU to an exacting review."

The first section of the letter addressed Gencarelli's request for feedback regarding legislative, regulatory, administrative or case-law developments in the United States since August 2016 that were "relevant for compliance by certified U.S. companies with their obligations under the Privacy Shield." Access Now listed several developments, including those it had discussed in its February letter to the European Commission. One such development was President Donald Trump's Jan. 25, 2017 executive order directing executive departments and agencies to strengthen their enforcement of federal immigration laws, which "demonstrated a disregard for the rights of any non-Americans."

Access Now also included a discussion of Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), 50 U.S.C.A. § 1881a, which provides authority for the United States government's "downstream" and "upstream" surveillance programs. The National Security Agency (NSA) defines "downstream" surveillance, previously referred to as PRISM, as "acquir[ing] communications 'to or from' a Section 702 selector (such as an email address)," according to an April 28, 2017 NSA statement. "Upstream" surveillance is defined as "acquir[ing] communications 'to, from, or about' a Section 702 selector."

Access Now contended in its letter that "[t]hese programs, which are targeted at non-U.S. persons, are exceptionally broad." The digital rights organization explained that Section 702 "does not require government agents to request surveillance related to specific targets.. . . Because of the broad nature of these programs, for anyone outside the United States, the issue is less about how 702 authority is 'abused' and more about the inherently privacy-invasive and harmful ways it can permissibly be used."

The letter to Gencarelli also noted that Director of National Intelligence (DNI) Dan Coats, in a June 2017 Congressional hearing, "disavowed" the commitment he made to "[provide] an estimate of the number of U.S. Persons which have had their communications incidentally collected under Section 702," which would have provided "necessary transparency into surveillance programs."

In the second section of the letter, Access Now contended that the redress mechanisms found under the Privacy framework "are inadequate to protect EU persons." First, the organization found that the Privacy Shield Ombudsperson, a new redress mechanism created under the Privacy Shield, "has not lived up to its promise" because the position is "not adequately independent from the intelligence community," "lacks investigatory powers," and "was not filled for several months" under the Trump Administration." Second, Access Now argued that other redress mechanisms under the Privacy Shield had failed because "the available avenues under Privacy Shield are dependent on mostly unenforceable self-regulation.. . . Instead of concrete remedies, like fines, compensation for the individual, or an order for a change in corporate practice, the most likely outcome of pursuit of redress under Privacy Shield is, at most, the removal of a company from the Privacy Shield."

> "[The Trump] administration has made it clear that it has little regard for the rights of many classes of people, including anyone who lives outside the United States.. . . As the operator of the largest and must well-funded surveillance apparatus in the world, the US owes a specific duty to respect human rights."
>
> **— Amie Stepanovich, Access Now U.S. Policy Manager**

Before concluding, the letter listed additional information the European Commission may find useful, including the U.S. Supreme Court agreeing to hear *Carpenter v. United States*, which presents the question of whether government actors need a warrant to obtain historical data from cell phone carriers detailing the movements of a cellphone user, known as cell site location information (CSLI). Access Now then listed several recommendations to Gencarelli, including that the European Commission work with U.S. Congress "to promote the implementation of meaningful reforms to Section 702 to increase respect for the human rights of people in the EU, particularly in regard to transparency" and "to promote stronger human rights language in the proposed amendment to the U.S. Electronic Communications Privacy Act." Access Now also recommended that the European Commission amend the Privacy Shield's redress mechanisms and work with the Article 29 Working Party, which provides independent advice on data protection matters to the European Commission and helps develop data protection policies in the EU Member States. Finally, Access Now recommended that the EU "[c]ommit publicly to transparency by publishing all relevant documents, working papers, and findings from the Privacy Shield review process." Access Now's full letter is available online at: https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf.

On July 26, 2017, in a letter to the European Commission, Amnesty International and Human Rights Watch "urge[d] the European Commission to re-evaluate its *Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield*." The human rights organizations argued in their letter addressed to European Commissioner for Justice, Consumers, and Gender Equality Vera Jourová that "the U.S. surveillance regime render the [EU-U.S.] Privacy Shield invalid." They wrote that "the [United States] does not ensure a level of fundamental rights protection regarding the processing of personal data that is essentially equivalent to that guaranteed within the European Union."

Furthermore, the organizations wrote that they "believe[d] the Commission's conclusions regarding the adequacy of rights protections afforded by the US [were] incorrect because . . . [the United States] demonstrably fall far short of essential equivalence to the standards set out in EU law and do not

comport with international human rights guarantees." They added, "We are also concerned about the lack of safeguards applicable to US intelligence-sharing arrangements with other states and of effective remedies for fundamental rights violations stemming from intelligence surveillance activities." The letter was signed by U.S. Program of Human Rights Watch Co-Director Maria McFarland Sánchez-Moreno and Iverna McGowan, the Head of European Institutions Office and Advocacy Director for Amnesty International.

Attached to the letter was a "Human Rights Watch and Amnesty International Briefing," which was an "Assessment of the Compliance of US Surveillance Laws and Practices with EU Law." In the assessment, Human Rights Watch and Amnesty International expanded on their concerns regarding U.S. government surveillance. More specifically, the organizations first discussed their concern with Executive Order 12333 (EO 12333), the "primary source of NSA's foreign intelligence-gathering authority." However, the organizations contended that EO 12333 "appears to grant free rein to the agencies to conduct surveillance overseas of the communications of non-US persons who are outside the US."

Additionally, the organizations noted that EO 12333 "allows the Director of National Intelligence to 'enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations.'" The organizations found it problematic that the NSA and FBI could disseminate personal data to other agencies "without any requirement of a suspicion of wrongdoing and without any individualized approval by an independent body."

Second, like Access Now, the organizations explained their concern regarding the breadth of Section 702 of the FAA. The assessment read, "although the executive branch has sought to portray Section 702 monitoring as 'subject to … independent judicial supervision' . . . we observe that this supervision is limited to the approval of certain procedures rather than specific decisions to obtain or gain access to personal data." Thus, because the surveillance is "broad and not limited to what is strictly necessary to achieve a legitimate objective" and there are "insufficient safeguards to guarantee against abuse," the organizations concluded that Section 702 is "noncompliant with EU fundamental-rights standards."

Third, the assessment discussed the human rights organizations' concerns with Presidential Policy Directive 28 (PPD-28), which allows the U.S. to collect "signals intelligence in bulk" without specifying that bulk collection be "strictly necessary," according to the assessment. Furthermore, the organizations contended that PPD-28 "contains several significant loopholes," further raising concerns about the extent of U.S. government surveillance. Finally, Human Rights Watch and Amnesty International contended that the United States lacks an "effective" remedy for abuses," despite repeated emphasis of its importance by the Court of Justice of the European Union (CJEU).

Thus, the organizations called on the European Commission "to encourage the US legislative and executive branches to adopt the necessary binding reforms so that the transfer of personal data to the United States does comply with the requirements of the Charter of Fundamental Rights of the EU, the Data Protection Directive, and the General Data Protection Regulation." The full letter and attachments are available online at: https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-EU-U.S.-privacy-shield.

High Court of Ireland Refers *Schrems II* to European Court of Justice; Schrems Faces Legal Setback in Complaint against Facebook Ireland in Austrian court

On Oct. 3, 2017, the High Court in Ireland requested that the European Court of Justice (ECJ) consider a case determining 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. *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Case No. 2016 4809P (*Schrems II*). In February and March 2017, experts on U.S. privacy and data transfer law provided testimony in *Schrems II*, which arose after Austrian data privacy activist Maximillian Schrems filed a renewed complaint in December 2015 regarding Facebook's use of SCCs. Meanwhile, on Nov. 14, 2017, Advocate General Michal Bobek, one of the EU's top law officers who advises the ECJ, found that Schrems would likely not be able to bring a class action case against Facebook Ireland in Austrian court, but could instead bring only his personal claims against the social media company for violation of his own privacy and data protection rights.

Schrems II arose following the CJEU's October 2015 decision to invalidate the EU-U.S. Safe Harbor framework (*Schrems I*). Facebook switched to using SCCs with the belief that they would provide adequate privacy protections for its users, according to a Sept. 22, 2017 story by *The Irish Times*. On Dec. 1, 2015, Schrems filed a renewed complaint to the Data Protection Commissioner of Ireland (DPC), Helen Dixon, asking her to halt data transfers under SCCs, according to a Sept. 11, 2017 *Lawfare* commentary. In the complaint, Schrems contended that SCCs do not provide adequate legal protection necessary to permit personal data transfers, including between Facebook Ireland and Facebook's headquarters in the United States. Schrems added that U.S. surveillance law was not in line with the *Schrems I* ruling. Schrems' full complaint is available online at: http://www.europe-v-facebook.org/comp_fb_ie.pdf.

According to an Electronic Privacy Information Center (EPIC) summary of *Schrems I* and *Schrems II*, 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 to regulate the transfer of data provide for or raise the level of protection that previously existed under the Safe Harbor framework, according to EPIC.

In May 2016, Dixon issued a Draft Decision, in which she explained her preliminary view that Schrems' complaint was "well-founded," as reported by *The Irish Times*. 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 these concerns, making them invalid under EU law.

However, because the SCCs issued under the authority of the European Commission had been deemed by the Commission to authorize data transfers, Dixon argued she did not have the authority to declare the SCCs invalid under EU law, according to EPIC. Furthermore, Dixon contended that she

Privacy, *continued on page 34*

Privacy, *continued from page 33*

could not complete the investigation into Facebook without a Court of Justice of the European Union (CJEU) ruling that the clauses were, in fact, invalid. Consequently, Dixon referred the case to the Irish High Court, Commercial Division and asked the court to refer the question of whether SCCs used by companies to transfer personal data are valid to the CJEU.

The proceedings in the Irish High Court began on Feb. 7, 2017 and lasted 21 days. During this period, the DPC provided her opening argument and explained the relevant EU and U.S. laws and authorities to the court. Additionally, several experts provided testimony, including Peter Swire, a professor in the Georgia Institute of Technology Scheller College of Business, 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." He also cited a team of "Oxford experts," who concluded that the United States "now serves as a baseline for foreign intelligence standards." Additionally, Swire described possible safeguards for law enforcement surveillance, and compared U.S. safeguards to those in the EU.

Second, Swire documented "how the U.S. legal system provides numerous ways for an individual to remedy violations of privacy." The remedies included "individual suits against service providers; Federal Trade Commission and other agency enforcement; state law protections; and class action litigation." Swire further explained the reasons behind national security exceptions to individual access to surveillance records, providing a hypothetical scenario in which a "hostile actor" was able to gain direct access to individuals' personal data from a U.S. government agency, such as the National Security Agency (NSA).

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" and that "the FISC provides independent and effective oversight over US government surveillance."

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. Swire argued that the implications "appear to go beyond the EU and US, as shown by analysis of surveillance rules in the BRIC countries – Brazil, Russia, India, and China." Swire continued, "For those and other countries whose safeguards are weaker than in the U.S., a finding of inadequate protections in the U.S. would logically mean that transfers from the E.U. to these countries would similarly be prohibited." Furthermore, Swire contended that an "inadequacy finding" for SCCs could also apply to other laws and frameworks regarding the transfer of personal data, including the Privacy Shield. Thus, Swire contended that "finding of inadequacy in the current case in Ireland could have far more sweeping ramifications than many observers have contemplated." Swire's complete document detailing his testimony is available online at: https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony.

> "[SCCs] provide critical safeguards to ensure that Europeans' data is protected once transferred to companies that operate in the U.S. or elsewhere around the globe, and used by thousands of companies to do business.. . . They are essential to companies of all sizes, and upholding them is critical to ensuring the economy can continue to grow without disruption."
>
> **— October 2017 Facebook statement**

On October 3, 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 contended that the case "raises issues of very major, indeed fundamental, concern to millions of people within the European Union and beyond" because it addresses data protections rights for EU residents and implicates "billions of euros worth of trade." She added, that the DPC had "raised well-founded concerns that there is an absence of an effective remedy in US law for an EU citizen whose data are transferred to the US where they may be at risk of being accessed and processed by US state agencies for national security purposes in a manner incompatible."

She also noted that "it is clear that there is mass indiscriminate processing of data by the United States government agencies, whether this is described as mass or targeted surveillance," citing the PRISM and Upstream programs by the National Security Agency (NSA), authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), 50 U.S.C.A. § 1881a.

Costello concluded that neither three CJEU 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 "lacks 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 [ECJ] for a preliminary ruling." Costello's full decision is available online at: http://www.europe-v-facebook.org/sh2/HCJ.pdf.

In a statement, Facebook defended the use of SCCs. "[SCCs] provide critical safeguards to ensure that Europeans' data is protected once transferred to companies that operate in the U.S. or elsewhere around the globe, and used by thousands of companies to do business," Facebook wrote. "They are essential to companies of all sizes, and upholding them is critical to ensuring the economy can continue to grow without disruption."

In a separate statement, Schrems wrote, "In simple terms, US law requires Facebook to help the NSA with mass surveillance and EU law prohibits just that.. . . As Facebook is subject to both jurisdictions, they got themselves in a legal dilemma that they cannot possibly solve in the long run."

In an October 3 commentary for *The Recorder*, reporter Ben Hancock noted that a final decision by the CJEU "is likely still years away." However, he explained that Costello's referral of the case "creates the possibility that the EU's highest court will find that those clauses, no matter how they are constructed, are invalid because of U.S. surveillance practices. In other words, even if companies spend the next year making SCCs complaint under the new regulation, there is risk that they could be wiped away."

As the *Bulletin* went to press, Costello had not announced the exact questions sent to the CJEU.

Meanwhile, Schrems was dealt a legal blow in a complaint against Facebook Ireland in Austrian court. Advocate General Bobek issued an opinion on Nov. 14, 2017 stating that Schrems could sue Facebook Ireland based on his own privacy claims, but could not file a class action lawsuit against the social media company. *Schrems v. Facebook Ireland Limited* Case C-498/16.

According to Bobek's opinion, Schrems was seeking €500 ($576) in damages on behalf of 25,000 people who signed up as volunteers on his website to be part of efforts to sue Facebook over numerous infringements of Austrian, Irish, and EU data protection rules. Of the 25,000, seven Facebook users' assigned claims were included in the proceedings before Bobek.

The Austrian court of first instance, the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters, Vienna, Austria), dismissed the application. The appeals court, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) altered that decision in part, allowing Schrems' personal claim against Facebook, but dismissing the assigned claims brought by the seven Facebook users. The court held that "the jurisdiction rules for consumers can be used to the advantage of a consumer only by those who are parties to a legal action." Schrems and Facebook both appealed the decision before the Austrian Supreme court, which stayed the national proceedings and referred the case to Advocate General Bobek.

In his November 14 opinion, Bobek found that Schrems could not bring a class action suit against Facebook Ireland in an Austrian court. Bobek wrote, "A consumer who is entitled to sue his foreign contact partner in his own place of domicile, cannot invoke, at the same time as his own claims, claims on the same subject assigned by other consumers." He continued, "The jurisdictional consumer privilege is always limited to the concrete and specific parties to the contract.. . . It would be incompatible with these rules to allow a consumer to also make use of this privilege for claims assigned to him by other consumers purely for litigation purposes." Bobek added that a class action suit, also known as collective redress, "could lead to unrestrained targeted assignment to consumers in any jurisdiction with more favourable case-law."

"A consumer who is entitled to sue his foreign contact partner in his own place of domicile, cannot invoke, at the same time as his own claims, claims on the same subject assigned by other consumers."

— Michal Bobek, Court of Justice of the European Union Advocate General

However, Bobek ruled that Schrems could bring his own claims against the social media company." He found that Schrems should be considered a consumer under EU law, making it possible for him to bring his own case. Bobek wrote, "Knowledge, experience, civic engagement or the fact of having reached certain renown due to litigation do not in themselves prevent someone from being a consumer." Bobek's full opinion is available online at: http://www.europe-v-facebook.org/sk/GA_opinion.pdf.

According to Reuters on Nov. 14, 2017, the advocate general's opinion is non-binding, though it is often followed by the ECJ. *EU Observer* noted on November 14 that the ECJ would likely rule on the case early in 2018. As the *Bulletin* went to press, no further legal proceedings had been announced.

In a November 14 statement, Schrems wrote that Bobek's ruling still allowed him to "at least bring a 'model case' at my home jurisdiction in Vienna, which may enable us to debate the illegal practices of Facebook in an open court for the first time."

However, Schrems also criticized Bobek's ruling against the class action suit. He wrote, "The consequence would be that thousands of courts in the whole European Union would have to deal with an identical, but local lawsuit against Facebook. Bringing a case in Ireland is equally impossible, because the legal costs for a data protection lawsuit of €500 could easily lead to legal costs of 10-20 million under the Irish system." He added, "I hope that the five judges that will ultimately decide over this case will take a closer look and will not follow the advocate general. I had the impression that the advocate general was more critical during the hearing, which may have led to this opinion."

UK and Germany Take Action Related to Implementation of the General Data Protection Regulation; Article 29 Working Party Provides Guidance for GDPR Implementation

In 2017, the United Kingdom (UK) and Germany, as well as the Article 29 Working Party, which provides the European Commission with independent advice on data protection matters and helps develop data protection policies in the EU Member States, took steps related to the implementation of the General Data Protection Regulation (GDPR). The GDPR, adopted by the EU in Spring 2016 to harmonize data privacy laws across Europe and to protect EU citizens' data privacy rights, will become effective in 2018. On Jan. 17, 2017, UK Prime Minister Theresa May announced that any current EU laws governing data privacy would remain in effect after the country's exit from the EU (Brexit), and that the UK would adopt GDPR provisions. Additionally, in July and September 2017, Parliament proposed legislation intended to harmonize UK privacy law with the GDPR. On April 27, 2017, Germany passed the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) to further supplement and define the GDPR within Germany, though observers raised concerns that several provisions were in conflict with or exceeded the GDPR. Finally, on April 5, 2017, the Article 29 Working Party approved revised guidance interpreting elements of the GDPR, including on the appointment of data protection officers (DPOs). On October 3, the Article 29 Working Party provided additional guidance related to administrative

Privacy, *continued on page 36*

Privacy, *continued from page 35*

fines levied against organizations or companies that violate provisions of the GDPR.

On April 27, 2016, the EU formally adopted the GDPR, which replaces the Data Protection Directive 95/46/EC. The GDPR, which will become effective on May 25, 2018, creates new obligations and responsibilities for data controllers and processors, while also expanding EU residents' privacy rights.

According to a July 7, 2017 posting by Bird & Bird, an international law firm, although GDPR provisions prevail over national law, EU Member States "retain the ability to introduce their own national legislation based on certain derogations provided for by the GDPR. These derogations include national security, prevention and detection of crime, and also apply in certain other important situations – the so-called 'opening clauses.'" Otherwise, national laws must align with the GDPR.

Article 85 of the GDPR provides for exemptions from the rules on protecting personal data where that data is used solely for journalistic purposes or for artistic or literary expression. However, these exemptions apply only if necessary to reconcile the right to privacy with the rules governing the freedom of expression. National governments will be required to put legislative measures in place to implement this exemption, which will be enforced by local regulatory authorities. (For more information about the passage of the GDPR and the key provisions, see *Adopted EU General Data Protection Regulation Establishes 'Right to Erasure'* in "Right to Be Forgotten Continues to Create Challenges for Online Entities" in the Summer 2016 issue of the Silha *Bulletin*.)

On Jan. 17, 2017, UK-based technology and business website *V3* reported that Prime Minister Theresa May had outlined her plans for Brexit, making clear that the UK would withdraw from both the European Union (EU) and its single business market. However, as part of this process, Prime Minister May created an "Article 50" letter detailing what changes and compromises would take place as the UK negotiated its exit from the EU. One notable aspect was that existing EU laws in force in the UK would be converted into full UK laws. Therefore, the GDPR's provisions would be in effect in the UK, even after it leaves the EU, according to *V3*.

On July 13, 2017, the Parliament of the United Kingdom published the Great Repeal Bill, also known as the EU Withdrawal Bill, which, if passed, would annul the 1972 European Communities Act and convert all existing EU law into UK law as part of Brexit. HC Bill 5. The bill would also provide for UK courts to refer to EU court rulings when interpreting the UK's EU-derived laws. In effect, the bill proposes that existing case law from the Court of Justice of the European Union (CJEU) will have the same binding status as UK Supreme Court rulings, and anticipates that the Court will depart from CJEU precedent in very rare cases. The full text of the bill is available online at: https://publications.parliament.uk/pa/bills/cbill/2017-2019/0005/18005.pdf.

Meanwhile, on Sept. 14, 2017, *Bloomberg BNA* reported that Parliament had introduced the UK Data Protection Bill the day before in order to harmonize UK privacy law with the GDPR by incorporating the majority of GDPR provisions, regardless of Brexit. The full text of the bill, HL Bill 66, is available online at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_1.htm.

The legislation "will give people more control over their data, support businesses in their use of data, and prepare Britain for Brexit," Culture Secretary Karen Bradley said in a statement launching the proposed legislation. If the bill is enacted, UK businesses would have to be GDPR compliant by May 2018. "If you are still in denial and relying on Brexit to relieve you from the GDPR, then think again," Vic Bange, a partner in the information technology, telecoms and competition group at London-based Taylor Wessing LLP, told Bloomberg BNA.

On April 27, 2017, the German Parliament passed the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), which aimed to supplement and further define provisions of the GDPR. The passage of the law raised concerns from observers about how the national law would potentially conflict with or exceed the GDPR.

According to Bird & Bird on July 6, 2017, the BDSG provides several new provisions relevant to the private sector, including the collection and use of employee data, administrative fines, and the processing of sensitive data. The German Federal Council approved the BDSG on May 12, 2017, and it will go into effect on May 25, 2018. However, observers expressed concerns that several provisions in the BDSG exceeded the scope of the GDPR, as reported by Fieldfisher on April 24.

The first area of concern involved administrative fines and penalties. Article 83 of the GDPR details the number of fines that can be levied against companies who violate the regulation. The BDSG provides for fines against individuals within the company, as well as potential prison sentences of up to three years for any violation of the Act.

Second, Fieldfisher explained that section 22 of the BDSG provides for the lawful processing of special categories of personal data found in the GDPR, including related to health and social services. Under section 22, public and private bodies may process special categories of personal data if it is "necessary to exercise the rights derived from the right of social security . . . necessary for the purposes of preventive medicine [or] medical diagnosis[,] . . . [and] necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats . . . or ensuring high standards of quality and safety." Public bodies, under section 22, may also process personal data related to health and social services if it is of "substantial public interest" or to prevent "substantial harm" and "threat[s] to public security." However, section 22 requires that in these cases of processing personal data, "appropriate and specific measures shall be taken to safeguard the interests of the data subject." The section includes several considerations, such as the designation of a DPO, the encryption of personal data, and a series of organizational measures, among other considerations.

Despite these protections, Fieldfisher and other experts raised concerns with a connected section of the BDSG, section 27, which allows for the processing of personal data related to scientific or historical research without consent of the data subject, so long as the processing "is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data." Although Section 27 does state that the controller must take "appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22," observers noted that the section "seems to be a quite generous exemption that

allows for a flexible interpretation." Fieldfisher also noted that the high level of protection for special categories of personal data provided for by the GDPR "experiences another dilution" in this section of the BDSG.

The third area of concern is that the BDSG deviates from the GDPR in terms of the required DPO appointment. The BDSG requires that every company that has at least 10 employees who work with automated personal data processing must appoint a DPO, whereas the GDPR requires companies to do so only in exceptional cases. Experts contended that this may cause additional financial burdens to companies doing business in Germany.

Finally, in 2017, the Article 29 Working Party, the short name for the Data Protection Working Party established by Article 29 of Directive 95/46/EC, provided guidance interpreting elements of the GDPR, including related to administrative fines and to the appointment of data protection officers (DPOs), who are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

On April 11, 2017, Bird & Bird wrote that the Article 29 Working Party had released a draft guidance related to the GDPR in December 2016, which was followed by a period of open public consultation that ran through the end of January 2017. The Article 29 Working Party approved revised guidance on April 5 during its plenary session, focusing primarily on the role of an organization or company's DPO. Among the new points raised in the revised guidance, the Article 29 Working Party contended that systematic DPO assessments must be "kept up-to-date and can be requested at anytime" in order to achieve greater accountability. The guidance also stated that although there can only be one DPO in an organization, they can be supported by a team and should be located within the EU. The full guidance is available online at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

On Oct. 3, 2017, the Article 29 Working Party released additional guidance on the application and setting of administrative fines, which are levied against organizations who violate GDPR provisions. The guidance stated that administrative fines "should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified."

The Article 29 Working Party further provided that the supervisory authorities in member states must identify corrective measures most appropriate for addressing the specific infringement(s) by assessing "each individual case." Article 83(1) of the GDPR states that corrective measures, including administrative fines, must be "effective, proportionate and dissuasive." The supervisory authorities must then apply the criteria listed in Article 83(2) of the GDPR when deciding whether to impose an administrative fine and determining the amount of such fine in each individual case. Among the criteria to be considered are "the nature, gravity and duration of the infringement," as well as "the intentional or negligent character of the infringement." Authorities must also consider any action taken to mitigate the damage to data subjects, the degree of cooperation, previous infringements, and the categories of personal data affected by the infringement, among several other considerations. The full guidance is available online at: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

Scott Memmel
Silha *Bulletin* Editor

Ashley Turacek
Silha Research Assistant

Director's Note

The Fall 2017 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 took place in New York City in November 2017. Professor Kirtley gratefully acknowledges the contributions of Silha research assistants Casey Carmody, Scott Memmel, and Ashley Turacek.

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

Utah District Court, Minnesota Court of Appeals Address First Amendment Questions

In the fall of 2017, the U.S. District Court for the District of Utah, Central Division and the Minnesota Court of Appeals considered whether statutes in their respective states were unconstitutionally overbroad and restricted protected speech under the First Amendment. On August 31, Utah Federal District Court Judge David Nuffer ruled that a section of the state's Alcoholic Beverage Control Act, Utah Code Ann. § 32B-1-504, which prohibits establishments from selling alcohol while showing sex acts or nudity, was "overinclusive" and restricted First Amendment protected content. On September 11, the Minnesota Court of Appeals ruled that a statute prohibiting a political candidate from knowingly making a false claim regarding support or endorsement by a major political party is not unconstitutionally overbroad because the First Amendment does not allow false claims during the course of political campaigns.

FIRST AMENDMENT

Utah District Court Judge Rules in Favor of Movie Theater in First Amendment Case

On Aug. 31, 2017, a federal district court judge in Utah struck down a state law prohibiting establishments from selling alcohol while showing sex acts or nudity. *Cinema Pub. LLC v. Petilos*, 2017 WL 3836049 (D. Utah 2017). U.S. District Court for the District of Utah, Central Division Judge David Nuffer ruled that Section 7 of the state's Alcoholic Beverage Control Act, Utah Code Ann. § 32B-1-504 (Section 7), was "overinclusive," because it included "many films that are far removed from what is colloquially termed 'hard core,' or even 'soft core,' pornography" and, therefore, imposed "unacceptable limitations on speech that the State admits should be accorded full First Amendment protection."

The case arose in February 2016 when Brewvies, a local movie theater, allowed customers over 21 to have the option of purchasing beer during a screening of "Deadpool," a movie that includes several instances of nudity and scenes involving sexual activity between characters. The Utah State Bureau of Investigation submitted a complaint to Utah's Department of Alcoholic Beverage Control (DABC), alleging that Brewvies had violated the state's Alcoholic Beverage Control Act.

On April 17, 2016, Brewvies filed a civil rights lawsuit under 42 U.S.C. § 1983 in the United States District Court for the District of Utah against the DABC, citing an infringement of its First Amendment rights. Brewvies attorney Rocky Anderson argued that the state's statute regulating liquor establishments was antiquated and unconstitutional, calling the regulations a "chilling effect on free speech" when the DABC "threaten[ed] to punish Brewvies for showing films protected under the First Amendment and the Utah Constitution." (For more information on the events leading to the case, see *Movie Theater Faces Revocation of Liquor License after Showing "Deadpool"* in "Media Law Issues at Forefront in Several States" in the Winter/Spring 2016 issue of the Silha *Bulletin*.)

> "We felt, from Day One, the statute is egregiously unconstitutional.. . . Our view has been that the attorney general should have met the highest obligation of that office, and vindicated the people's constitutional rights."
>
> **— Rocky Anderson, Brewvies attorney**

On Aug. 31, 2017, Nuffer ruled in favor of Brewvies, finding that Section 7 violated the First Amendment. First, Nuffer considered whether it regulated protected speech. He listed the "so-called exceptions" to protected speech, which include obscenity, defamation, fraud, incitement, and speech integral to criminal conduct. Nuffer concluded, based on court documents submitted by the DABC (the State), that the State did not argue that any of the exceptions were applicable. Thus, Nuffer wrote, Section 7 "necessarily includes material within the full protective force of the First Amendment" because it regulated a movie that contained only protected speech.

Next, Nuffer considered whether strict scrutiny was the appropriate test. The State argued that a less exacting intermediate scrutiny test applied because the purpose of Section 7 "was to avoid negative secondary effects." Nuffer explained that the U.S. Supreme Court has found that a content-based law "may be subjected to lower scrutiny if the legislature's purpose in enacting the law was not aimed at the content, 'but rather at the secondary effects [of that content] on the surrounding community.'" Nuffer concluded that strict scrutiny was, in fact, the appropriate test because the secondary effects doctrine "has only been applied to 'regulations affecting physical purveyors of adult sexually explicit content,'" citing *Free Speech Coalition, Inc. v. Attorney General United States*, 825 F.3d 149, 161 (3rd Cir. 2016). Because Brewvies "is not primarily a business centered on explicit sexual activity," it does not fall under the secondary effects doctrine, according to Nuffer.

Finally, Nuffer found that the law failed strict scrutiny, which "requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." According to Nuffer, in order to be "narrowly tailored," the compelling interest "must be the 'least restrictive means among available, effective alternatives.'" The State raised only one government interest in support of the law, which was the avoidance of negative secondary effects stemming from combining alcohol with sexually explicit images. Nuffer wrote that although this may be a compelling government interest, Section 7 "is not the least restrictive means for accomplishing it." Nuffer found that because Section 7 reached "many films that are far removed from what is colloquially termed 'hard core,' or even 'soft core,' pornography," it imposed "unacceptable limitations on speech that the State admits should be accorded full First Amendment protection." Therefore, Section 7 is "overinclusive," meaning it "punishes a substantial amount of protected free speech, judged in relation to the statute's plainly legitimate sweep." Nuffer also noted that Idaho amended a similar statute to "substantially narrow [its] scope," further demonstrating less restrictive means of accomplishing the State's compelling interest in Section 7.

Following the ruling, Anderson said he was not surprised by the decision. "We felt, from Day One, the statute is egregiously unconstitutional," he told *The Salt Lake Tribune*. "Our view has been that the attorney general should have met the highest obligation of that office, and

vindicated the people's constitutional rights."

In an interview with FOX 13 in Salt Lake City, Anderson added that he did not believe the case would go any further. "I can't imagine the state appealing this case. It's rock solid under the law," Anderson said. "They would be absolutely foolish and it would cost them in the long run, I think hundreds of thousands more because they're going to be liable for attorneys fees incurred by Brewvies in this matter." As the *Bulletin* went to press, Utah Attorney General Sean Reyes had not announced whether the State intended to appeal Nuffer's ruling.

Minnesota Court of Appeals Upholds Law Preventing False Claims During Political Campaigns

On Sept. 11, 2017, the Minnesota Court of Appeals upheld a lower court ruling that the First Amendment does not protect false claims during the course of political campaigns. *Linert v. MacDonald*, 2017 WL 3974403 (Minn. Ct. App. 2017). The court concluded that Section 211B.02 of the Minnesota Fair Campaign Practices Act, Minn. Stat. § 211B.02, which prohibits a political candidate from knowingly making a false claim regarding the support or endorsement of a major political party, party unit, or organization, was not unconstitutionally overbroad because it was "narrowly tailored to serve the state's compelling interest in promoting informed voting and protecting the political process."

The case arose in 2016 when relator Michelle MacDonald, then a candidate for the Minnesota Supreme Court, sought the endorsement of the Republican Party of Minnesota (RPM), which had previously endorsed her in an unsuccessful 2014 campaign. MacDonald was interviewed by the RPM's judicial election committee, which is authorized to recommend candidates for endorsement, but cannot endorse candidates itself. Although the committee voted 20-2 to recommend MacDonald's endorsement, the party decided not to endorse any candidate in the race.

On Oct. 18, 2016, the Minneapolis *Star Tribune* published a "Voter Guide," which contained information submitted by candidates running for various government offices in the state. Included in the information submitted by MacDonald and published in the guide was an endorsement that read "GOP's Judicial Selection Committee 2016." On October 21, MacDonald requested that information be removed from her profile, and the *Star Tribune* complied.

Minnesota residents Barbara Linert and Steven Timmer filed a complaint with the Minnesota Office of Administrative Hearings (OAH), alleging that MacDonald, in claiming the RPM's judicial election committee endorsed her, had violated state law. Specifically, the respondents contended that MacDonald violated Minn. Stat. § 211B.02, titled "False Claim of Support," which prohibits an individual or political candidate from "knowingly mak[ing], directly or indirectly, a false claim stating or implying that a candidate or ballot question has the support or endorsement of a major political party or party unit or of an organization." The statute further provides that "[a] person or candidate may not state in written campaign material that the candidate or ballot question has the support or endorsement of an individual without first getting written permission from the individual to do so."

On Nov. 5, 2016, the *Star Tribune* reported that an administrative law judge (ALJ) had found probable cause that MacDonald had violated state campaign law. Judge Jessica Palmer-Denig's ruling sent the complain to a panel of three ALJs, who determined that MacDonald had violated the statute "by knowingly claiming an endorsement that she had not in fact received" and levied a $500 civil penalty against the candidate. MacDonald appealed the case on the grounds that because the statute prohibits speech based on its content, it implicates the First Amendment.

Judge Louise Bjorkman wrote the opinion of the Minnesota Court of Appeals. Bjorkman began by explaining that statutes regulating the content of speech can "survive First Amendment strict-scrutiny analysis only if they are necessary to serve a compelling state interest and are narrowly drawn to achieve that end." Bjorkman wrote that a statute is narrowly tailored if it "advances a compelling state interest in the 'least restrictive means among available, effective alternatives.'"

Bjorkman explained that one such compelling interest is "promoting informed voting and protecting the political process" and that MacDonald had contended that Minn. Stat. § 211B.02 "is not narrowly tailored to serve this compelling interest because it is facially overbroad," meaning it prohibits constitutionally protected activity. MacDonald also argued that the statute "substantially sweeps outside this aim and chills truthful political speech because 'a candidate cannot truthfully report a sub-unit's endorsement without threat of a violation that the statement is false because [the RPM] did not endorse.'"

However, the court ruled that the statute was not constitutionally overbroad for four reasons. First, Bjorkman wrote that the statute "on its face only prohibits a candidate from making a 'knowingly . . . false claim.'" Therefore, truthful political speech was not prohibited by the law, according to Bjorkman.

Second, the court rejected MacDonald's claim that the statute prohibited a candidate from truthfully reporting a party sub-unit's endorsement. Bjorkman agreed with the OAH's determination that MacDonald violated the statute "by claiming that the judicial-election committee endorsed her when it had not and lacked the authority to do so." She wrote, "It is the falsity of her statement that the committee endorsed her candidacy that violated the statute."

Third, the court determined that there were no apparent less-restrictive means of promoting the state's compelling interest regarding informed voting and the protection of the political process from false claims.

Finally, the court ruled that the threat of prosecution under Minn. Stat. § 211B.02 does not chill truthful speech. MacDonald contended that candidates are "easy targets" for meritless complaints and the statute therefore discourages candidates from making truthful claims of support or endorsement. Bjorkman explained that "the statutory complaint process contains procedural safeguards to protect against such abuse," including a review by an ALJ within three days of filing. Bjorkman also noted that complaints against candidates' claims of support or endorsement "must be submitted under oath, further discouraging the filing of false complaints."

Therefore, the appeals court concluded that Minn. Stat. § 211B.02 was not unconstitutionally overbroad because it was "narrowly tailored to serve the state's compelling interest in promoting informed voting and protecting the political process and does not substantially sweep outside the statute's legitimate aim." Thus, the court affirmed OAH's decision and upheld the fine levied against MacDonald. As the *Bulletin* went to press, MacDonald had not announced whether she would appeal the decision.

Scott Memmel
Silha *Bulletin* Editor

Civil Rights Organizations, Federal Agency, and House of Representatives Raise Different Issues Regarding Searches at U.S. Borders

In the fall of 2017, civil rights organizations raised renewed legal questions regarding the searches and seizures of individuals' electronic devices at U.S. borders, while a federal agency continued efforts to require immigrants to the United States to turn over social media account information and the U.S. House of Representatives passed legislation augmenting surveillance at U.S. borders. In a September 13 lawsuit, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the ACLU of Massachusetts contended that the warrantless searches of 11 individuals' electronic devices, and the seizure of four individuals' smartphones or laptops, violated the First and Fourth Amendments. On September 18, the U.S. Department of Homeland Security (DHS) published a new rule in the Federal Register requiring immigrants into the United States to provide social media information, including "handles, aliases, associated identifiable information, and search results." Finally, on Oct. 4, 2017, the House of Representatives Committee on Homeland Security passed a bill authorizing increased use of surveillance technologies by U.S. Customs and Border Protection (CBP) agents at U.S. borders. H.R. 3548 also provided $10 billion for the construction of a border wall along the U.S.-Mexico border, which was proposed in 2015 by then-presidential candidate Donald Trump.

SEARCHES AND SEIZURES

ACLU and EFF Sue Government Agency Regarding Searches at U.S. Borders

On Sept. 13, 2017, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the ACLU of Massachusetts filed a complaint in the U.S. District Court for the District of Massachusetts against the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE), after border agents searched 11 travelers' smartphones and laptops without warrants. *Alasaad v. Duke*, No. 1:17-cv-11730-DJC (D. Mass. 2017). The complaint also alleged that federal officers seized and retained several of the individuals' devices for weeks or months.

In August 2009, CBP released Directive No. 3340-049, titled "Border Search for Electronic Devices Containing Information," which remains an active policy. The purpose of the directive is to provide "guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered . . . at the border."

Significantly, the directive allows "an Officer or other individual authorized to perform or assist in such searches . . . [to] examine electronic devices and may review and analyze the information encountered at the border." The individual can do so "with or without individualized suspicion," meaning a search warrant or probable cause are not required, according to a March 13, 2017 ProPublica story. Amidst the legal questions and uncertainty, the practice of searching electronic devices and requesting passwords by CBP agents at U.S. borders increased between October 2015 and March 2017, according to data published by CBP in an April 11, 2017 release. The full press release is available online at: https://www.cbp.gov/newsroom/ national-media-release/cbp-releasesstatistics-electronic-device-searches-0.

CBP's policy and the increase in searches have raised numerous legal questions, particularly that an agent can search an electronic device without a warrant or probable cause and that the federal government "has long claimed that Fourth Amendment protections prohibiting warrantless searches don't apply at the border," according to an ACLU release on March 14, 2017. Journalists have been particularly concerned about searches of their electronic devices, even if they are used for work purposes, according to the Reporters Committee for Freedom of the Press (RCFP). In an Oct. 28, 2014 commentary, the Committee to Protect Journalists (CPJ) contended that searches of journalists' personal devices used for work purposes can expose sensitive data, such as confidential sources, classified documents, or notes taken during investigative reporting. (For more information on the 2009 directive and legal questions regarding the directive, see "U.S. Customs and Border Protection Searches of Electronic Devices, Data at U.S. Borders Raise Privacy and Legal Concerns" in the Summer 2017 issue of the Silha *Bulletin*.)

On Sept. 13, 2017, the ACLU, EFF, and the ACLU of Massachusetts filed a lawsuit "challeng[ing] the government's fast-growing practice of searching travelers' electronic devices without a warrant," according to an ACLU press release the same day. The plaintiffs were 10 U.S. citizens and one lawful permanent resident, and included "a military veteran, journalists, students, an artist, a NASA engineer, and a business owner. Several are Muslims or people of color. All were reentering the country from business or personal travel when border officers searched their devices." According to the ACLU, the journalists included Jeremy Dupin, "[a]n award-winning journalist and filmmaker who covers news coming out of South America and the Caribbean," and Isma'il Kushkush, a freelance journalist in Virginia. Additionally, plaintiffs included Zainab Merchant, a Florida-based graduate student in international security and journalism at Harvard University, and Akram Shibly, a New York-based independent filmmaker who runs his own production company.

Another of the plaintiffs was Sidd Bikkannavar, an engineer for The National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory in California, who was detained at the Houston, Texas airport where a CPB officer demanded that he reveal the password for his smartphone, even though it was owned by NASA. The officer allegedly used "algorithms" to search Bikkannavar's phone. (For more information on the search of Bikkannavar's phone, see "U.S. Customs and Border Protection Searches of Electronic Devices, Data at U.S. Borders Raise Privacy and Legal Concerns" in the Summer 2017 issue of the Silha *Bulletin*.) The complaint also detailed the searches and seizures of the other 10 plaintiffs, some of which included "physical force in order to conduct electronic device searches."

The complaint alleged that federal CBP agents "seized and searched Plaintiffs' electronic devices at U.S. ports of entry without probable cause to believe that the devices contained contraband or evidence of a violation of immigration or customs laws." The ACLU also alleged that officers had "confiscated and kept the devices of

several plaintiffs for weeks or months," including one individual's device which had been held since January 2017.

The complaint contended that these "searches and seizures of smartphones, laptops, and other electronic devices at the U.S. border," which were authorized by CBP's 2009 directive, as well as ICE's 2009 directive titled "Border Searches of Electronic Devices," "[were] in violation of the First and Fourth Amendments to the U.S. Constitution." Regarding the First Amendment, the plaintiffs argued that the searches of electronic devices meant that travelers "[would] be chilled from exercising their First Amendment rights of free speech and association, in knowing that their personal, confidential and anonymous communications and expressive material may be viewed and retained by government agents without any wrongdoing on their part."

The complaint further argued that DHS, CBP, and ICE violated the Fourth Amendment "by searching the content that electronic devices contain, absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched." The complaint cited *Riley v. California*, 134 S.Ct. 2477 (2014), in which U.S. Supreme Court Chief Justice John Roberts, writing for the unanimous Court, ruled that "what police must do before searching a cell phone seized incident to an arrest is accordingly simple— get a warrant."

The complaint asked the court to declare that CBP's and ICE's policies and practices violated the First and Fourth Amendments. Furthermore, the plaintiffs asked the court to enjoin the CBP and ICE from "searching [and seizing] electronic devices absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws, and without particularly describing the information to be searched." The full complaint is available online at: https://www.aclu.org/legal-document/alasaad-v-duke-complaint. As the *Bulletin* went to press, the district court had not announced any proceedings related to the lawsuit.

After filing the complaint, EFF Staff Attorney Sophia Cope explained the privacy interests of individuals' electronic devices. "People now store their whole lives, including extremely sensitive personal and business matters, on their phones, tablets, and laptops, and it's reasonable for them to carry these with them when they travel," she said in a statement. "It's high time that the courts require the government to stop treating the border as a place where they can end-run the Constitution."

ACLU attorney Esha Bhandari agreed. "The government cannot use the border as a dragnet to search through our private data," she said in a separate statement. "Our electronic devices contain massive amounts of information that can paint a detailed picture of our personal lives, including emails, texts, contact lists, photos, work documents, and medical or financial records. The Fourth Amendment requires that the government get a warrant before it can search the contents of smartphones and laptops at the border."

Bhandari explained in an interview with *Gizmodo* that the searches and seizures detailed in the lawsuit also raise First Amendment concerns. "People will think twice about who they communicate with and what they say if they know that the government can simply search through their phones and see all of that information—private communications, which can reveal not only the content of the communications, but also your associates, your contact lists, the people you're in touch with."

According to a September 13 *CNET* report, CBP spokeswoman Jennifer Gabris said the agency does not comment on pending litigation, but defended DHS's actions as being consistent with its responsibility to protect the country. She also explained that every person, piece of baggage, and any merchandize crossing U.S. borders are subject to search, according to *CNET*.

Department of Homeland Security Publishes Regulation Requiring Immigrants to Disclose Social Media Information

On Sept. 25, 2017, *BuzzFeed News* reported that the U.S. Department of Homeland Security (DHS) had published a new rule in the Federal Register that would require "social media handles, aliases, associated identifiable information, and search results" to be added to an individual's immigration file. DHS stated in a September 18 notice that it would accept public comments through October 18, at which time the rule would go into effect. Privacy advocates criticized the move, calling the plan "disturbing" and creating a "chilling effect" on social media use. Conversely, DHS defended the new rule, contending that it was not a new policy, but instead an effort to be transparent and comply with existing regulations.

Previously, DHS officials planned to "significantly increase demands for information from all visa applicants, including visitors and others seeking to immigrate," according to *The Wall Street Journal* on April 4. DHS proposed that U.S. Customs and Border Protection (CBP) agents would require certain individuals crossing the U.S. border to hand over their phones to be examined and to provide social media handles and passwords.

The DHS plans fell during a period in which President Donald Trump's administration and the U.S. State Department had proposed or implemented policy changes regarding the "extreme vetting" of visa applicants and foreign visitors to the United States. The Trump administration sent four cables between March 10 and March 17 to U.S. embassies, requesting that they conduct "extra scrutiny" of visa applicants, according to *The New York Times* on March 23. On May 4, the State Department proposed tougher questions for some visa applicants, including their "[s]ocial media platforms and identifiers, also known as handles, used during the last five years; and [p]hone numbers and email addresses used during the last five years." On May 31, Reuters reported that the Trump administration and the Office of Management and Budget had approved the State Department's new questionnaire for U.S. visa applicants, which required five years' worth of social media handles, among other information. (For more information on the Trump administration's and State Department's policies regarding collecting social media information at U.S. borders, see *Federal Agencies, Trump Administration Propose and Implement Measures for "Extreme Vetting"* in "U.S. Customs and Border Protection Searches of Electronic Devices, Data at U.S. Borders Raise Privacy and Legal Concerns" in the Summer 2017 issue of the Silha *Bulletin*.)

In a Sept. 18, 2017 notice, DHS formally published its proposal to update the current DHS system of records titled, "Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records." Document 82 FR 43556, Docket No. 2017-19365. According to the draft regulation, this system "contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process."

Among the proposed changes, DHS expanded the categories of records in the so-called "Alien Files," detailed profiles of individual immigrants, to include "social media handles, aliases, associated identifiable information, and search

Searches, *continued on page 42*

Searches, *continued from page 41*

results." According to *Fortune* magazine on September 26, the information would be gathered not only from recent United States immigrants, but also green card holders and naturalized citizens.

The DHS notice asked for comments to be submitted on or before Oct. 18, 2017 when the changes to the system of records would become effective. The full draft regulation is available online at: https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records.

According to *BuzzFeed News*, DHS said the regulation is not a new policy, but instead an effort to be transparent and to comply with existing regulations. "DHS published this notice in the Federal Register on Sept. 18 to comply with the administrative requirements of the Privacy Act to help address these requirements, not launch a new policy initiative," the agency said in a statement. "DHS, in its law-enforcement and immigration-process capacity, has and continues to monitor publicly-available social media to protect the homeland."

Conversely, Adam Schwartz, an attorney with the Electronic Frontier Foundation (EFF), called the plan "disturbing" in an interview with *BuzzFeed News* on September 25. "We see this as part of a larger process of high-tech surveillance of immigrants and more and more people being subjected to social media screening," Schwartz said. "There's a growing trend at the Department of Homeland Security to be snooping on the social media of immigrants and foreigners and we think it's an invasion of privacy and deters freedom of speech."

Faiza Patel, co-director of the Brennan Center for Justice's Liberty & National Security program, contended that the social media information obtained could be used for ideological vetting. "The question is do we really want the government monitoring political views?" Patel told *BuzzFeed News*. "Social media may not be able to predict violence but it can certainly tell you a lot about a person's political and religious views."

The American Civil Liberties Union (ACLU) argued that the collection of social media data could have a chilling effect. "This Privacy Act notice makes clear that the government intends to retain the social media information of people who have immigrated to this country, singling out a huge group of people to maintain files on what they say. This would undoubtedly have a chilling effect on the free speech that's expressed every day on social media," the organization said in a September 26 statement.

House Committee Considers Legislation Increasing Surveillance at U.S. Borders

On Oct. 4, 2017, the U.S. House of Representatives Committee on Homeland Security passed a bill increasing surveillance activities by U.S. Customs and Border Protection (CBP) agents at U.S. borders, including the use of drones, automatic license plate readers (ALPRs), unmanned cameras, and other surveillance technologies. Introduced by Rep. Michael McCaul (R-Texas), the committee chairman, H.R. 3548 also provided $10 billion for the construction of a border wall along the U.S.-Mexico border. Before a loophole was removed by Rep. Martha McSally (R-Ariz.), the bill had largely exempted CBP agents from the Freedom of Information Act (FOIA), 5 U.S.C. § 552, raising concerns from freedom of information experts that border enforcement activity would be kept a secret.

Titled "Border Security for America Act of 2017," H.R. 3548 was introduced to the House by McCaul on July 28, 2017 and was amended on September 27. The bill was referred to the House Committee on Homeland Security, which passed the bill on a party line 18-12 vote on October 4, as reported by *The Hill* the same day. As the *Bulletin* went to press, the legislation remained on the House floor for consideration. A full version of the bill is available online at: https://www.congress.gov/bill/115th-congress/house-bill/3548/text#toc-H1A1E67F9CCA945608F3DC1FDDF07C641.

The purpose of the legislation was "[t]o make certain improvements to the security of the international borders of the United States, and for other purposes." The bill authorized the Department of Homeland Security (DHS) to "take such actions as may be necessary (including the removal of obstacles to detection of illegal entrants) to construct, install, deploy, operate, and maintain tactical infrastructure and technology in the vicinity of the United States border to deter, impede, and detect illegal activity in high traffic areas." The bill also authorized the use of radar surveillance systems, unmanned cameras, ALPRs, and drones along U.S. borders, as well as the establishment of a biometric exit data system, which would use facial recognition software or collect other identifiers, such as fingerprints, to verify travelers' identities upon entering or leaving the United States.

Additionally, *The Hill* noted on October 4 that the bill included $10 billion in border wall funding, which was proposed on June 16, 2015 by Donald Trump, the same day he announced his campaign for president, according to a Feb. 28, 2017 *Huffington Post* report. The bill also contained $5 billion to improve ports of entry and the addition of 5,000 new border agents.

According to CNN on July 28, H.R.3548 was a "scaled back" version of S.1757, a bill introduced in the U.S. Senate on August 3 by Sen. John Cornyn (R-Texas). S.1757 contained similar provisions to H.R. 3548, but also authorized the collection of immigrants' DNA and biometrics, as well as social media screenings of visa applications. A full version of the Senate bill is available online at: https://www.congress.gov/bill/115th-congress/senate-bill/1757/text?q=%7B%22search%22%3A%5B%22s.+1757%22%5D%7D&r=1#toc-id3825f1ec4a414d5ba99b273ad9df89e6. As the *Bulletin* went to press, no further action on S.1757 had been announced.

In an Oct. 3, 2017 statement, the Electronic Frontier Foundation (EFF) raised several concerns regarding the surveillance implications of both bills, including CBP's use of biometric border screening; dissemination of immigrants' biometrics; screening of visa applicants' social media accounts; and utilizing and ALPRs near the U.S. border. EFF contended that CBP "should not track people's movements merely because they live and work near the border" and that both pieces of legislation would "invite 'extreme vetting' of visitors from Muslim nations."

In an Oct. 4, 2017 statement, the American Civil Liberties Union (ACLU), the Southern Border Communities Coalition (SBCC), and the Norther Borders Coalition (NBC) also raised concerns regarding the increased surveillance technologies at U.S. borders authorized by H.R. 3548. "Beyond physical barriers, H.R. 3548 proposes a further buildup of border surveillance, with no provisions to ensure that the rights of border residents and immigrants are protected," the ACLU wrote. "Border residents are already subject to invasive surveillance technologies with inadequate privacy protections. Instead of addressing this problem, the bill proposes increased deployment of surveillance and detection technology, including aerial drones and unmanned cameras."

On October 4, the *Tucson Sentinel* reported that Rep. McSally had pulled a provision of the bill that would have allowed CBP agents to be exempted from FOIA laws. The provision in question was titled "Prohibitions on Actions that Impede Border Security on Certain Federal Land" and authorized CBP agents "on covered Federal land to execute search and rescue operations or to prevent all

Searches, *continued on page 43*

Minnesota Supreme Court Begins Livestreaming Video of Oral Arguments

In an Aug. 23, 2017 news release, the Minnesota Judicial Branch announced that the Minnesota Supreme Court would begin livestreaming video of oral arguments in an effort to increase public access to the work of the state's highest court. The livestreaming would include oral arguments held in both the Minnesota State Capitol Courtroom and the Supreme Court's courtroom in the Minnesota Judicial Center.

CAMERAS IN COURTROOM

On Aug. 28, 2017, *MinnPost* reported that oral arguments in *The Ninetieth Minnesota State Senate v. Dayton* were the first to be streamed live. No. A17-1142 (Minn. 2017). The case revolved around a May 2017 veto by Gov. Mark Dayton of $130 million worth of legislative funding for 2018 and 2019.

According to Mark Anfinson, a lawyer and lobbyist for the Minnesota Newspaper Association, the Minnesota Supreme Court had previously allowed news organizations to set up cameras in the courtroom. He said in an interview with Minnesota Public Radio (MPR), "It's not an earth-shaking breakthrough.. . . The Supreme Court has allowed cameras and microphones in oral arguments for some time.. . . What's really valuable is the immediacy this brings to the oral arguments."

According to Director of Communications and Public Affairs for the Minnesota Judicial Branch Court Information Office Beau Berentson in an October 13 email to Silha *Bulletin* Editor Scott Memmel, the decision to begin livestreaming oral arguments "did not change the Court's long-standing rules related to the media's use of cameras and other recording devices in the courtroom." He continued, "Under the [Rule 134.10] of Civil Appellate Procedure, cameras and other recording devices are allowed to be used in Supreme Court proceedings as long as the media provides at least 24 hours' notice to the Court Information Office." Minn. R. 134.10 (2014). He also noted that the media "had a pool video camera and a pool still camera in the courtroom" during *The Ninetieth Minnesota State Senate v. Dayton* oral arguments.

In addition to streaming live video of oral arguments, the Court will continue the long-standing practice of posting recorded video of the oral arguments after the proceedings have concluded. According to the St. Paul *Pioneer Press* on Aug. 23, 2017, the Court has made recorded video of oral arguments available since 2005. Both the live and recorded video of oral arguments are available online at: www.mncourts.gov/SupremeCourt.

Chief Justice Lorie Gildea said in a statement that the allowing livestreaming would help the public trust the judicial system. "By livestreaming our oral arguments, we hope to give more Minnesotans the opportunity to see their highest Court in action, and to learn more about how our Court considers and decides the important legal matters that come before us," Gildea said.

In an interview with KFGO on September 19, Gildea added, "So far, the feedback has been very positive.. . . People are watching and they're enjoying the opportunity to have easier access to the work of the Supreme Court."

Anfinson also told the Minneapolis *Star Tribune* on August 23 that he expected a larger audience for the Minnesota Supreme Court's oral arguments. "Because it's going to be live and immediate, I think a lot more people are going to watch it than have ever watched a Supreme Court oral argument before," Anfinson said. He added, "It's a good thing, it's a really good thing, because it's going to make the court system generally, and especially the most powerful court, more visible to the public.. . . And it should be."

In an interview with the *Pioneer Press*, Mike Cavender, executive director of the Radio Television Digital News Association, a national group that advocates for cameras in courtrooms, said that Minnesota was a "laggard" in allowing recording devices in the courtroom. "But in recent years, that has improved, and with this decision now at the Supreme Court level for livestreaming, that's a big boost for public access in the courts," Cavender said.

Ashley Turacek
Silha Research Assistant

Searches, *continued from page 42*

unlawful entries into the United States, including entries by terrorists, other unlawful aliens, instruments of terrorism, narcotics, and other contraband through the southern border or the northern border." The loophole permitted agents to carry out those operations "without regard to the provisions of law" listed in the ensuing subsection, which included 36 federal laws. Among the laws listed was the Administrative Procedure Act, which includes FOIA. The *Tucson Sentinel* in an October 3 editorial and American Society of News Editors (ASNE) in an October 3 press release pointed out that the bill, therefore, could "[exempt] CBP activities taken on covered federal land within 100 miles of the southern or northern border from the act could also exempt records of those activities from FOIA."

ASNE explained the potential consequences of the provision. "The risk of leaving this stone unturned is clear: The public and press would be in the dark with regard to CBP activities near the border. We wouldn't have access to records of arrests, injuries, deaths and other major incidents at the border or the costs of securing the borders, including the cost and other details of building a border wall. The CBP would be able to run wild and without oversight for the most part."

In an October 3 interview with the *Tucson Sentinel*, University of Arizona School of Journalism director David Cuillier added, "Basically, the Border Patrol could do whatever it wants throughout Tucson and this legislation would prohibit anyone from the public to find out.. . . Is that the America we want to live in — where the government can act secretly doing whatever it wants with our tax dollars and our liberties at stake, and we don't ever find out?"

McSally told the *Tucson Sentinel* on October 4 that removing the FOIA loophole "was an "important issue to clear up.. . . Transparency is an important part of governance." McSally's staff told the *Tucson Sentinel* the day before that they did not know why the FOIA loophole had been included in the earlier drafts of the bill.

Scott Memmel
Silha *Bulletin* Editor

Media Groups Allowed to Join Lawsuit over Access to Documents in Wetterling Investigation; Dispute Expands to over Half the Case File

In the fall of 2017, two hearings were held regarding the possible release of documents related to the Jacob Wetterling investigation, stemming from the notorious 1989 abduction and murder of an 11-year-old boy. On September 22, Stearns County (Minnesota) District Court Judge Ann Carrott allowed media groups, including the Silha Center for the Study of Media Ethics and Law, to intervene in a lawsuit which will determine whether investigative documents containing alleged personal and sensitive material pertaining to the Wetterling family would be released. During the hearing, Carrott suggested that the files created by the Federal Bureau of Investigation (FBI) over the course of the investigation may not be subject to state open records laws. On October 9, the Wetterlings' lawyers asked whether documents in the 56,000-page case file that originated with the FBI would have to be returned to the agency, potentially making more than half the case file subject to the federal Freedom of Information Act (FOIA), rather than state law. Additionally, on November 10, Mark Anfinson, a Minneapolis media lawyer representing the media groups, filed a motion for summary judgement, requesting that Carrott deny the Wetterlings' request to block public access to certain documents and return others to the FBI. On November 29, the Wetterlings' attorneys filed a memorandum opposing Anfinson's motion.

ACCESS

The documents in question stem from the 1989 abduction and murder of 11-year-old Jacob Wetterling in St. Joseph, Minn. On Sept. 1, 2016, Danny Heinrich, who was already jailed on federal child pornography charges, confessed to kidnapping and killing Jacob in October 1989, according to the Minneapolis *Star Tribune*. The 27-year investigation included local, state and national investigators, including the FBI, compiling more than 56,000 pages of information and 10,000 documents containing interviews, tips, lead sheets, and investigative reports which were set to be released in June 2017.

On June 2, the Wetterlings filed a lawsuit in the Minnesota District Court for the Seventh Judicial District, requesting a temporary restraining order (TRO) to halt the release of some documents in the investigative file. *Patty Wetterling and Jerry Wetterling v. Stearns County*, No. 73-CV-17-4904 (2017). In the lawsuit, the Wetterlings alleged the investigative documents include "personal information regarding [their] marriage and family relationship" and "highly personal details about the Plaintiffs, their minor children, and the inner working of the Wetterling family." The complaint contended that such information "is protected from disclosure by the state and federal constitutions," rather than the Minnesota Government Data Practices Act (MGDPA), Minn. Stat. § 13.01 *et seq.*, which classifies documents and information from closed or inactive investigations as "public data," except in circumstances in which "the release of the data would jeopardize another pending civil legal action, and except for those portions of a civil investigative file that are classified as not public data by this chapter or other law." Minn. Stat. § 13.39. Furthermore, the Wetterlings argued that "[b]oth the United States Supreme Court and the Minnesota Supreme Court afford individuals a fundamental and personal right to informational privacy that prevents governmental intrusion into and public discourse about intimate details regarding personal and family matters." The full complaint is available online at: https://www.courthousenews.com/wp-content/uploads/2017/06/WetterlingComplaint.pdf.

On June 2, Judge Carrott issued a TRO enjoining the Stearns County Sheriff's Office from "disseminating or disclosing the personal information contained in the Jacob Wetterling criminal investigative file to any person."

On, June 27, the Silha Center for the Study of Media Ethics & Law, along with nine other media organizations and transparency advocates, filed a "complaint in intervention," arguing for the release of the documents under the MGDPA, contending that there was no exception in the Act preventing the release of the sensitive documents. The organizations sought to intervene "for the purpose of challenging plaintiffs' claim that there is a right of privacy arising under the state or federal constitutions that takes precedence over the public access requirements of the MGDPA." The complaint added, "Applicants are not aware of any legal authority suggesting that records subject to the MGDPA and classified as public can be withheld based on a purported constitutional privacy right.. . . Should this Court accept plaintiffs' argument . . . it would severely impair the ability of Applicants and their members to protect their interest in public access to government records, because it would create enormous uncertainty about when and under what specific circumstances public records could be withheld based on the constitutional privacy right." The complaint further explained that the MGDPA "establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public." Minn. Stat. §13.01(3).

Minnesota law requires that in order for an applicant "to be permitted to intervene in an action," the party must "claim an interest relating to the property or transaction which is the subject of the action." The applicant must also show that their interest is not adequately protected by the existing parties in the legal action. Minn. R. Civ. P. § 24.01 *et seq.* The news and transparency organizations alleged that "have a strong and substantial interest in the subject matter of this action, which focuses on the issue of public access to records created, collected, and maintained by government agencies." They also contended that "no existing party is likely to challenge plaintiffs' claim that disclosure of the records in question is prohibited by a constitutional privacy right." The full complaint in intervention is available online at: https://www.scribd.com/document/352444051/Minnesota-Media-Organization-Intervention-in-Wetterling-Documents-Release.

In a statement after filing the complaint, the Minnesota Newspapers Association (MNA), which was one of the interveners, wrote, "While sincerely sympathetic to the Wetterlings, [MNA] believes the lawsuit poses a direct threat to the integrity of the Data Practices Act, the state law that governs the classification of government records and that requires most to be made public." (For more information on the background of the Jacob Wetterling investigations, the Wetterlings' complaint and the media organizations' motion to intervene, see "Media Groups and Transparency Advocates Challenge Family's Lawsuit, Judge's Ruling Halting the Release of 'Personal' Information" in the Summer 2017 issue of the Silha *Bulletin*.)

In a September 22 hearing, Carrott allowed the ten media and transparency organizations to become part of the legal proceedings, according to Minnesota Public Radio (MPR) on the same day. Anfinson commended the ruling. "Now that we're parties here, we're in the ring," Anfinson said. "We're not in the peanut gallery anymore. It makes a big difference."

However, Carrott also raised the possibility that the files created by the FBI over the course of the investigation were not subject to state law and thus could not be released by Stearns County because they belonged to the federal agency. Doug Kelley, the attorney for the Wetterling family, told the *St. Cloud Times* that his clients were pleased with that aspect of the ruling. "They believe that many of these items should never have been in a law enforcement file in the first place," Kelley said.

According to the *Star Tribune*, an October 9 hearing further raised the question of whether the files created by the FBI would have to be returned to the agency. If so, they would become subject to FOIA, rather than state open records laws. Kelley noted that FOIA includes two federal exemptions to protect personal privacy interests. Exemption 6 protects information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Exemption 7(C) provides protection for law enforcement information the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). The *Star Tribune* noted that the potential FBI data release could expand from the original 168 pages to potentially thousands of documents, making up over half of the case file.

The *Star Tribune* also reported on October 9 the FBI had sent letters to Stearns County Attorney Janelle Kendall and Sheriff Don Gudmundson demanding the return of all FBI documents in the file, which Kendall refused.

On November 10, Anfinson filed a motion for summary judgment on behalf of the intervening parties, asking that Carrott deny the Wetterlings' requested relief and arguing against the Wetterlings' constitutional arguments. The motion first asserted that neither the U.S. Supreme Court nor the Minnesota Supreme Court has ever recognized a constitutional privacy right to overrule the public disclosure of government records. The motion stated, "Plaintiffs fail to cite any decision from either the United States Supreme Court or the Minnesota Supreme Court that supports the significant expansion of constitutional privacy which they urge in this action. In other words, plaintiffs seek to persuade the Court that it should go beyond what established precedent in Minnesota allows."

The motion next addressed the constitutional right of privacy, both at the state and federal level, contending that court precedent does not support the Wetterlings' argument. Anfinson cited the 1995 Minnesota Supreme Court case *Women of State of Minn. By Doe v. Gomez*, in which the court held that it "has long recognized that we may interpret the Minnesota Constitution to offer greater protection of individual rights than the U.S. Supreme Court has afforded under the federal constitution.. . . However, we do not do so lightly." 542 N.W.2d 17, 26 (Minn. 1995). In *Gomez*, the Court also quoted *State v. Gray*, which held that the right of privacy protects only fundamental rights, defined as "those which have their origin in the express terms of the Constitution or which are necessarily to be implied from those terms" 413 N.W.2d 111 (Minn. 1987). Therefore, Anfinson contended that "the body of precedent comprising the law applicable in Minnesota demonstrates that the scope of such fundamental rights is narrow" and that no decision by the Minnesota Supreme Court "has held that the right can be used to prevent public disclosure of records held by a government agency in accordance with applicable law." In fact, the Minnesota Supreme Court, according to the motion, "has extended constitutional privacy rights only to matters relating to 'the possession and control of [one's] own person,' such as medical treatment, sexual behavior, and reproductive decisions." Additionally, Anfinson noted that in a case involving public disclosure, the Minnesota Court of Appeals held that even if a constitutional claim is asserted, "the right to informational privacy is substantially constricted when the information at issue is public information." *Mpls. Fed. Of Teachers v. Mpls. Public School*, 512 N.W.2d 107, 110 (Minn. App. 1994).

The motion also contended that the U.S. Supreme Court had considered three cases involving a constitutional claim of informational privacy, but that "all three focused on efforts to block the government from collecting and maintaining certain information, not requests to prevent the disclosure of presumptively public government records.. . . [I]n each of the cases, the Court rejected the plaintiffs' constitutional objections and declined to hold that the constitutional privacy right applied." Anfinson added, "The Supreme Court has never held that the freedom from disclosure component of the right to privacy is protected by the Constitution."

Next, the motion addressed the plaintiffs' argument for a constitutional right of informational privacy used to prevent disclosure of records otherwise classified as public by state law. The motion argued that if adopting such a right could effectively be used to disrupt the framework for balancing public access and privacy set by the Minnesota legislature. Anfinson explained that the extensive legislative history and statutory construction of the MGDPA should not be undermined by the plaintiffs' assertion in the case, especially because the "core of the Data Practices Act is the provision that all 'government data' shall be public unless otherwise classified by statute or other law." He added, "There is no precedent applicable in Minnesota holding that informational privacy rights under either the state or federal constitutions can be used to prohibit disclosure of public government records, there is no clear majority position on the issue among courts in other jurisdictions, and there are compelling policy reasons for declining to recognize such a constitutional right of privacy in Minnesota."

Next, Anfinson turned to the question of whether the Wetterlings have standing to ask that records held in Stearns County be returned to the FBI. The complaint explained that a party has standing "when (1) the party has suffered an injury-in-fact, or (2) the party is the beneficiary of a legislative enactment granting standing." Anfinson contended that because the Wetterlings "do not have a legislative grant of standing authorizing them to pursue the claim involving the FBI records, they must establish an injury-in-fact," which is a "concrete and particularized invasion of a legally protected interest." However, Anfinson argued that the plaintiffs cannot establish such an injury because "they have no legal interest in the [FBI] records themselves." He added that the Wetterlings "do not assert that they have any ownership or possessory interest in the records" and that the refusal of Stearns County to return the records to the FBI does not legally injure the plaintiffs.

Anfinson also disputed the plaintiffs' contention that the "[d]isclosure of the FBI Records is governed by federal law, not the MGDPA, and such records must be obtained, if at all, pursuant to the FOIA" and that the information in question would be exempt from disclosure under FOIA. Anfinson contended that FOIA

Wetterling, *continued on page 46*

Wetterling, *continued from page 45*

"does not govern the status of records in the possession of Minnesota government agencies such as Stearns County. [FOIA] applies only to federal government agencies." As a result, FOIA is not sufficient for the Wetterlings to establish standing, according to Anfinson.

Finally, the motion argued that, under the MGDPA, it would be improper for Stearns County to return the documents to the FBI. Anfinson argued that the plain language of the statute indicates the MGDPA governs all data collected, received, or maintained by Stearns County and that because the county attorney's office has concluded the records are public data under the Act, members of the public have an established legal right of access to the documents at issue. The motion further notes that the Wetterlings rely on 28 U.S.C. § 534, a federal law "authorizing the U. S. attorney general to 'exchange' records and information with other government entities, and providing that the exchange 'is subject to cancellation if dissemination is made outside the receiving departments or related agencies.'" Anfinson contended that the federal law does not apply to Stearns County because it "does not direct or require that Stearns County do anything" and that the law "says nothing about a return of records that have already been exchanged upon cancellation."

Anfinson concluded by discussing several "adverse effects" of requiring a local government body to "not just return of all original documents, but . . . any copies as well" to a federal agency. Anfinson contended that such a requirement "could seriously disrupt the ability of local government officials and members of the public and news media to evaluate, after a criminal case investigation was over, how law enforcement agencies involved in the investigation performed their duties." He continued, "With respect to the FBI specifically, it would allow the agency to completely conceal the record of its participation in the investigation and frustrate any semblance of public accountability, since under the FOIA, the agency has broad discretion to deny requests for public access to its records." The motion also alleged that the removal of the FBI records from Stearns County, including any copies, "could seriously impair the ability of Stearns County to defend itself in litigation currently pending against the County and some of its officials related to the Wetterling investigation."

The hearing on the motion of summary judgement was tentatively scheduled for the Douglas County Courthouse in Alexandria, Minn. on December 8. As the *Bulletin* went to press, the hearing on the motion was postponed until at least Jan. 11, 2018.

On November 29, attorneys for the Wetterlings filed a memorandum opposing Anfinson's motion for summary judgement. The memorandum first argued that the Wetterlings had "legally cognizable claims based on their right to informational privacy under the state and federal constitutions." In Minnesota, according to the memorandum, courts have "recognize[d] a constitutional right to informational privacy having two facets: (1) the right not to disclose personal information to the government, and (2) the right to prevent the government from disclosing private information it collects about individuals." The memorandum also cited several U.S. Supreme Court and other federal decisions that "acknowledged privacy rights of a constitutional magnitude in multiple contexts, including the sanctity of the home." Therefore, the Wetterlings contended that federal courts and state courts have "overwhelmingly found that a constitutionally based right of privacy protects personal information of the type and character at issue in this case," particularly related to "fundamental liberties, including marriage, family relationships and child rearing."

Second, the memorandum contended that "[u]pholding the Wetterlings' constitutional privacy rights [would] not undermine the MGDPA." Specifically, it argued that "[n]othing in the MGDPA suggests that the Minnesota Legislature consciously decided to direct public dissemination of crime victim information disclosing personal and private matters held confidential by the due process clauses of the state and federal constitutions." Further, the memorandum claimed that an adjudication upholding the Wetterlings' constitutionally based rights to informational privacy would actually "give effect to the MGDPA," because the Act "by its very terms prohibits disclosure of data made private by other state or federal law." Minn. Stat. §§ 13.01, subd. 3 and 13.03, subd. 1.

Third, the memorandum argued that the Wetterlings had standing to assert claims based on federal law related to issues related to the FBI records. In order to have standing, the plaintiffs must have "a sufficient stake in a justiciable controversy to seek judicial relief." The memorandum further explained that in Minnesota, "a party whose legitimate interest is 'injured in fact' has standing unless the legislature has indicated that the interest is not to be protected." The Wetterlings contended that the release of their personal information would cause an "injury in fact" to the Wetterlings' reputation and privacy, providing sufficient grounds to establish standing.

Finally, the memorandum reemphasized the Wetterlings' arguments that the federal records should be returned to the FBI. The memorandum stated that in "rare instances" where ownership of federal documents is contested, "courts have uniformly sided with the United States and ordered the return of federal records to the federal government." When the documents are returned to the federal agency, federal law, rather than state law, then guides their disclosure, according to the memorandum.

As a result, the Wetterlings argued that FOIA Exemption 7(C) and Exemption 6 would restrict the release of private victim information in this case. Exemption 7(C) prevents the disclosure of documents compiled for law enforcement purposes that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." Exemption 6 prevents the disclosure of "personnel and medical files and similar files where the disclosure would constitute a clearly unwarranted invasion of personal privacy." According to the memorandum, courts have found "similar files" to include FBI records discussing crime information, citing the U.S. Court of Appeals for the Second Circuit's 1981 case, *Brown v. Federal Bureau of Investigation*. 658 F.2d 71, 75 (2nd Cir. 1981).

Additionally, the Wetterlings contended that the Privacy Act of 1974 also "exempts from disclosure information maintained by a federal agency whose principal function is enforcing federal laws that was "compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual." 5 U.S.C. § 552a(j)(2)(B). The memorandum concluded by stating that the Wetterlings "state legally actionable claims for judicial relief. Intervenors are thus not entitled to summary judgment as a matter of law and their motion for summary judgment should be denied."

On December 5, the *Star Tribune* reported that the U.S. Department of Justice had filed a motion to intervene in the case. The motion also sought to require Stearns County to return all of the FBI's documents. As the *Bulletin* went to press, Carrott had not ruled on the motion.

Brittany Robb
Silha Research Assistant

Update: University of Minnesota Regents Investigation Fails to Uncover Leaker of Information to KSTP-TV

On Sept. 14, 2017, the University of Minnesota (University) released a statement announcing that an investigation by the University Board of Regents (regents) had failed to uncover who leaked confidential information to KSTP-TV, the ABC affiliate in St. Paul, about Randy Handel, the University associate athletic director of development. Although the University and two regents defended the investigation, other observers criticized the probe.

REPORTER'S PRIVILEGE

The investigation began on May 11, 2017 after KSTP reported the previous day that Handel was being investigated by the University's Office of Equal Opportunity and Affirmative Action (EOAA). KSTP's report was based on a May 10 email sent from the EOAA office to the Board of Regents alleging that Handel had sexually harassed an employee in the athletic department. KSTP reported that the contents of that email were provided to the news station by a regent under the condition of anonymity. The regents summarily launched an investigation "to determine who provided the email to the TV station," according to the Minneapolis *Star Tribune* on May 12. The Board required all 12 of its members, as well as university employees who had access to the information, to sign affidavits swearing they were not the anonymous source.

On June 22, the Associated Press (AP) reported that the University had hired the Minneapolis branch of the risk management firm Stroz Friedberg LLC to investigate the leak. Minnesota Public Radio (MPR) also reported on June 22 that the university had retained Don Lewis, an outside attorney, to represent the university. According to the *Star Tribune* on September 15, Lewis was hired "to review the release of confidential information," out of concern that state privacy laws had been violated. Several media groups criticized the investigation, citing the Minnesota Free Flow of Information Act, the state shield law which provides qualified protection to journalists. Minn. Stat. 595.021 et seq. (For more information on KSTP's report, the regents' investigation, and criticism by media experts and advocates, see *KSTP Reports Internal Regents Email; Regents Launch Investigation to Find Source of the "Leak"* in "Vermont Governor Signs New Shield Law; A Minnesota Television Station and a New York Appeals Court Address Reporter's Privilege Issues" in the Summer 2017 issue of the Silha *Bulletin*.)

In a September 14 statement, the University wrote, "The results of the review were inconclusive — information reviewed did not identify the source of the private personnel information." According to the University, the investigation included "an examination of both electronic mail and cell telephone records of Regents and other University personnel and interviews with those who had access to the confidential information," and took about 150 hours to complete. According to KSTP on September 14, the independent probe cost the University more than $74,000.

> "It's [the University's] responsibility to keep their information confidential.. . . It's not a matter of condoning the leak. It's the hunt . . . that has the effect of discouraging people from talking to the press about anything.. . . It puts people on notice that if they have the temerity to speak to the press . . . there likely will be repercussions."
>
> **— Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley**

Despite failing to identify the leaker, the University defended the importance of the investigation. "Even if inconclusive, this review demonstrates the [University's] commitment to respecting the confidentiality of information concerning individuals within the University community, the importance of ensuring that University officials are complying with Minnesota State Law, and the importance the Board places on its fiduciary responsibility to this institution," the statement read.

Regent Steve Sviggum told the *Star Tribune* that the investigation was successful in that it confirmed that no regents leaked the information. "They found nothing," he said. "No e-mails, no texts, no phone calls. That's good and comforting . . . that we can trust one another's word."

Regent Chairman David McMillan also defended the investigation, contending that it was necessary because the leak violated state data privacy laws. "When something like this [leak] happens, we have to do our very best to figure out what happened and why," he told the *Star Tribune*.

However, other observers were critical of the leak. Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley called the investigation into the leak "inappropriate" in an interview with the *Star Tribune*. "It's [the University's] responsibility to keep their information confidential," she said. "It's not a matter of condoning the leak. It's the hunt . . . that has the effect of discouraging people from talking to the press about anything." Kirtley added, "It puts people on notice that if they have the temerity to speak to the press . . . there likely will be repercussions. It doesn't seem to me that a land-grant university should be engaging in those kinds of operations."

Rep. Sarah Anderson (R-Plymouth) agreed that the university should not have invested the time and resources into looking for the leaker. "My concern is what's happening at the University," she told the *Star Tribune*. "Their priority should have been: How do we address this concern of sexual misconduct on campus?"

The University's September 14 statement said the regents considered the investigation to be closed.

Scott Memmel
Silha *Bulletin* Editor

No More Monkey Business: Settlement Ends "Monkey Selfie" Copyright Lawsuit

On Sept. 11, 2017, the People for the Ethical Treatment of Animals (PETA) announced on its website that the organization had reached a settlement with photographer David John Slater after a two-year legal dispute over the rights to a selfie taken by a monkey in Indonesia in 2011. PETA had claimed in the U.S. District Court for the Northern District of California that the primate had rights to the photograph taken using Slater's unattended camera, while Slater contended that the Copyright Act, 17 U.S.C. §§ 101 *et seq.*, does not apply to animals. As part of the settlement, Slater agreed to donate part of the proceeds from the famous selfie to organizations dedicated to protecting macaque monkeys.

COPYRIGHT

The case arose in 2011 when a 6-year-old crested macaque named Naruto used Slater's camera to take several pictures, including one of himself, according to court documents. Slater had placed the camera on a tripod amidst a group of monkeys, setting it to automatically focus and wind, as reported by *The New York Times* in January 2016. The photographer published the photographs taken by Naruto in his book, "Wildlife Personalities," according to an August 2014 CNN story.

In 2015, PETA filed a lawsuit on behalf of Naruto, arguing that publishing the photographs infringed on the primate's rights under the Copyright Act. Slater argued that a monkey could not own a copyright and that his company, Wildlife Personalities Ltd., owns worldwide commercial rights to the photos taken by Naruto.

> "PETA and David Slater agree that this case raises important . . . issues about expanding legal rights for nonhuman animals, a goal that they both support, and they will continue their respective work to achieve this goal."
>
> **— PETA and David Slater joint statement**

In a tentative opinion filed on Jan. 8, 2016, Judge William Orrick disagreed with PETA's claim that Naruto's rights had been violated. "While Congress and the president can extend the protection of law to animals as well as humans," he wrote, "there is no indication that they did so in the copyright act." *Naruto v. Slater*, 2016 WL 362231 (N.D. Cal. 2016). Following the ruling, both sides asked the U.S. Court of Appeals for the Ninth Circuit to vacate Orrick's decision and dismiss the case, according to the Associated Press (AP) on September 12.

On Sept. 11, 2017, the parties reached a settlement in which Slater agreed to donate 25 percent of future revenue from the photograph to charitable organizations that protect crested macaques, like Naruto. In a joint statement, the parties wrote, "PETA and David Slater agree that this case raises important, cutting-edge issues about expanding legal rights for nonhuman animals, a goal that they both support, and they will continue their respective work to achieve this goal." The statement continued, "As we learn more about Naruto, his community of macaques, and all other animals, we must recognize appropriate fundamental legal rights for them as our fellow global occupants and members of their own nations who want only to live their lives and be with their families."

Scott Memmel
Silha *Bulletin* Editor

The Silha *Bulletin* is available online at the University of Minnesota Digital Conservancy.

Go to:
http://conservancy.umn.edu/discover?query=Silha+Bulletin
to search past issues.

32nd Annual Silha Lecture Addresses Freedom of the Press During the Trump Presidency

Deputy general counsel of *The New York Times* David McCraw argued during the 32nd annual Silha Lecture that beyond President Donald Trump's tweets and disparaging of "fake" and "failing" news outlets, the current media landscape raises questions as to whether legal precedents for First Amendment protections are still viable today.

SILHA CENTER EVENTS

Throughout his lecture, "Making Media Law Great Again: The First Amendment in the Time of Trump," McCraw, a 15-year veteran of the *Times* and litigator of over 35 Freedom of Information Act (FOIA) suits, discussed the origins and potential ramifications of President Trump's attacks on the First Amendment right of freedom of the press. "Like no president before, Trump has both questioned our tradition of protecting freedom of the press and directly engendered a debate about our laws governing freedom of the press. It would be easy to dismiss all of that: it's not real, it's partisan, it's a way to avoid accountability and it isn't done in a really smart way. #Politics #Silly #Sad," McCraw said.

The lecture took place on Oct. 2, 2017 at the University of Minnesota's Cowles Auditorium with nearly 300 people in attendance.

In October 2016, McCraw wrote a letter to then-presidential candidate Trump's attorneys defending the right of *The New York Times* to publish a news story titled "Two Women Say Donald Trump Touched Them Inappropriately," over which Trump's attorneys had threatened a defamation lawsuit. The letter garnered over two million views on the *Times* website alone and brought McCraw into the national spotlight. (For more information on McCraw's letter and more information about the lecturer, see "*New York Times* Deputy General Counsel to Deliver 2017 Silha Lecture, 'Making Media Law Great Again: The First Amendment in the Time of Trump'" in the Summer 2017 issue of the Silha *Bulletin*.)

McCraw opened his lecture by recounting the experience surrounding the release of his letter. McCraw said he received varied responses, but took note of those with more personal emphases. "As the letter went out and the calls started coming in, my inbox exploded instantly. It was really a sort of inspiring time because there were people who criticized the letter, but the number of people who wrote and talked about how much it meant to them that I'd stood up for the *Times* and stood up for the women was really quite extraordinary," he said. McCraw added that one of the lessons he learned from the experience was that perhaps it was not "a super great idea to send a 'bring it on' letter to the next president of the United States without first checking with senior management."

A major theme of McCraw's lecture was the differences between the modern media landscape as compared to its past iterations. "In media landscape 1.0, we had large and influential organizations that dominated the flow of information. They served as gatekeepers.. . . These were professional organizations, so when the courts said 'let the press self-regulate, let's get the government out of the business of regulating the press' it was easy to understand that you weren't surrendering this to irresponsible players; you were giving freedom to those people who took seriously their role as a conscientious gatekeeper to the information that flowed into society. There was an understanding that there was a need for powerful media to check powerful government," McCraw explained.

> "Media landscape 1.0 is gone and media landscape 2.0 looks nothing like it.. . . It has been replaced by a landscape dominated by digital communication with a cacophony of voices."
>
> **— David McCraw, *New York Times* deputy general counsel**

However, McCraw contended that the former landscape no longer exists. "Media landscape 1.0 is gone and media landscape 2.0 looks nothing like it," he said. "It has been replaced by a landscape dominated by digital communication with a cacophony of voices." McCraw added that there are no gatekeepers left, and that the current landscape has eliminated any semblance of a news cycle and changed the role of both creators and consumers of information.

However, the legal foundation for freedom of the press still relies on cases decided long before the digitally-dominated news cycle of this new landscape, during landscape 1.0. McCraw explained that the foundation for freedom of the press jurisprudence largely took place during the period between 1964-1989, beginning with *New York Times v. Sullivan*, which established the actual malice standard in which a public figure must prove that a journalist acted with knowledge of falsity or reckless disregard for the truth. 376 U.S. 254 (1964). What followed was a 25-year period of First Amendment and right of access cases which continue to stand as the foundational media law decisions governing the modern landscape, according to McCraw. Additionally, McCraw cited *New York Times v. United States*, 403 U.S. 713 (1971), also known as the "Pentagon Papers" case, and *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979) as cases from this "incredible" 25-year period.

McCraw asked the audience to consider whether the preexisting body of media law was still relevant in the 2.0 landscape. "Have the decisions that made a whole lot of sense 30 years ago grown old? Does the First Amendment really still work in the way it's been interpreted in those great decisions from 50, 40 and 30 years ago?"

In comparing landscape 1.0 to landscape 2.0, McCraw noted the example of the tort of intentional infliction of emotional distress. According to McCraw, landscape 1.0 was demonstrated by the U.S. Supreme Court's ruling in *Hustler Magazine, Inc. v. Falwell*, 485 US 46 (1988). The case involved a satirical *Hustler Magazine* ad parody insinuating that Jerry Falwell, an American Southern Baptist pastor and televangelist, had engaged in intercourse with his mother. McCraw contended that the Supreme Court had found it obvious that it should rule in favor of *Hustler*, but questioned whether the Court would have made the same ruling in landscape 2.0. "Now you look at things like revenge porn and hate speech and bullying online. Would the Supreme Court feel the same when it's

Lecture, *continued on page 50*

Lecture, *continued from page 49*

not a magazine ad but that sort of abuse you see online?"

One issue McCraw said did not appear in landscape 1.0 was "fake news." McCraw discussed one example in the 2016 presidential election, in which the website "Red Nation Rising" claimed Pope Francis had endorsed Donald Trump for the presidency. "Pope Francis Shocks World, Endorses Trump for President, Releases Statement" was read over 900,000 times, but was ultimately just an example of fake news. "What do you do about this? This wasn't even a problem in media landscape 1.0," McCraw noted.

McCraw concluded the lecture by arguing that resolving the conflict between media landscapes 1.0 and 2.0 will not be a simple or quick task. The strategies to do so will take a change in attitude, and collaboration across the aisle and the digital divide, according to McCraw. He pointed to the unanimous vote for passage of the 2010 SPEECH Act, which made foreign libel judgments unenforceable in U.S., and overwhelming support for FOIA renewals as signs that cooperation is attainable. "We need to resurrect this unanimity. We need to support speech no matter who is speaking. How do we have both government transparency and national security? How do we stop fake news but not give up free press?" (For more information on the passage of the SPEECH Act, see "Federal 'Libel Tourism' Law to Nullify Anti-Free Speech Rulings" in the Summer 2010 issue of the Silha *Bulletin*.)

> "We need to support speech no matter who is speaking. How do we have both government transparency and national security? How do we stop fake news but not give up free press? . . . We can't answer these questions in 140 characters or less."
>
> **— David McCraw, *New York Times* deputy general counsel**

"We can't answer these questions in 140 characters or less," McCraw concluded.

During a Q&A period, McCraw fielded questions regarding the prosecution of leakers of classified information and the impact on journalists. Additionally, one audience member asked McCraw, "Where does protected speech end and incitement of violence start?" McCraw responded, "I'm a free expression guy. And I believe the line is drawn appropriately, which is . . . to actually get over the line it has to be that there is an imminent threat that the speech is likely to lead to violence.. . . I am very very reluctant to endorse the idea that we should follow the European lead and regulate hate speech. There is no question that hate speech does harm. There is no question about that. The question is whether the remedy would be worse. And that is having a government that decides what is allowable." He added, "I find that [government regulation of speech is] a greater threat.. . . I'm not optimistic that government can regulate hate speech."

A video of the lecture is available on the Silha Center website at silha.umn.edu. Silha Center activities, including the annual lecture, are made possible by a generous endowment from the late Otto and Helen Silha.

Brittany Robb
Silha Research Assistant

Silha Research Assistantships

The Silha Center offers Research Assistantships to outstanding law and graduate students with an interest in media law and media ethics. Silha Research Assistants are responsible for writing, editing and producing the Silha *Bulletin* during the academic year and the summer semester. They also assist Silha Professor Jane Kirtley with a variety of research projects, such as preparing a comprehensive outline on global privacy for the Practising Law Institute's annual Communications Law in the Digital Age conference handbook; *amicus* briefs (including before the Supreme Court of the United States); and comments on proposed rules and regulations submitted to federal, state and international bodies.

The number of available Research Assistantships varies from year to year. Appointments are competitive. A strong academic record and excellent legal research and writing skills are required. Journalism experience is strongly preferred. Applicants must be currently enrolled at the University of Minnesota.

Applications for Summer 2018 and for the 2018-19 academic year will be due on March 19, 2018.

For more information, please visit the Silha Center website at http://www.silha.umn.edu

Helen Silha, Beloved and Constant Supporter of the Silha Center, Passes Away in October 2017

The Silha Center staff mourns the recent passing of donor Helen Silha. Silha* Bulletin *Editor Scott Memmel wrote the following article in her memory.

On Oct. 21, 2017, Helen Fitch Silha passed away at the age of 98. Together with her husband, the late Otto Silha, Mrs. Silha generously provided a grant to establish the Silha Center for the Study of Media Ethics and Law and the Silha Professorship in 1984. The Silha Center was founded to be the vanguard of the University of Minnesota School of Journalism and Mass Communication's interest in the ethical responsibilities and legal rights of the mass media in a democratic society.

Otto Silha had been president and publisher of *The Minneapolis Star* and *The Minneapolis Tribune*. He was later chairman of the Board of Directors of the company, renamed Cowles Media Company, from 1979 until his retirement from the Board in 1984. He predeceased his wife in 1999. Mrs. Silha continued to support the Silha Center after the passing of her husband through her attendance at the Center's annual Silha Lectures and Spring Forums.

Mrs. Silha was born May 21, 1919 in Manhattan, Kan., the youngest of three children. She attended Principia College in Elsah, Ill., for two years, then the University of Minnesota, where she received her Bachelor of Science degree in education in 1941.

After graduating, Mrs. Silha taught social studies and English at schools in Tracy, Minn., and worked in the Student Activities Bureau at the University of Minnesota. Beginning in 1963, she organized classes at her home in Edina for the Continuing Education for Women Program at the University of Minnesota. Mrs. Silha also served on the boards of Minnesota Early Learning Design, COMPAS, and the Edina Special Children's Group.

Mrs. Silha's spiritual life was very important to her. She was a lifelong Christian Scientist and was active in her church, Third Church of Christ, Scientist in Minneapolis.

Part of the work of the Silha Center is to provide research assistantships and fellowships to graduate students and law students. Since 1984, numerous students have benefitted from these assistantships, many of whom can now be found teaching and conducting research at leading universities or practicing at law firms across the country. The financial support from the Silha family provides numerous opportunities for research, writing, networking, and learning more about critical topics in media law and ethics.

> "Though not an attorney herself, [Helen] took a keen interest in the media law topics we explored at the Silha Center, and she loved talking with the prominent media attorneys who delivered Silha Lectures on topics such as libel, privacy, reporter's privilege, regulation of electronic media, and national security. In fact, when the Silha Research Assistants and I sat down to talk about what stories we would cover in each issue of the Silha *Bulletin*, we used Helen as our bellwether."
>
> **— Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley**

Elisia Cohen, director of the Hubbard School of Journalism and Mass Communication at the University of Minnesota, observed that Mr. and Mrs. Silha left a lasting legacy at the School. "I had the opportunity to meet Helen Silha at the fall lecture. She was a delight to speak with, and committed to the promotion of professional journalism and media ethics for the betterment of our democratic society," Cohen wrote in an email. "The legacy that she and her late husband, Otto, have provided in endowing the Silha Center for the Study of Media Ethics and Law and its Director position will benefit the Minnesota community for years to come. Now, more than ever, we need leaders like the Silha family to support professional journalism and media ethics education. On behalf of the faculty and students in the Hubbard School of Journalism and Mass Communication I extend my condolences to the Silha family. We are grateful for their legacy and continued support."

Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley also reflected on getting to know Mrs. Silha and her keen interest in media law and ethics. "I met Helen soon after I was named the Silha Professor of Media Ethics and Law in 1999.. . . I discovered that Helen was intensely concerned about contemporary issues affecting freedom of the press. Though not an attorney herself, she took a keen interest in the media law topics we explored at the Silha Center, and she loved talking with the prominent media attorneys who delivered Silha Lectures on topics such as libel, privacy, reporter's privilege, regulation of electronic media, and national security. In fact, when the Silha Research Assistants and I sat down to talk about what stories we would cover in each issue of the Silha *Bulletin*, we used Helen as our bellwether." Kirtley added, "Helen also cared -- a lot -- about ethics, just as Otto had. She sometimes fretted about what she saw as a decline in standards in the traditional mainstream media, and encouraged the Silha Center to address that."

On a personal note, I always made a point of talking to Mrs. Silha and her family at Silha Center functions. Mrs. Silha was always willing to listen to the latest happenings with the Silha Research Assistants and was so complimentary of our work. I think I speak on behalf of all past and present Silha Research Assistants when I say how thankful we are for the funding and opportunities provided by the Silha Family. Mrs. Silha will be missed, but certainly never forgotten. Thank you, Helen Silha.

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
(612) 625-3421

Non-profit Org.
U.S. Postage
PAID
Twin Cities, MN
Permit No. 90155

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW
HUBBARD
SCHOOL OF JOURNALISM
& MASS COMMUNICATION

THE STATE OF OUR SATIRICAL UNION

Hustler Magazine, Inc. v. Falwell at 30

The State of Our Satirical Union: *Hustler Magazine, Inc. v. Falwell* at 30 symposium will mark the anniversary of a landmark Supreme Court decision, issued in 1988, affirming the First Amendment right of editorial cartoonists and satirists to lampoon public figures.

But 30 years later, satirists of all stripes are working in an environment that presents challenges to freedom of speech unimaginable when the unanimous court decided *Hustler v. Falwell*. There are calls to change libel laws to make it easier to sue the news media. Cartoonists and journalists face intimidation on social media platforms. In the era of Trump and *Charlie Hebdo*, will *Hustler's* protections endure?

The symposium will explore the many dimensions of the *Hustler* decision, including the history of the case and participation by editorial cartoonists and other First Amendment advocates as "friends of the court." Leading media law scholars and editorial cartoonists will interpret the legacy of the ruling in the context of major political events and legal developments of the last 30 years.

The symposium will feature some of the country's best-known editorial cartoonists, whose work will be displayed throughout the event.

April 20-21, 2018 Cowles Auditorium, West Bank

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW
HUBBARD
SCHOOL OF JOURNALISM
& MASS COMMUNICATION

ASSOCIATION
OF AMERICAN
EDITORIAL
CARTOONISTS

MINNESOTA JOURNALISM CENTER
HUBBARD SCHOOL OF JOURNALISM
& MASS COMMUNICATION