THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | SUMMER 2016

Gawker Shuts Down After Losing Its Initial Appeal of $140 Million Judgment in Privacy Case

On Aug. 22, 2016, celebrity and media gossip website *Gawker* ceased operations after losing its initial appeal of a $140 million judgment in a March 2016 trial court battle with Terry Bollea, better known as professional wrestler Hulk Hogan. The closure came after several tumultuous months for *Gawker*'s parent company, Gawker Media, in which Florida state courts denied motions that the $140 million judgment be stayed pending appeal, bankruptcy filings, and revelations that a billionaire tech entrepreneur funded Hogan's lawsuit as part of a personal vendetta against the media company. The final blow against *Gawker* came on August 16 after Gawker Media was sold during a bankruptcy auction to Univision Communications Inc., which opted to close down the gossip website. Many legal observers remained divided over the end of *Gawker*'s operations. Some critics suggested that *Gawker* could only blame itself for its legal woes, while other commentators argued that the tech investor's involvement in *Gawker*'s demise was a worrisome development for independent journalism.

Gawker's legal troubles began in 2012 after it 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. The story also contained a written description of the remainder of the video as well as commentary by Daulerio about the public's fascination with celebrity sex tapes. In December 2012, Hogan filed a lawsuit against Gawker Media, its founder Nick Denton, and Daulerio in a Florida state circuit court alleging claims of invasion of privacy and intentional infliction of emotional distress. Hogan sought approximately $100 million in damages. Following several years of procedural delays and pretrial proceedings, the lawsuit went to trial in March 2016. The approximately two-week trial ended on March 18 when 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. Adding further complexity to the case, the Florida Court of Appeal for the Second District overturned a decision made by Judge Pamela Campbell, who oversaw the *Gawker* trial, to seal several court records related to an investigation that the FBI conducted into an alleged extortion attempt against Hogan by a third party. The records were unsealed on March 18 while jurors were deliberating and contained statements that Hogan, Clem, and Cole gave to the FBI under oath that directly contradicted sworn deposition statements given to *Gawker*'s attorneys in 2015. In April 2016, *Gawker* filed motions in the Florida state trial court asking Judge Campbell to overturn the jury's verdict or to greatly reduce the damages awarded to Hogan. (For more on the background of the legal dispute between *Gawker* and Hogan, see "*Gawker* Faces $140 Million Judgment after Losing Privacy Case to Hulk Hogan" in the Winter/Spring 2016 issue of the Silha *Bulletin*.)

Billionaire Tech Investor Revealed as Secret Financer of Hogan Lawsuit

Prior to the court ruling on the motions, *The New York Times* reported on May 24, 2016 that Denton suspected that an unknown third party was financing Hogan's lawsuit because several new lawsuits had been recently filed against *Gawker* by several other plaintiffs, many of whom were represented by Hogan attorney Charles J. Harder. "My own personal hunch is that it's linked to Silicon Valley, but that's nothing really more than a hunch," Denton told the *Times*. "If you're a billionaire and you don't like the coverage of you, and you don't particularly want to embroil yourself any further in a public scandal, it's a pretty smart, rational thing to fund other legal cases."

The *Times* also reported that Hogan's legal team had made several unusual economic decisions throughout the course of the lawsuit against *Gawker*, such as refusing to accept sizable settlement offers from Gawker Media as well as deciding to drop a negligent infliction of emotional distress allegation. The emotional distress claim would have required *Gawker*'s insurance company to provide financial support to the website's legal defense and provide funds toward any potential settlement. Larry Geneen, a risk management consultant, told the *Times* that the latter decision by Hogan's legal team was an atypical development. "It's a very unusual thing to do, because the insurance company would have deeper pockets than *Gawker*," Geneen said. "I've never had a situation where the plaintiff intentionally took out the claim involving the insurance company."

Gawker, *continued on page 3*

Inside This Issue

Summer 2016: Volume 21, No. 3

Silha Center Staff

***Gawker**, continued from page 1*

Later on May 24, *Forbes* reported that Peter Thiel, billionaire tech investor and co-founder of online payment service company PayPal, had been secretly funding Hogan's lawsuit against *Gawker*. *Forbes* wrote that Thiel's involvement appeared to be driven by a personal vendetta against the online gossip website. In 2007, *Gawker* spin-off website *Valleywag*, which focused on Silicon Valley gossip and rumors, outed Thiel as gay despite his attempts to conceal his sexual orientation. The investor later said that *Valleywag* had the "psychology of a terrorist" and likened it to Al-Qaeda, a terrorism organization.

In a May 25 interview with *The New York Times*, Thiel confirmed that he had funded Hogan's lawsuit. He explained that *Gawker*'s stories about him, his friends, and others had "ruined people's lives for no reason." As a result, Thiel began funding a team of lawyers to help "victims" bring lawsuits against *Gawker*. "It's less about revenge and more about specific deterrence," Thiel told the *Times*. "I saw *Gawker* pioneer a unique and incredibly damaging way of getting attention by bullying people even when there was no connection with public interest. . . . I thought it was worth fighting back."

COVER STORY

The *Times* also noted that Thiel, a member of Facebook's governing board, had previously donated money to press-advocacy group Committee to Protect Journalists and often spoke about maintaining strong protections for freedom of speech. Thiel told the *Times* that his legal pursuit of *Gawker* did not conflict with his free expression advocacy. "I refuse to believe that journalism means massive privacy violations. I think much more highly of journalists than that. It's precisely because I respect journalists that I do not believe they are endangered by fighting back against *Gawker*," Thiel said. "It's not like it is some sort of speaking truth to power or something going on here. The way I've thought about this is that *Gawker* has been a singularly terrible bully. In a way, if I didn't think *Gawker* was unique, I wouldn't have done any of this. If the entire media was more or less like this, this would be like trying to boil the ocean." Thiel also confirmed to the *Times* that he had provided financial backing to several other lawsuits that had been brought against in *Gawker* in recent years but did not provide further details.

After Thiel's confirmation of involvement with the Hogan suit, Gawker Media founder Denton published an open letter on *Gawker* on May 26 that criticized the tech investor's covert involvement in the lawsuits against the website. "Peter, this is twisted. Even were you to succeed in bankrupting Gawker Media, the writers you dislike, and me, just think what it will mean. The world is already uncomfortable with the unaccountable power of the billionaire class, the accumulation of wealth in Silicon Valley, and technology's influence over the media," Denton wrote. "You are a board member of Facebook, which is under [C]ongressional investigation after our site *Gizmodo* reported on the opaque and potentially biased way it decides what news sources are seen by its billions of users. Now you show yourself as a thin-skinned billionaire who, despite all the success and public recognition that a person could dream of, seethes over criticism and plots behind the scenes to tie up his opponents in litigation he can afford better than they."

After the investors' involvement was confirmed, some legal observers argued that Thiel's financial assistance in Hogan's legal victory over *Gawker* had little to do with the outcome of the case. In a May 26 post on *The Volokh Conspiracy* blog, Northwestern University School of Law Professor Eugene Kontorovich wrote that Thiel's actions were immaterial if Hogan's claims against *Gawker* were legitimate. "Critics of Thiel's role in the *Gawker* case argue that it is particularly inappropriate because they think he is motivated by 'revenge' over the gossip site's earlier publication of stories about his private life," Kontorovich wrote. "But if the lawsuit is not frivolous, it is hard to see how the motivations of funders are relevant (or discernible). One would not say a civil rights organization could not accept donations from philanthropists angered by a personal experience with discrimination. All Thiel has done is cut out the middleman."

> "I saw *Gawker* pioneer a unique and incredibly damaging way of getting attention by bullying people even when there was no connection with the public interest. . . . I thought it was worth fighting back."
>
> **— Peter Thiel,**
> **Billionaire tech investor and PayPal Co-Founder**

However, several other legal commentators and press advocates expressed concerns over Thiel's funding of Hogan's lawsuit against *Gawker*. In a June 10 discussion on the National Constitution Center's "We the People" podcast, Director of the Silha Center and Professor of Media Ethics and Law at the University of Minnesota Jane Kirtley said that Thiel's pursuit of *Gawker* was dangerous for press freedom. "It's not illegal for somebody to bankroll this litigation, but I think it is very troubling that we did not have, until ultimately the press dug it out, transparency about who was really behind the money that was being spent on this case," Kirtley said. "I realize that a lot of people regard *Gawker*, at best, as a poor relation to traditional news media sources, but there's a long history in this country of unconventional news media sources breaking very important stories. The fact that we are talking about an organization that many people regard as little more than a pretty spurious gossip organ is something I understand. But it doesn't seem to me to change the concern that people should have that [*Gawker*] gets run out of business by this kind of litigation. . . . I cannot say that I don't think this is troubling, either that somebody outside, without being transparent about it, is funding litigation or that a judgment of this nature would put an organization out of business. To me, those are very disturbing [developments]."

Gawker *Declares Bankruptcy After Losing Motions to Dismiss*

On May 25, 2016, the *Tampa Bay Times* reported Florida Circuit Court Judge Pamela Campbell denied *Gawker*'s motion requesting that she overturn the jury's verdict or reduce the $140 million in damages awarded to Hogan. The decision came one day after *Forbes* reported that Thiel had funded Hogan's civil suit. The *Tampa Bay Times* noted that Judge Campbell's denial of *Gawker*'s motions created a significant challenge for

***Gawker,** continued on page 4*

***Gawker**, continued from page 3*

Gawker to continue litigation because, under Florida law, the website would be required to post a $50 million bond prior to appealing the jury's decision. *Gawker* had previously stated in court documents that its net worth was $83 million in 2015, according to the *Tampa Bay Times*.

On June 10, 2016, *Slate* reported that *Gawker* had announced it had filed for Chapter 11 bankruptcy protection after Judge Campbell ruled that the website would be required to post the $50 million bond. *Gawker*'s decision to file for bankruptcy was a strategic move that would allow it to continue to operate while it began the process of appealing the $140 million judgment, according to *Slate*. By entering into bankruptcy, *Gawker* was able to automatically halt the collection of the judgment and could prevent Hogan from attempting to seize its assets as a form of payment. *Slate* reported that declaring bankruptcy also allowed *Gawker* to avoid paying the $50 million bond in order to appeal the judgment. *The Hollywood Reporter* noted on June 10 that Gawker's bankruptcy filing indicated that it had less than $100 million in assets and its biggest creditor was Hogan. As part of the bankruptcy proceedings, Gawker Media also agreed to put itself up for sale through a bankruptcy auction. *Politico Media* reported on June 10 that publishing company Ziff Davis had entered an initial bid of approximately $90 million for Gawker Media's assets.

In a June 15 post on *Gawker*, Denton wrote that filing for bankruptcy would not interrupt the day-to-day business of *Gawker* or any of Gawker Media's other websites. "The future of the business is secured by a provisional sale agreement with Ziff Davis, and by our filing on Friday for Chapter 11 protection," Denton wrote. "The legal battle, separated from the ongoing business, moves onto the next round. The spirit that animates *Gawker* remains strong. The free press is vigorous. And the power of a shadowy billionaire looks much less alarming now that it has emerged blinking into the spotlight."

"Yes, Peter Thiel's covert legal vendetta has undoubtedly depressed Gawker Media Group's valuation. His onslaught, prompted by items about Thiel and his friends on *Gawker*'s *Valleywag*, has been financially draining. Whoever buys us, it will not be for the sort of headline price that Henry Blodget or Arianna Huffington received when selling *Business Insider* to Axel Springer and *Huffington Post* to AOL. So be it," Denton added. "Where it ends up, the purchase price will also reflect the editorial choices we have made. Nobody goes into the news business, certainly not the convention-breaking news we and our readers love, simply to get rich. Better to risk, to win some and lose some, than pursue the path of least offense — at least if you're a journalist."

> "It's not illegal for somebody to bankroll this litigation, but I think it is very troubling that we did not have, until ultimately the press dug it out, transparency about who was really behind the money that was being spent on this case."
>
> **— Jane Kirtley,**
> **Director of the Silha Center and**
> **Silha Professor of Media Ethics and Law**

Gawker *Sold to Univision, Ends Operations*

On Aug. 16, 2016, *Forbes* reported that Univision Communications, Inc. had agreed to purchase Gawker Media's assets for approximately $135 million, outbidding Ziff Davis' initial $90 million offer during the bankruptcy auction that began in June 2016. Univision Communications, best known for its Spanish-language television channel, had been in talks with Gawker Media to make an investment in the company earlier in 2016 but backed out because of the Hogan verdict, according to *Forbes*. That same day, Denton released a statement explaining that the sale was in the best interest of his company. "Gawker Media Group has agreed this evening to sell our business and popular brands to Univision, one of America's largest media companies that is rapidly assembling the leading digital media group for millennial and multicultural audiences," Denton said in the August 16 statement, according to *Forbes*. "I am pleased that our employees are protected and will continue their work under new ownership — disentangled from the legal campaign against the company."

After the sale, *The Wall Street Journal* reported on August 18 that Univision Communications announced that it would end *Gawker*'s operations the following week. However, Univision Communications said that it planned to continue the operations of several of Gawker Media's other websites, such as sports-focused *Deadspin*, feminist blog *Jezebel*, and tech-oriented *Gizmodo*, among others. *The Wall Street Journal* also noted that Denton had sent a memo to *Gawker* staff indicating that he was leaving Gawker Media in the wake of its sale. "Sadly, neither I nor Gawker.com, the buccaneering flagship of the group I built with my colleagues, are coming along for this next stage," Denton wrote in the memo, according to *The Wall Street Journal*. "Desirable though the other properties are, we have not been able to find a single media company or investor willing also to take on Gawker.com. The campaign being mounted against its editorial ethos and former writers has made it too risky. I can understand the caution." *Gawker* formally ceased operations on August 22.

The announcement of the demise of *Gawker* raised concerns among many news industry observers and press advocates. In an August 17 commentary for *Time* magazine, staff writer Jack Dickey, who formerly worked for *Deadspin*, argued that the sale of Gawker Media to Univision Communication was a troubling sign for independent media organizations. "Gawker [Media] isn't going out of business, but Thiel's gambit worked. The sites are losing their independence — and what a loss that is," Dickey wrote. "[Stories about late Toronto Mayor Rob Ford smoking crack, revelations that Notre Dame football player Manti Te'o's deceased girlfriend never existed, and reports on iPhone prototypes, among others, are] stories any outlet would have chased and published. But others could be touched only by *Gawker* sites, unencumbered as they were by financial relationships with major entities.

The company's goals flowed from its editorial mission rather than its business aims. Even when *Gawker* announced aspirations to transcend publishing and become a major tech player, those initiatives never came together well enough to displace journalism as the company's primary business."

In an August 18 column, *Washington Post* media critic Erik Wemple argued that *Gawker* had held media, celebrity, and political elites accountable despite its often missteps. "Whether the figure was Brian Williams or Hulk Hogan, *Gawker* was hellbent on publishing things about [elites] that other media outlets wouldn't even allow into an editorial meeting. Though the site was a general-interest affair with obsessions in politics, entertainment and culture, its essence involved shoving a [flash light] in the eyes of celebrities, media types and politicians. The site believed in this mission so much that it applied the treatment to its own boss, [Denton], who'd risen to media elitism himself through the growth of Gawker Media," Wemple wrote. "It's no wonder that elites brought the site down. Little did *Gawker*, or the rest of the world, know that Peter Thiel . . . had bankrolled Hogan's legal action against the site, as well as other proceedings. That tidbit emerged after the trial. Extreme journalism had met extreme manipulation of the civil justice system. What ensued is a great loss for the United States, if for no other reason than that Gawker.com pushed the limits of propriety in hammering the powerful. A mainstream media too inclined to coddle these people has now lost a running example of journalistic fearlessness. And occasional recklessness, too."

Others were less laudatory when reflecting on the end of *Gawker*. In an August 22 commentary, *Ad Age* editor-at-large Simon Dumenco argued that *Gawker* only had itself to blame for its demise. "Peter Thiel, backer of Hulk Hogan's lawsuit, which drove *Gawker*'s parent company Gawker Media into bankruptcy, is responsible for *Gawker*'s death — that's the prevailing media narrative. ('Peter Thiel Just Got His Wish: *Gawker* is Shutting Down' is how *Wired* put it.) But of course, there's a parallel narrative, 13 years in the making: *Gawker* ran itself off the road," Dumenco wrote. "*Gawker* simply didn't know when to hit the brakes — or maybe it didn't even know how to operate the brakes. It slammed into a tree or crashed through the guardrail and over the cliff or [insert a visual of your choice here, with the horror level depending on whether or not you or any of your colleagues or friends or family have ever been brutalized by *Gawker*] (*sic*). By the logic of this narrative, *Gawker* killed itself. We can't rule it a suicide, though, because clearly *Gawker* didn't intend to die. But maybe it was more along the lines of, say, autoerotic asphyxiation."

In a final post on *Gawker* published on August 22, Denton defended the site's work during the 13 years of its operation while also criticizing Thiel's role in the Hogan litigation. "*Gawker*'s record for accuracy is excellent," Denton wrote. "For a site as reckless as it is purported to be, there have been no Jayson Blairs, no conflict-of-interest or plagiarism scandals, no career-ending corrections. The chief rule of establishment journalism that it violated to its detriment, it seems, is the one that recommends against pissing off billionaires."

> "*Gawker*'s record for accuracy is excellent. For a site as reckless as it is purported to be, there have been no Jayson Blairs, no conflict-of-interest or plagiarism or scandals, no career-ending corrections. The chief rule of establishment journalism that it violated to its detriment, it seems, is the one that recommends against pissing off billionaires."
>
> **— Nick Denton, Gawker Media Founder**

"Peter Thiel has gotten away with what would otherwise be viewed as an act of petty revenge by reframing the debate on his terms," Denton added. "Having spent years on a secret scheme to punish *Gawker*'s parent company and writers for all manner of stories, Thiel has now cast himself as a billionaire privacy advocate, helping others whose intimate lives have been exposed by the press. It is canny positioning against a site that touted the salutary effects of gossip and an organization that practiced radical transparency. . . . In cultural and business terms, this is an act of destruction, because Gawker.com was a popular and profitable media property — before the legal bills mounted. *Gawker* will be missed. But in dramatic terms, it is a fitting conclusion to this experiment in what happens when you let journalists say what they really think."

However, Thiel had continued to defend his legal pursuit of *Gawker* in an August 15 op-ed for *The New York Times*. "[Hogan] could not have secured justice without a fight, and he displayed great perseverance. For my part, I am proud to have contributed financial support to his case. I will support him until his final victory — *Gawker* said it intends to appeal — and I would gladly support someone else in the same position," Thiel wrote. "The defense of privacy in the digital age is an ongoing cause. As for *Gawker*, whatever good work it did will continue in the future, and suggesting otherwise would be an insult to its writers and to readers. It is ridiculous to claim that journalism requires indiscriminate access to people's sex lives. A free press is vital for public debate. Since sensitive information can sometimes be publicly relevant, exercising judgment is always part of the journalist's profession. It's not for me to draw the line, but journalists should condemn those who willfully cross it. The press is too important to let its role be undermined by those who would search for clicks at the cost of the profession's reputation."

As the *Bulletin* went to press, *Gawker*'s appeal of the $140 million judgment in favor of Hogan remained in its initial stages before the Florida Second District Court of Appeal as a result of the company's decision to file bankruptcy in June 2016.

Casey Carmody
Silha *Bulletin* Editor

Sixth Circuit Rules that Booking Photos Implicate Privacy Interests Under FOIA

In July 2016, the U.S. Court of Appeals for the Sixth Circuit held that criminal defendants have a non-trivial privacy interest in booking photos, also known as mug shots, in relation to Freedom of Information Act (FOIA), 5 U.S.C. § 552. *Detroit Free Press, Inc. v. U.S. Dep't of Justice (Free Press II)*, No. 14-1670, (6th Cir. July 14, 2016). The 2016 ruling reverses a 20-year-old decision by the Sixth Circuit holding that government officials were required under FOIA to release booking photos of criminal defendants because defendants lacked any privacy interest in the photos. *Detroit Free Press, Inc. v. U.S. Dep't of Justice (Free Press I)*, 73 F.3d 93 (6th Cir. 1996). The appellate court's 2016 decision raised concerns among several advocates for government transparency. Meanwhile, privacy advocates argued that the Sixth Circuit's decision provided necessary protections in an era when easy access to digital content can often impede upon individual privacy rights.

FOIA

The case arose in 2013 after the United States Marshals Service (USMS), a sub-division of the U.S. Department of Justice (DOJ), denied a *Detroit Free Press* FOIA request for the mug shots of four Michigan police officers charged with bribery and drug conspiracy. In denying the request, the USMS cited FOIA Exemption 7(C), which permits agencies to deny requests for "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). *The Detroit Free Press* then filed a lawsuit against the DOJ in the U.S. District Court for the Eastern District of Michigan in order to require the department to comply with FOIA. In 2014, the federal district court granted summary judgment in favor of the newspaper, holding that the Sixth Circuit's 1996 decision in *Free Press I* required that DOJ disclose the requested photos. In *Free Press I*, the Sixth Circuit ruled that the public's access to federal booking photos was not an invasion of criminal defendants' privacy rights. However, that view began to change in 2011 as the Tenth Circuit and Eleventh Circuit ruled that booking photos could interfere with individuals' privacy interests, disagreeing with the Sixth Circuit's analysis in *Free Press I*.

The DOJ appealed the ruling to the U.S. Court of Appeals for the Sixth Circuit. In August 2015, a three-judge panel for the Sixth Circuit upheld the district court's ruling, holding that it was bound by *Free Press I*'s precedent that booking photos did not fall within the scope of FOIA's privacy exemptions. *Detroit Free Press, Inc. v. U.S. Dep't of Justice*, 796 F.3d 649 (6th Cir. 2015). However, the three-judge panel's *per curiam* opinion "urge[d] the full court to reconsider the merits of *Free Press I*," noting the conflicting rulings coming out of the Tenth and Eleventh Circuits. On Nov. 20, 2015, the Sixth Circuit voted to rehear the case *en banc*.

In a Nov. 23, 2015 post on Squire Patton Boggs LLP's *Sixth Circuit Appellate Blog*, Justin Jennewine wrote that the Sixth Circuit's decision to review the case *en banc* was not surprising due to the nature of the *per curiam* opinion that the three-judge panel issued. "Given the recent reluctance to grant *en banc* review, the Sixth Circuit's decision to rehear *Free Press II* demonstrates the significance of the issue," Jennewine wrote. "The majority of the Sixth Circuit's opinion in *Free Press II* was dedicated to discussing the factors that merit reversing the holding in *Free Press I*, and it appears that a majority of the judges in the Sixth Circuit agree that the issue is one that demands a closer review."

On July 14, 2016, the full U.S. Court of Appeals for the Sixth Circuit ruled 9-7 in favor of the DOJ, determining that federal authorities can withhold booking photos of criminal defendants under Exemption 7(C) of FOIA after considering privacy interests. Judge Deborah Cook, writing for the nine-judge majority, explained that technology and society had changed significantly since the Sixth Circuit's 1996 ruling in *Free Press I*. Judge Cook wrote that these changes had rendered *Free Press I* "untenable" and that, contrary to *Free Press I*, individuals do have a non-trivial privacy interest in having their booking photos shielded from the public.

"Booking photos — snapped 'in the vulnerable and embarrassing moments immediately after [an individual is] accused, taken into custody, and deprived of most liberties' — fit squarely within [the] realm of embarrassing and humiliating information," Judge Cook wrote, citing an Eleventh Circuit decision holding that the disclosure of booking photos raised privacy concerns. "More than just 'vivid symbol[s] of criminal accusation,' booking photos convey guilt to the viewer. Indeed, viewers so uniformly associate booking photos with guilt and criminality that we strongly disfavor showing such photos to criminal juries."

Judge Cook's opinion largely focused on the differences between privacy interests in 1996 and 2016. "Disclosed booking photo casts a long, damaging shadow over the depicted individual," wrote Judge Cook. "In 1996, when we decided *Free Press I*, booking photos appeared on television or in the newspaper and then, for all practical purposes, disappeared. Today, an idle internet search reveals the same booking photo that once would have required a trip to the local library's microfiche collection. In fact, mug-shot websites collect and display booking photos from decades-old arrests: *BustedMugshots* and *JustMugshots*, to name a couple. . . . Desperate to scrub evidence of past arrests from their online footprint, individuals pay such sites to remove their pictures. Indeed, an online-reputation-management industry now exists, promising to banish unsavory information — a booking photo, a viral tweet — to the third or fourth page of internet search results, where few persist in clicking. The steps many take to squelch publicity of booking photos reinforce a statutory privacy interest."

As a result, the appellate court said that individuals have a non-trivial privacy interest in their booking photos. The court wrote that this determination meant that agencies receiving FOIA requests for booking photos must balance individuals' privacy interests against the public's interest on a case-by-case basis. "In 1996, this court could not have known or expected that a booking photo could haunt the depicted individuals for decades. Experience has taught us otherwise," Judge Cook wrote. "As the Tenth and Eleventh Circuits recognize, individuals have a privacy interest in preventing disclosure of their booking

photos under Exemption 7(C). Of course, some public interests can outweigh the privacy interest, but *Free Press I* wrongly set the privacy interest at zero. We overrule *Free Press I*, reverse the grant of summary judgment, and remand to the district court for proceedings consistent with this opinion."

Chief Judge R. Guy Cole Jr. wrote a concurring opinion, finding the majority's opinion "persuasive," and further emphasizing the changes between 1996 and 2016. "Twenty years ago, we thought that the disclosure of booking photographs, in ongoing criminal proceedings, would do no harm. But time has taught us otherwise," wrote Cole. "The internet and social media have worked unpredictable changes in the way photographs are stored and shared. Photographs no longer have a shelf life, and they can be instantaneously disseminated for malevolent purposes. Mugshots now present an acute problem in the digital age: these images preserve the indignity of a deprivation of liberty, often at the (literal) expense of the most vulnerable among us. Look no further than the online mugshot-extortion business. In my view, *Free Press I* — though standing on solid ground at the time — has become 'inconsistent with the sense of justice.' These evolving circumstances permit the court to change course."

Judge Cole also added that the majority's ruling did not categorically prevent the release of booking photos in some situations. "Today's opinion, as I read it, does not foreclose the possibility that, in the appropriate case, a requester might make a meaningful showing of the 'significant public interest' in 'reveal[ing] the circumstances surrounding an arrest and initial incarceration,'" wrote Judge Cole. "There will be time enough to deal with such a situation. The majority rightly gives the lower courts the chance to balance, in the first instance, the equally important values of public disclosure and personal privacy. Neither is abrogated."

In a dissenting opinion, Judge Danny Boggs, writing on behalf of the seven dissenting judges, argued that the majority's opinion placed too little emphasis on the strong public interest in the availability of booking photos. "Today's decision obscures our government's most coercive functions — the powers to detain and accuse — and returns them to the shadows," Judge Boggs wrote. "Open government is too dear a cost to pay for the mirage of privacy that the majority has to offer. I respectfully dissent."

Judge Boggs cited several public interest reasons for the release of booking photos, including public confidence in the criminal-justice system. "Public oversight is essential in criminal proceedings, in which the government wields the power to place the individual in jeopardy of imprisonment," wrote Judge Boggs. "Closing a window into such proceedings undermines the public confidence that is essential to any effective criminal-justice system." The dissenting opinion also noted that booking photos could "help the public learn about what the government does to those whom it detains." Judge Boggs argued that booking photos help reveal who is being arrested and prosecuted. "Booking photographs also reveal what populations the government prosecutes — black or white, young or old, female or male — and for what sorts of alleged crimes. Their release may raise questions about prosecutorial decisions, enabling the public to detect and hold to account prosecutors who disproportionately charge or overlook defendants of a particular background or demographic." Finally, the dissenters maintained that booking photos had the important public interest of helping "avoid cases of mistaken identity, by prompting individuals to assist the government in finding the actual perpetrator."

The U.S. Court of Appeals for the Sixth Circuit's decision in *Free Press II* divided privacy and government transparency advocates. In a July 15 story on the Reporters Committee for Freedom of the Press' (RCFP) website, Electronic Privacy Information Center attorney John Tran praised the ruling for protecting individuals' privacy. "They do make a point to recognize that we are in a digital age — this is an online world, and booking photos can persist in perpetuity online," Tran told the RCFP. "People's reputations can really be tarnished in a way that we didn't see 20 years ago."

American Civil Liberties Union of Minnesota Executive Director Chuck Samuelson said in a July 25, 2016 interview with the Minneapolis *Star Tribune* that the Sixth Circuit's decision to change course on privacy considerations under Exception 7(C) of FOIA was necessary to prevent the government from "broadcast[ing]" mug shots in bulk. However, Samuelson maintained that booking photos should not be completely withheld from the public either. "Secret arrests are bad, period," Samuelson told the *Star Tribune*. "You don't want it to be secret, because you want to know where the guy is."

In a July 14 interview with the *Detroit Free Press*, Orrick, Herrington & Sutcliff LLP partner Robert Loeb, who argued the case on behalf of the newspaper, said that the Sixth Circuit's decision incorrectly equated embarrassing information with the right to privacy. Loeb argued that the government was more concerned about controlling the types of information provided to the public rather than privacy rights because the Federal Bureau of Investigation often posts booking photos of criminal defendants on its website. "They just want their own discretion," Loeb told the *Detroit Free Press*. "It's about government control of information to the press."

In the same story, *Detroit Free Press* attorney Herschel Fink argued that the public should have a right to know who the government is prosecuting, and for what. "Booking photos tell the 'who' story in a way that a (defendant's) name alone can't," Fink told the *Detroit Free Press*. "They literally put a face on the government's prosecution, all the better for the public to see what the government is up to." Fink said after the ruling that the *Detroit Free Press* attorneys were considering taking the case to the Supreme Court. "We knew from the oral argument in Cincinnati that the court was very divided on the issue. The resulting 9-7 split confirms that," Fink said in the interview with the *Detroit Free Press*. "The strong dissenting opinion gives us support as we consider whether to ask the Supreme Court to give finality to this two-decades-long fight by the *Free Press* for transparency in the criminal justice system."

The case now goes back to U.S. District Court for the Eastern District of Michigan, which will decide whether the USMS should release the booking photos of the four officers per the *Detroit Free Press*' FOIA request after considering the privacy interests of the officers, according to the RCFP's July 15 story.

Scott Memmel
Silha Research Assistant

D.C. Circuit Upholds "Net Neutrality" Rules

On June 14, 2016, a three-judge panel for the U.S. Court of Appeals for the D.C. Circuit upheld the Federal Communications Commission's (FCC) 2015 Open Internet Order, Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738 (Apr. 13, 2015) (codified at 47 C.F.R. 1),

which reclassified broadband internet access as a utility and imposed provisions on internet service providers (ISPs) enforcing net neutrality principles. *U.S. Telecom Assoc. v. Fed. Comm. Comm'n*, 825 F.3d 674 (D.C. Cir. 2016) The ruling is now part of an ongoing debate between net neutrality advocates and opponents, who remain divided over the policy. Both the FCC vote and the D.C. Circuit's decision were narrow victories for proponents of net neutrality, which still faces challenges and uncertainty moving forward.

Net neutrality is the principle that ISPs should treat all data on the internet the same regardless of the source. This principle prevents discrimination or censorship of certain types of online data based on content, source, or platform. In an Aug. 16, 2016 statement, the International Federation of Library Associations and Institutions (IFLA) noted that much of the debate surrounding net neutrality has emerged from two parallel fears. "On the one hand, users fear that, in the absence of net neutrality frameworks, [ISPs] may implement undue traffic management, for instance blocking access to or downgrading the quality of applications providing competing services," the IFLA wrote. "On the other hand, ISPs argue that growth in traffic online . . . is outstripping the capacity of Internet infrastructure (wires, mobile networks) to carry it."

Proponents of net neutrality include tech firms, consumer advocates, and Internet companies, including Twitter and Amazon. Net neutrality supporters promote internet freedom and deter discrimination of online data, with many holding the view that broadband internet access should be classified as a utility, which would prevent ISPs from screening, blocking, or inappropriately interfering with the transmission of internet content.

The largest opponents to net neutrality are ISPs, which seek to maintain control over their data delivery standards. Opponents of net neutrality often argue that it deters competition among ISPs and reduces investment in broadband. In an interview with *National Review*'s Matthew Shaffer, Peter Thiel, billionaire tech investor and co-founder of online payment service company PayPal, expressed skepticism at the government's ability to effectively regulate a constantly changing industry. "Until it is a mature industry, we have no idea where real abuses would be," Thiel said.

The net neutrality debate gained public attention in 2014, after a three-judge panel for the D.C. Circuit struck down provisions of a 2010 FCC order that sought to regulate ISPs, finding that the commission had exceeded its statutory authority. *Verizon v. Fed. Comm. Comm'n*, 740 F.3d 623 (D.C. Cir. 2014). Primarily, the panel concluded that the FCC's decision to classify ISPs as "information service providers" meant that the Commission could not impose strict "common carrier" requirements on internet companies. In response to the decision, the FCC began formulating new rules to enforce net neutrality while also staying in line with the Circuit decision. These rules included a new draft provision that would permit ISPs to offer content providers the ability to pay for higher connection speeds. Critics argued that these internet "fast lanes" would effectively undermine net neutrality principles, placing start-up companies at a disadvantage to those who could afford to pay for higher speeds.

Discussion of net neutrality reached a fever pitch in the summer of 2014. In addition to a proliferation of news stories and online article discussing net neutrality, the issue was satirized on HBO's "Last Week Tonight," hosted by John Oliver, where the comedian encouraged viewers to submit comments in support of net neutrality rules on the FCC's website. Between July 15 and Sept. 15, 2014, the FCC received a record 3.7 million public comments on the issue, overwhelmingly in favor of net neutrality. In a November 2014 statement, President Obama responded to the public outcry by calling on the FCC to "implement the strongest possible rules to protect net neutrality."

On Feb. 26, 2015, in response to pressure from the public and the Obama administration, the FCC adopted the Open Internet Order, which abandoned the draft provisions allowing for internet "fast lanes" and implemented rules that reclassified broadband internet access as a "telecommunications service" under Title II of the Communications Act. The reclassification was a significant shift because broadband internet access providers had previously been classified as an "information service," which prevented courts from applying FCC regulations similar to those applied to "common carrier" communication services, like telephones.

The Open Internet Order also sought to enforce net neutrality through various provisions. These provisions included by enacting three "bright-line" rules, which ban blocking, throttling, and paid prioritization for internet content delivery. "No Blocking" prevents ISPs from blocking access to lawful destinations on the internet. "No Throttling" prohibits the impairment or degradation of lawful internet content based on its source, destination, or content. "No Paid Prioritization" prevents the creation of internet "fast lanes," whereby ISPs could favor some internet traffic over others.

In a Feb. 26, 2015 letter, President Obama praised the FCC decision, saying that it will "protect innovation and create a level playing field for the next generation of entrepreneurs." ISPs were less welcoming of the new rules. Shortly after the FCC decision, three separate groups of petitioners, consisting primarily of broadband providers and their associations, challenged the Open Internet Order, arguing that the FCC lacked authority to reclassify broadband internet access as a telecommunications service and that some of the provisions violated the First Amendment, among other claims. (For more information about the previous debate over net neutrality, see "D.C. Circuit Strikes Down FCC 'Net Neutrality' Rules" in the Winter/Spring 2014 issue of the Silha *Bulletin*, "Debates Continue Over Net Neutrality as FCC Nears Decision on 'Open Internet'" in the Fall 2014 issue, and "New FCC Rules Spur Heated Debate about Net Neutrality Regulation" in the Winter/Spring 2015 issue.)

In a 2-1 decision on June 14, 2016, the D.C. Circuit upheld the FCC's 2015 Open

Internet Order. This was a shift from the prior D.C. Circuit opinion in *Verizon v. Fed. Comm. Comm'n*, where the court vacated net neutrality provisions because broadband internet access service was classified as an "information service." In the Open Internet Order, the Commission stated that it was "in light of *Verizon*" that it was compelled to reclassify broadband. The court agreed, holding that this represented a perfectly "good reason" for reclassifying broadband internet access as a "telecommunications service."

The three-judge panel's decision took the position that an ISP is a utility and should provide equal access to all. In a jointly written opinion, Judges David Tatel and Sri Srinivasan noted that "the role of broadband providers is analogous to that of telephone companies: they act as neutral, indiscriminate platforms for transmission of speech of any and all users." In his dissent, Judge Stephen Williams argued for the Commission's Order to be vacated, in part because "[t]he Commission's justification of its switch in classification of broadband from a Title I information service to a Title II telecommunications service fails for want of reasoned decision making."

Reaction to the D.C. Circuit ruling was positive among net neutrality supporters. In a June 14 press release, U.S. Sen. Al Franken (D-Minn.), a vocal net neutrality advocate, praised the D.C. Circuit's decision. "Today's decision upholding net neutrality is an enormous victory for consumers, for businesses and startups, and ultimately for the innovation that has helped drive our modern economy," Sen. Franken said in the press release. "Net neutrality has been part of the architecture of the Internet since the beginning — and as we've seen for the past several decades, a free and open Internet has been a tremendous engine for innovation and economic growth."

Opponents of the FCC's Open Internet Order criticized the D.C. Circuit's decision, expressing concerns regarding the federal government's involvement in regulating ISPs. In a June 19 column, *The Wall Street Journal*'s L. Gordon Crovitz argued that the industry will soon face burdensome government regulations with the reclassification of broadband as a utility under the Communications Act. "Congress never intended such regulation. The Telecommunications Act of 1996 declared the internet will be 'unfettered by federal or state regulation,' except to promote competition. The FCC 'specifically forswears any findings of a lack of competition' on the internet," Crovitz wrote, citing Judge Williams' dissent. "In a better-functioning Washington, Congress would immediately reconfirm its 1996 legislation to restore the internet as a haven for permissionless innovation. The Supreme Court is the likelier salvation. The justices should refuse to defer to a regulatory agency that is neither independent nor expert. Until then, Silicon Valley is on notice that Washington is now in the business of picking its winners and losers."

On July 29, 2016, *Fortune* reported that the wireless, cable, and broadband trade association groups that had challenged the FCC's 2015 Open Internet Order asked the U.S. Court of Appeals for the D.C. Circuit to review the three-judge panel's June 14 decision *en banc*. If the full Court of Appeals denies the request, the trade association groups may appeal to the Supreme Court. In a June 14 post on *The Volokh Conspiracy*, Case Western University School of Law Professor Jonathan Adler, noting the observations of Boston College Law School professor Daniel Lyons, wrote that the Supreme Court "would have greater latitude to consider some of the arguments made against the FCC's rule than the D.C. Circuit did."

Although the D.C. Circuit decision was a win for net neutrality advocates, there are still several potential threats to the FCC's 2015 Open Internet Order. One threat is a workaround used by ISPs and mobile network operators called "zero-rating," according to the IFLA's August 16 statement. Zero-rating is a process by which ISPs data plans exempt certain content from counting against a user's data cap — certain websites, often popular ones like Facebook or YouTube, would not count against a user's data limit. Additionally, some plans require payment by content providers to the ISPs in order for their content would be zero-rated. The IFLA wrote that these "pay-to-play" arrangements could violate net neutrality principles because the deals generally favor large content providers who can afford to pay a fee, potentially discriminating against smaller businesses.

Another potential threat to net neutrality involves the 2016 presidential election. The president appoints FCC commissioners and designates the chairman as well. The Open Internet Order was adopted on a 3-2 party line vote, with the Democratic-appointed commissioners voting in favor of instituting the new rules. A Republican win in the 2016 presidential election would mean changes in FCC leadership, and possibly a change in direction for rules around net neutrality.

As of August 2016, Democratic presidential candidate Hillary Clinton's campaign website stated that she "strongly supports the FCC decision under the Obama Administration to adopt strong network neutrality rules that deemed internet service providers to be common carriers." Clinton had previously advocated for net neutrality principles in 2007 while serving as a U.S. Senator for New York, co-sponsoring the Internet Freedom Preservation Act, S. 215, 110th Cong. (2007). The bill sought to amend the 1934 Communications Act to ensure that ISPs abided by net neutrality principles, but the bill later died in committee.

Meanwhile, Republican candidate Donald Trump has remained relatively silent on net neutrality during his presidential campaign. Prior to his candidacy, Trump tweeted in 2014 that "Obama's attack on the internet is another top down power grab. Net neutrality is the Fairness Doctrine. Will target the conservative media." Other prominent Republicans have been more transparently opposed to the enforcement of net neutrality principles, including Trump's running mate, Indiana Gov. Mike Pence. As a U.S. Representative in 2011, Pence co-sponsored the Internet Freedom Act, H.R. 96, 112th Cong. (2011), which sought to prohibit the FCC from "further regulating the internet." Gov. Pence also hosted a syndicated conservative talk radio show during the 1990s.

Ronald Waclawski
Silha Research Assistant

President Obama Signs Law Making Significant Amendments to the Freedom of Information Act

On June 30, 2016, President Barack Obama signed the FOIA Improvement Act of 2016, S. 337, 114th Cong. (2016), into law, which reforms several aspects of the Freedom of Information Act (FOIA). 5 U.S.C. §552. The law's major changes to FOIA included promoting greater public access to government records that are frequently requested, creating a single online portal for FOIA requests, and placing limitations on agencies' use of FOIA Exemption 5, which allows agencies to withhold certain types of inter-agency or intra-agency communications indefinitely, according to a June 30, 2016 Reporters Committee for Freedom of the Press (RCFP) story. However, the most praised change is the explicit requirement that federal agencies must consider releasing records under a "presumption of openness" standard, rather than presuming government information is secret. The changes to FOIA came nearly 50 years after the law was originally adopted in 1966. Government transparency advocates praised the changes but also argued that further improvements to FOIA are still needed.

FOIA

In February 2015, Sens. John Cornyn (R-Texas), Charles Grassley (R-Iowa), and Patrick Leahy (D-Vt.) introduced the FOIA Improvement Act of 2016 in the U.S. Senate, which proposed several amendments to FOIA. After more than a year of committee hearings and debate, the bill was approved by unanimous consent in the Senate on March 15, 2016. The Senate's version of the bill was later introduced in the House, which adopted the Senate's version of the bill after it had previously approved a House bill on Jan. 11, 2016 introduced by Reps. Darrell Issa (R-Calif.) and Elijah Cummings (D-Md.) that proposed similar amendments to FOIA. The House passed the Senate's FOIA Improvement Act of 2016 by a voice vote on June 13, 2016. President Obama signed the bill into law on June 30. The FOIA Improvement Act of 2016 received bipartisan support in Congress as well as from several government transparency advocacy groups, including the Sunlight Foundation, OpenTheGovernment.org, the Electronic Frontier Foundation (EFF), and the Sunshine in Government Initiative (SGI), among others, throughout Congress' consideration of the bill.

Substantively, the FOIA Improvement Act of 2016 made several significant changes to FOIA. First, the bill codified a "presumption of openness," meaning that it "places the burden on agencies to justify withholding information, instead of on the requester to justify release," according to a June 13 statement on Rep. Issa's Congressional website. *U.S. News and World Report* reported on June 30 that the presumption of openness also meant that agencies could no longer rely on a standard presuming that requested records are secret. Instead, agencies can only withhold requested records when "foreseeable harm" could be caused by the release, according to a statement that White House spokesperson Brandi Hoffine provided to the Sunlight Foundation on June 14, 2016. This change to FOIA also codified President Obama's order in a memorandum sent to the heads of the federal agencies on his first full day in office in 2009 in which he ordered federal departments to operate under a presumption of openness. By codifying a presumption of openness in FOIA, future presidential administrations will be unable to reverse course by simply dismissing President Obama's memo, according to a June 30 blog post by Sunlight Foundation policy analyst Alex Howard.

> "Our very democracy is built on the idea that our government should not operate in secret. The FOIA Improvement Act will help open the government to the 300 million Americans it serves and ensure that future administrations place an emphasis on openness and transparency."
>
> **— Sen. Patrick Leahy (D-Vt.)**

The bill also strengthened requirements that federal agencies engage in the "proactive disclosure" of records in digital formats, meaning that agencies are required to disclose certain types of records without waiting for a request from the public. The law would extend these proactive disclosure provisions under FOIA to require agencies to make frequently requested records — those records which have been requested three or more times — easily available to the public in an electronic format online.

The RCFP reported on June 30, 2016 that the new law also mandated the creation of a single online portal to accept FOIA requests for any governmental agency. This portal would be similar to *FOIAonline*, which allowed for the public to submit records requests electronically and was already in use by 12 federal agencies and offices. The Office of Government Information Services (OGIS) was directed to establish the single website. The law also strengthened the OGIS' authority to function as the federal government's FOIA Ombudsman, "giving more independence and responsibility to a non-partisan, non-political office to oversee FOIA compliance," according to Rep. Issa's June 13 statement. The FOIA Improvement Act of 2016 also established a Chief FOIA Officers Council, which is made up of federal agencies' chief FOIA officers and is charged with addressing ways to improve the administration of FOIA in the federal government.

The law updated the timing of when agencies submit annual FOIA processing statistics. According to the SGI June 13 analysis of the bill, federal agencies' FOIA statistics will be processed in February so that the data is available for public release during Sunshine Week in March, an annual event overseen by the American Society of News Editors (ASNE) and RCFP to promote public awareness of access to government information. Finally, the bill limited agencies' ability to deny records requests under Exemption 5 of FOIA, which allows agencies to deny requests related to inter-agency or intra-agency

communications. Previously, various agencies would cite Exemption 5 in order to withhold records indefinitely, according to the RCFP's June 30 story. The FOIA Improvement Act of 2016 limited the withholding of "deliberative process documents" to 25 years. These include memoranda, letters, and drafts. The White House also released a fact sheet that provided more details about the law and announced new members of the FOIA Advisory Committee. The full fact sheet is available at https://www.whitehouse.gov/the-press-office/2016/06/30/fact-sheet-new-steps-toward-ensuring-openness-and-transparency.

After President Obama signed the FOIA Improvement Act of 2016, several Congressmen voiced their support of the changes, including the bill's co-sponsor, Rep. Issa. "This critical update to the Freedom of Information Act is a major milestone that enshrines into law the people's right to know what their government is actually doing. It's a significant step forward to the accountable government the people deserve," Rep. Issa said in a June 30 press release. "We've seen countless examples of how easy it is for government to cover up waste, fraud, abuse, or anything politically embarrassing through years of delays, redactions and special exemptions. The bill which will now become law will help ensure these types of injustices are a way of the past."

Sen. Leahy was optimistic that the law would have an impact for years to come. "Our very democracy is built on the idea that our government should not operate in secret," Leahy told the RCFP when the bill passed the Senate in March. "The FOIA Improvement Act will help open the government to the 300 million Americans it serves and ensure that future administrations place an emphasis on openness and transparency." Rep. Jason Chaffetz (R-Utah), Chairman of the House Oversight and Government Reform Committee, was also optimistic about the changes, as reported on Issa's website on June 13. "Passing bipartisan FOIA legislation is a major milestone and big step forward in fixing a broken process, he said. "This bill will help make government more transparent and accountable to the public." In the same press release, Rep. Cummings added, "This bill will put into law a presumption of transparency and make it easier for the public to access information from the federal government."

Jason Leopold, a VICE News senior investigative reporter, told the RCFP on June 30 that he believed that the law addressing Exemption 5 was beneficial for journalists. "I think the reform bill definitely addresses many, many concerns that we, as journalists, have with regards to FOIA," said Leopold. "Most notable [is] the B-5 exemption, which is the most abused and overused FOIA exemption." Leopold has often been critical of various federal agencies' failure to comply with FOIA in the past. During a House Oversight and Government Reform Committee hearing in June 2015, Leopold testified that the Pentagon's Office of Net Assessment offered to fulfill a FOIA request he submitted only if he promised not to file another one. (For more on Leopold's testimony and criticism, see "Obama Administration's Handling of Freedom of Information Act Requests Under Fire" in the Summer 2015 issue of the Silha Bulletin.)

> "While there is still much work to be done, the provisions enacted today will help ensure the law lives up to its purpose — informing the public about what its government is up to. As we approach FOIA's birthday this July 4th we should not only celebrate what has been accomplished over the last few decades, but also imagine what we, the people, want it to look like 50 years from now."
>
> **— Adam Marshall, Jack Nelson Dow Jones Foundation legal fellow, Reporters Committee for Freedom of the Press**

Despite the bipartisan support for the legislation in 2016, the path to amend the 50-year-old FOIA, which was last updated in 2007, had met several obstacles in recent years. Patrice McDermott, executive director of OpenTheGovernment.org, told the RCFP on June 30 that a similar FOIA reform bill in 2014 never saw a final vote in the House because several organizations within the banking industry raising concerns with the possible disclosure of records related to financial institutions. The RCFP also reported in the June 30 story that records disclosed in February 2016 as part of a FOIA request indicated that the DOJ lobbied against the major reform provisions in 2014, arguing there would be an increase in administrative costs and delays in FOIA processing.

Despite the praise of the changes to FOIA, Howard wrote in his June 30 post on the Sunlight Foundation's blog that further reforms were needed. "This bill is not a panacea for all the ills that persist around the use of FOIA," Howard wrote. "For instance, there is nothing stopping agencies from posting an email address for chief FOIA officers. Some structural issues that can and should be addressed by this Congress exercising its oversight function, communicating with the strengthened Office of Government Information Services. Others will be improved by senior agency leadership taking a stronger interest in information disclosure policy that explicitly connects open data policies to FOIA requests. The bill also does not allocate additional funding for processing requests, including investment in staffing and training to guide agencies not only toward the presumption of openness but to increase the capacity of those agencies to respond to the rising volume of requests."

In the RCFP's June 30 story, Adam Marshall, Jack Nelson Dow Jones Foundation legal fellow at the RCFP, agreed that further efforts were needed to strengthen FOIA. "While there is still much work to be done, the provisions enacted today will help ensure the law lives up to its purpose — informing the public about what its government is up to," Marshall said. "As we approach FOIA's birthday this July 4th we should not only celebrate what has been accomplished over the last few decades, but also imagine what we, the people, want it to look like 50 years from now."

Scott Memmel
Silha Research Assistant

Right to Be Forgotten Continues to Create Challenges for Online Entities

In May 2014, the Court of Justice of the European Union (CJEU) ruled that European citizens retain a right to have online search engine results deleted that link to "inaccurate, inadequate, irrelevant or excessive" information about themselves under the European Union's Data Protection Directive. Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos* (AEPD), Mario Costeja González, ECLI:EU:C:2014:317 (May 13, 2014), available at http://curia.europa.eu/juris/liste.jsf?num=C-131/12. The CJEU's ruling created significant challenges for internet search engines, online content publishers, and news media organizations that sought to comply with the decision. (For more information the CJEU's ruling and subsequent challenges, see "European Union Court Holds that Citizens Have the 'Right to Be Forgotten' from Internet Searches" in the Summer 2014 issue of the Silha *Bulletin*, and "'Right to Be Forgotten' Continues to Develop in the Year Following European High Court Decision" in the Sumer 2015 issue.)

INTERNATIONAL NEWS

These challenges continued in several ways the last half of 2015 and throughout 2016. During this time, the European Union fully enshrined a "right to erasure" in its adopted General Data Protection Regulation. Google found itself continuing to battle with EU regulators over whether it should delist links across its various domains. High courts in France and Belgium differed on the balance between a right to be forgotten and press freedoms. Countries across the world also considered whether a right to be forgotten applied within their jurisdictions.

Adopted EU General Data Protection Regulation Establishes 'Right to Erasure'

On Dec. 15, 2015, the European Commission of the European Union (EU) announced that it had reached agreements with the European Parliament and the Council of the European Union to adopt the General Data Protection Regulation (GDPR) to replace the EU's Data Protection Directive, which was adopted in 1995, in order to update and harmonize data protection regulations across the EU. Council Regulation 2016/679, 2016 O.J. (L 119). In April 2016, both the Council and the European Parliament formally adopted the GDPR, which was later published in the EU Official Journal in May 2016. The regulation will require full compliance by May 25, 2018. The EU's adoption of the GDPR came after more than four years of negotiation among EU bodies.

> "Platforms need to know in advance that the GDPR will not be interpreted to punish them for protecting users' expression and information rights. Powerful and respected bodies like the Article 29 Working Party, the office of the European Data Protection Supervisor, and national data protection authorities can and should provide that guidance."
>
> **— Daphne Keller, Intermediate Liability Director, Stanford Law School's Center for Internet and Society**

Among the many provisions of the GDPR, Article 17, titled "Right to erasure ('right to be forgotten')," provides EU citizens with "the right to obtain from [a data] controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" under specific conditions. These include when: "personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"; individuals withdraw their consent from data processing; individuals object to the data processing and there are no overriding reasons that the data processing must take place; personal data have been processed unlawfully; a different law requires a controller to erase data; or the data are collected from children.

Additionally, Article 19 of the GDPR requires data controllers to forward data subjects' erasure requests to "each recipient to whom the personal data have been disclosed." Article 17 does require that the "right of erasure" be balanced against "the right of freedom of expression and information," controller's legal obligations, public health interests, and scientific or historical research needs. The GDPR also permits data protection regulators to impose administrative fines on companies that fail to abide by the right to erasure's provisions, which can range up to 20 million euros or four percent of the company's annual turnover, whichever is higher. The full text of the GDPR is available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1.

With the delay in GDPR enforcement until 2018, legal observers have begun to speculate on how the right to erasure will work in practice. In a Jan. 27, 2016 op-ed for *Politico*, Stanford Law School's Center for Internet and Society Intermediary Liability Director Daphne Keller expressed concerns that the GDPR's right to erasure provisions could lead to excessive deletion of online content. "The new law does one very good thing for Internet users: It creates a swift process to erase the data that Internet companies collect and store internally for use in profiling, targeted advertising and the like. The downside is that this streamlined process can be used to erase content put online by Internet users — whether or not that content actually violates anyone else's rights," Keller wrote. "That's a problem. It is already far too easy for individuals or companies to raise dubious legal claims against content they disagree with, and pressure private Internet platforms to take it down. . . . The GDPR will make deleting online content even easier. Its right to be forgotten section nominally protects legitimate expression, but

it also introduces disturbing rules that, in practice, will undermine that protection."

"The exact meaning of the new right to be forgotten provisions for Internet platforms is, thankfully, debatable. Many will argue that the law doesn't apply to important platforms like SoundCloud or Facebook at all, or that other provisions are less draconian than they appear at first glance. But asking lawyers like me to endorse those interpretations is not enough. Until regulators themselves speak up to clarify the law, cautious companies will hesitate to resist any removal requests," Keller added. "To be clear, the problem is not that EU law provides a right to be forgotten for truthful information — this is consistent with Europe's longstanding approach to privacy and free expression. And the problem isn't just that Internet companies decide what information to delete (that's an issue for another day). The problem is that the GDPR's combination of rigid procedural rules, unclear application to Internet platforms, and bankruptcy-inducing high fines will encourage Internet platforms to erase their users' content — whether the law actually requires it or not."

Other legal experts have also noted that the GDPR was likely to have an impact on organizations' data practices worldwide. Article 3 of the GDPR states that the law "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union." In an April 14, 2016 interview with *The Guardian*, Sidley Austin LLP partner William Long said that non-EU companies needed to take note because of Article 3. "Organisations should be under no doubt that now is the time to start the process for ensuring privacy compliance with the regulations," Austin said. "Importantly, companies outside of Europe, such as those in the US who offer goods and services to Europeans, will fall under the scope of this legislation and will face the same penalties for non-compliance."

Online content publishers, search engines, and social media organizations will need to wait for further clarifications about the scope of the right to erasure in order to know what their obligations may be once the GDPR goes into full effect in 2018. In her *Politico* op-ed, Keller encouraged EU officials to issue such clarification in the meantime in order to assist companies with the forthcoming right to erasure. "Platforms need to know in advance that the GDPR will not be interpreted to punish them for protecting users' expression and information rights," Keller wrote. "Powerful and respected bodies like the Article 29 Working Party, the office of the European Data Protection Supervisor, and national data protection authorities can and should provide that guidance."

> "As a matter of both law and principle, we disagree with [CNIL's demand to remove links across all domains]. We comply with the laws of the countries in which we operate. But if French law applies globally, how long will it be until other countries — perhaps even less open and democratic — start demanding that their laws regulating information likewise have global reach?"
>
> **— Kent Walker, Google Global General Counsel**

Google Continues to Face Challenges over Territorial Reach of the Right to Be Forgotten

In 2016, Google continued to negotiate with European Union (EU) data protection regulators over the reach of "the right to be forgotten." Throughout the process, Google provided proposals on how to implement the right to be forgotten in a way that it hoped would be acceptable to data protection authorities. The search engine company also continued its high profile battle with France's Nationale de l'Informatique et des Liberté (CNIL) about whether it must delist search results across all of its domains.

In June 2015, CNIL ordered Google to apply the right to be forgotten to all of its global extensions. Prior to the order, Google had only removed search links from its country specific sites, such as google.fr in France, but did not remove the same results from google.com. CNIL argued that individuals' right to be forgotten would be rendered ineffective if search engine users could circumvent the delisting process by simply going to Google.com. Google refused to comply with the order, arguing that the French regulator was over-extending its territorial reach and censoring the company. In September 2015, CNIL denied an informal appeal by Google asking the regulator to reconsider its order.

In January 2016, CNIL initiated sanction proceedings against Google for failing to comply with the order. However, Bloomberg BNA reported on February 26 that Google had held discussions with national data privacy regulators throughout the EU about a potential compromise over how it could delist search links that would satisfy complaints that the company was not fully complying with EU law. In a March 4, 2014 post on the *Google Europe Blog*, Google Global Privacy Counsel Peter Fleischer announced that in addition to removing links from only European extensions of its website, the search engine would also begin to use geo-location signals, such as IP addresses, to effectively limit user access to delinked URLs among all its various domains.

This change in policy meant that European users would be unable to see delisted links on any of Google's extensions, including google.com, when their IP address located them in the country where the deletion request originated. "So for example, let's say we delist a URL as a result of a request from John Smith in the United Kingdom. Users in the UK would not see the URL in search results for queries containing [John Smith] when searching on any Google Search domain, including google.com," Fleischer wrote. "Users outside of the UK could see the URL in search results when they search for

Forgotten, *continued on page 14*

Forgotten, *continued from page 13*

[John Smith] on any non-European Google Search domain." He also noted that the change would apply retrospectively to all links that Google had previously removed.

Fleischer explained that Google's decision was aimed at addressing EU data protection regulators' concerns. "We're changing our approach as a result of specific discussions that we've had with EU data protection regulators in recent months," Fleisher wrote. "We believe that this additional layer of delisting enables us to provide the enhanced protections that European regulators ask us for, while also upholding the rights of people in other countries to access lawfully published information."

Bloomberg BNA reported on Feb. 26, 2016 that several regulators were considering whether Google's new approach would sufficiently adhere to the requirements of the CJEU's May 2014 decision. "[The CJEU's judgment] entails full-fledged recognition of data subjects' rights," a spokesman for the Garante, Italy's data protection authority, told Bloomberg BNA. "[T]he measures announced by Google recently do show innovative features compared to [Google's] initial response." Legal experts also wondered whether the change in Google's practice would ease regulators' concerns. "It's difficult to assess whether the DPAs will be satisfied," Berlin-based JBB Lawyers attorney Carlo Piltz told Bloomberg BNA in a March 7 interview. "If one looks at their prior statements, perhaps not. On the other hand, this solution might now be considered as the best compromise."

However, CNIL announced on March 24, 2016 that Google's change in policy was not sufficient to "give people effective, full protection of their right to be delisted." The agency said that Google's new processes were not acceptable for several reasons, including that individuals outside of Europe could still access search results that would infringe upon the privacy rights of French citizens, individuals within the EU could still access delisted search results related to French citizens when the search originated from a non-French IP address, and digital tools that mask IP addresses could easily circumvent Google's new process.

CNIL determined that Google was obligated to apply the right to be forgotten across all of its domains because the search engine only used a single data processing procedure across all of its web domains. CNIL also maintained that its requirements did not impede upon freedom of expression because it was not ordering the deletion of any online content. "At a physical person's request, it simply removes any links to website pages from the list of search results generated by running a search on the person's first name and surname," CNIL wrote in a statement announcing its decision. "These pages can be accessed when the search is performed using other terms." As a result of its findings, CNIL fined Google 100,000 euros, approximately $112,000, for failure to delete links across all of its domains.

> "U.S. businesses and consumers accessing information that is lawfully disseminated over the internet would be hampered by search results that are limited by CNIL's take on the right to be forgotten."
>
> **— Scott Vernick, Fox Rothschild LLP Partner and Summer associate Jessica Kitain**

On May 19, 2016, *The Guardian* reported that Google intended to appeal CNIL's ruling to the Conseil d'État, France's highest court for administrative justice. In a May 19 op-ed in French newspaper *Le Monde*, Google Global General Counsel Kent Walker argued that agreeing to CNIL's demands would lead to further censorship. "As a matter of both law and principle, we disagree with [CNIL's demand to remove links across all domains]. We comply with the laws of the countries in which we operate. But if French law applies globally, how long will it be until other countries — perhaps less open and democratic — start demanding that their laws regulating information likewise have global reach?" Walker wrote in the op-ed, which was also posted on the *Google Europe Blog*. "This order could lead to a global race to the bottom, harming access to information that is perfectly lawful to view in one's own country. For example, this could prevent French citizens from seeing content that is perfectly legal in France. This is not just a hypothetical concern. We have received demands from governments to remove content globally on various grounds — and we have resisted, even if that has sometimes led to the blocking of our services."

"In deference of this foundational principle of international law, we today filed our appeal of the CNIL's order with France's Supreme Administrative Court, the Conseil d'État," Walker added. "We look forward to the Court's review of this case, which we hope will maintain the right of citizens around the world to access legal information." As the *Bulletin* went to press, Google's appeal had not moved beyond the initial stages of the appellate process.

The EU's adoption of the General Data Protection Regulation may raise the stakes for Google in its litigation over the right to be forgotten. In a May 2, 2016 Bloomberg BNA commentary, DLA Piper LLP attorneys Carol Umhoefer and Caroline Chancé predicted that Google could face much larger penalties in the future if CNIL's order is upheld on appeal. "If CNIL's decision becomes final, Google will have to further adapt its approach to the right to be forgotten or face an additional fine up to 300,000 euros ($339,535). Although the financial implications may not seem very threatening to Google today, the French Assembly recently voted to increase the CNIL's sanctioning power," the attorneys wrote. "The current draft of the French Law for a Digital Republic[a comprehensive bill designed to regulate digital activity in France] provides fines up to the higher of 20 million euros ($22.6 million) or, for legal entities, 4 percent of yearly worldwide revenues during the financial year preceding the year during which the violation occurred. Although not yet law, this provision could take effect before the GDPR's anticipated application in the first half 2018. And even today, violations of the Law are punishable by criminal sanctions; a fine up to 1,500,000 euros ($1,696,950) can be ordered for processing individuals' personal data despite their legitimate objection."

Legal observers have also suggested that the ultimate outcome of the battle between CNIL and Google could have worldwide implications. In a June 20 commentary for Bloomberg BNA, Fox Rothschild LLP partner Scott Vernick and summer associate Jessica Kitain argued that CNIL's order could potentially limit information access for any person internationally. "If upheld, French law would control the search engine results of a person accessing Google in the U.S. The foregoing sets a dangerous precedent, raising questions of state sovereignty and conflicts of laws, and triggering a slippery slope of extraterritorial rule over the availability of information over the Internet," they wrote. "U.S. businesses and consumers accessing information that is lawfully disseminated over the internet would be hampered by search results that are limited by CNIL's take on the right to be forgotten. Cutting off sections of the internet as dictated by a nation-state tends to legitimize the efforts of countries like China, Iran and Turkey that have long controlled, or attempted to control, the information their citizens access online."

"Although each country may have a right to protect the personal privacy of its citizens in ways that it sees fit, this right should not impede the rights of other countries to do the same," Vernick and Kitain added. "If upheld, the approach to personal privacy proscribed by CNIL threatens to trample the equal and competing legitimate rights of businesses and consumers outside the EU."

High Courts in EU Member Countries Differ on Whether Right to Be Forgotten Trumps Freedom of Press

In 2016, high courts in EU member countries took different approaches on balancing the "right to be forgotten" and freedom of expression concerning newspapers' online archives. In late April 2016, the Belgian Court of Cassation determined that an individual's request to have his name removed from a digital version of a story in an online archive could override a newspaper's freedom of expression rights. A few weeks later, the French Court of Cassation ruled that the removal of two brothers' names from an online digital newspaper archive hindered the newspaper's rights of free expression.

On April 29, 2016, the Belgian Court of Cassation upheld a lower appellate court decision that *Le Soir*, a French-language Belgian newspaper, needed to comply with a doctor's request that it remove his name from a story from a 1994 story found in its digital archive. Cour de Cassation [Cass.] [Court of Cassation], April 29, 2016, No. C.15.0052.F (Belg.). *Le Soir*'s story reported that the doctor was involved in a car accident that killed two people. In 2008, *Le Soir* made its news story archives freely available online, which included the 1994 story. After *Le Soir* refused to honor the request to remove his name, the doctor brought a civil action against the newspaper in an attempt to make it comply.

> "The Board acknowledges the relevance of the human right to privacy, as defended by the so-called 'right to be forgotten,' but strongly believes that newspaper archives, whether on paper or digitalised, should remain intact in the interests of freedom of informatin and historical accuracy."
>
> **— Elena Perotti, World Association of Newspapers and News Publishers (WAN-IFRA)**

In September 2014, the Court of Appeal of Liège ruled that the archived version of the story online violated the doctor's right to be forgotten under the EU Data Protection Directive. The Belgian Court of Cassation upheld the lower court's decision, ruling that the publication of a digital archive was considered a new disclosure of facts of an individual's past that could infringe upon his privacy rights. When trying to balance privacy and free expression, the high court determined that the story with the doctor's name was more likely to cause greater harm to his privacy as compared to the harm caused to the newspaper's expressive rights if the story was removed. As a result, the Court of Cassation determined that the interference with freedom of expression was justified and that *Le Soir* must remove the doctor's name from the news stories in its archives.

In response to the decision, the Board of World Association of Newspapers and News Publishers (WAN-IFRA) announced in June 2016 that it had adopted a resolution opposing the Belgian court's decision. "The Board acknowledges the relevance of the human right to privacy, as defended by the so-called 'right to be forgotten,' but strongly believes that newspaper archives, whether on paper or digitalised, should remain intact in the interests of freedom of information and historical accuracy," Elena Perotti, WAN-IFRA executive director of legal affairs and external relations, wrote in a June 12, 2016 blog post announcing the resolution. "Furthermore, it maintains that any imposed alteration of news articles represents an unacceptable restriction on the freedom of the press."

However, not all high courts in EU member states took the same approach as Belgium's court. On May 12, the French Court of Cassation issued a short ruling in a similar case that found that the removal of two brothers' names from the online archives of French newspaper *Les Echos* infringed upon free expression principles, according to a June 2, 2016 post by Kristof Van Quathem and Nicolase Rase on Covington & Burling LLP's *Inside Privacy* blog. The brothers had asked *Les Echos* to remove a news story from its searchable online archive that reported on sanctions imposed upon them by the French government's securities and exchange authority. The newspaper refused the request. The brothers brought a civil suit against *Les Echos* in an attempt to get the digital story removed, which eventually reached the French Court of Cassation. In its ruling, the high court determined that EU Data Protection Directive's exceptions for the journalistic processing of data exempted *Les Echos* from complying with the brothers' request. As a result, the brothers' case was dismissed.

Forgotten, *continued on page 16*

Forgotten, *continued from page 15*

Russia's Right to Be Forgotten Law Goes into Effect

On Jan. 1, 2016, a Russian law granting a right to be forgotten within the country went into full effect, according to an April 4, 2016 Bloomberg BNA story. The law, which Russian President Vladimir Putin signed in July 2015, permits Russian citizens to ask search engines to delete links to personal information online that are inaccurate or unlawfully published. The Russian law also permits citizens to sue search engines that fail to comply in a timely manner. On Dec. 30, 2015, Bloomberg BNA reported that President Putin signed a bill that also established financial penalties for search engine companies that failed to comply with the country's right to be forgotten requirements. Search engine companies could face fines between approximately $1,000 and $1,400 for failing to remove links at the requests of users, as well as fines between approximately $11,000 and $14,000 for failing to adhere to court orders requiring the removal of links, according to Bloomberg BNA.

In April 2016, Bloomberg BNA reported that Russia's largest search engine, Yandex, announced in a March 2016 statement that it had denied a majority of individuals' requests to remove information. The company reported that it had received more than 3,600 removal requests from 1,348 individuals since the law went into effect in January, but rejected 73 percent of the requests because it could not confirm whether the links that individuals requested to be removed actually contained personal information that was inaccurate or illegally published.

In its statement, Yandex argued that the Russian law should be amended so that individuals would first need to obtain a court ruling or receive approval from a law enforcement agency prior to seeking the removal of information. The company also suggested that the law be changed to mandate that all individuals submit their requests electronically because handling paper requests had proven to be time-consuming and difficult, according to Bloomberg BNA.

Canada's Office of the Privacy Commissioner Calls for Public Discussion on the Right to Be Forgotten

During 2015, the Office of the Privacy Commissioner of Canada announced that it would tackle reputational privacy as a primary issue in the coming years. As a result, the office published a discussion paper, titled "Online Reputation: What are they saying about me?", on Jan. 21, 2016 analyzing many of the significant challenges for maintaining privacy and personal reputation online. In its analysis, the Privacy Commissioner's Office discussed the CJEU's ruling on "the right to be forgotten" and the consequential implications in the EU. The office recognized that Canada did not have any laws that would clearly permit recognition of such a right and discussed various challenges that the right to be forgotten might pose in the Canadian context. The discussion paper also called on the public to provide its responses on whether a right to be forgotten could be applied in Canada, and, if so, in what ways. The full report of the Commissioner's Office is available at https://www.priv.gc.ca/information/research-recherche/2016/or_201601_e.pdf.

> "A 'right to be forgotten' could have serious harms to a wide range of societal interests. Hyperlinks communicate that something exists. It is difficult to overstate the importance of search engine results and the essential role that hyperlinks play with respect to the exercise of freedom of information in today's world."
>
> **— Eloïse Gratton, Borden Ladner Gervais LLP**

In a May 2 letter responding to the Office of the Privacy Commissioner of Canada's call for public response, a coalition of 12 Canadian news organizations and press freedom advocates, including Canadian Journalists for Free Expression, Newspapers Canada, *Buzzfeed Canada*, and *Vice News*, among others, argued in an open letter that a right to be forgotten would violate the Canadian Charter of Rights and Freedoms. "The right to be forgotten mandate can and has been used as a tool for wealthy and powerful individuals to clean Google searches of negative, truthful information linked to their names, restricting the public's ability to fairly access legal and accurate information. This makes it harder for dissidents and journalists to reach the public, and leaves citizens less well-informed," the coalition wrote. "The right to be forgotten, [no matter how it may be] interpreted in the Canadian context, conflicts with the Charter of Rights and Freedoms, section 2(b): the right to 'freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.' Information and stories published online should not be made to disappear from the purview of inquisitive citizens. The right to be forgotten is a danger to press freedom and freedom of expression and has no application in Canada." The coalition's open letter is available at http://www.cjfe.org/the_right_to_be_forgotten_a_threat_to_press_freedom_in_canada.

Some legal observers have also suggested that a Canadian right to be forgotten would raise significant problems. In a May 9, 2016 op-ed for *The Financial Post*, Eloïse Gratton, a partner at Montréal-based firm Borden Ladner Gervais LLP, wrote that its recognition would have a negative impact on Canadian society. "A 'right to be forgotten' could have serious harms to a wide range of societal interests. Hyperlinks communicate that something exists. It is difficult to overstate the importance of search engine results and the essential role that hyperlinks play with respect to the exercise of freedom of information in today's world," Gratton wrote. "By allowing people to remove access to their personal information at will, important information might become inaccessible, incomplete or misrepresentative. There might be a great public interest in the remembrance of information, especially

since one can never predict what information might become useful in the future."

A spokesperson for the Office of the Privacy Commissioner told Bloomberg BNA on June 9 that the office had not made a final decision about how it would approach the issue and that it was not planning to recommend legislation anytime soon. "We'll be using what we learn to inform public debate on online reputation, to better inform the Canadian Parliament on the issues and potential solutions and also to develop our own policy positions on the right to be forgotten and other forms of recourse," spokesperson Tobi Cohen said. "However, at this point we have yet to develop a position, and we also have an investigation underway that deals directly with the right to be forgotten."

At least one Canadian province has considered whether the right to be forgotten would apply to information accessible online. In April 2016, Québec's Commission d'accès à l'information (CAI), the province's administrative body handling complaints over data privacy, considered whether a right to be forgotten could be found in the province's Act Respecting the Protection of Personal Information in the Private Sector, which requires private sector companies to correct inaccurate information they hold about individuals. C.L. c. BCF Avocats d'affaires, 2016 QCCAI 114 (2016) (Can.). The CAI's decision involved a former legal assistant who had ended her employment with a law firm. The firm subsequently scrubbed any information that it had about the assistant from its website. However, a Google search of the assistant would provide at least one result still linking her name to the former firm due to third-party internet archive websites publishing an archived version of the firm's page from 2013. Fearing that prospective employers may contact her former employer and learn negative information, the assistant submitted a rectification request to the CAI to have the search result links removed. During proceedings, the law firm claimed that it had done everything in its power to remove the information from its actual website and that it had little control over the third-party websites.

In its ruling, the CAI determined that the Private Sector Act's "right to rectification" was distinct from a right to be forgotten. The Commission found that the law firm had done everything within its ability to remove any information linking the former assistant to the firm. The information that remained available through search engine results was from an internet archive service, which was publishing information that was accurate when initially collected in 2013. As a result, the law firm was under no obligation to find a way to remove information that was found after a Google search of the assistant's name. The CAI also did not indicate whether Google should be ordered to remove the links.

> "Criminals who were exposed to the public due to media reports of their arrest are entitled to the benefit of having their private life respected and their rehabilitation unhindered. In modern society, it is extremely difficult to live a calm life once information is posted and shared on the Internet, which should be considered when determining whether [the information] should be deleted."
>
> **— Hisaki Kobayashi, Japanese District Court Judge**

In a July 20 commentary in Fasken Martineau LLP's *Intellectual Property Bulletin*, attorneys Marc-André Boucher and Antoine Guilmain wrote that the CAI's decision might cast doubt on a right to be forgotten under existing Canadian law. "The courts continue to hammer home the message that 'no one is required to do the impossible. Common sense must always prevail' in the matter at hand[.] [W]hile we must acknowledge that this case offers an excellent opportunity to debate fine points of the law, the problem is striking in its simplicity: the (uncontested) evidence was that the firm did everything necessary to remove the applicant's information online; the firm fulfilled all of its legal obligations," they wrote. "Finding the firm liable for violating an unattainable obligation — delisting/de-indexing the applicant's information on the Web — could therefore not be seriously contemplated. The application for examination of a disagreement was therefore dismissed. That is the story in its simplified, not simplistic, telling."

"This decision is the first sighting on the Québec scene of the 'right to be forgotten'. The idea has been considered, examined and understood, but has not been agreed to. Outside the courtroom walls, the societal component of the right to be forgotten certainly did not escape the Commission; it encompasses a 'certain vision of society', a choice about the future and the need to find a permanent balance between the collective interest (and in particular the duty of remembrance) and private interests (the right to informational self-determination, for example)," Boucher and Guilmain added. "Now, more than ever, the legal community will have to take the right to be forgotten seriously. Was this right truly appropriate in the Canadian and Québec contexts? What are the constitutional limits, or what might they be, particularly in respect of freedom of expression? Can we rethink a 'right to be forgotten' and formulate it in a way that is tailored to reflect the legal systems across Canada? That is the challenge that the Office of the Privacy Commissioner of Canada issued in January."

Right to Be Forgotten Developments Elsewhere

Several other countries have also been considering whether their citizens have a right to be forgotten. On Feb. 27, 2016, *The Japan Times* reported that a Japanese district court cited a "right to be forgotten" in December 2015 when it ordered Google to remove links to news stories about a man's arrest in connection to child prostitution and pornography that were three years old. Presiding Judge Hisaki Kobayashi's order was the first time that a Japanese court had explicitly recognized a right to be forgotten, according to *The Japan Times*. Previous cases had

Forgotten, *continued on page 18*

Forgotten, *continued from page 17*

cited individuals' right to privacy as a justification to issue such orders.

In the order, Judge Kobayashi determined that, depending on the nature of the crime, individuals had a right to have information about them be forgotten after an adequate amount of time. "Criminals who were exposed to the public due to media reports of their arrest are entitled to the benefit of having their private life respected and their rehabilitation unhindered," Kobayashi wrote, according to *The Japan Times*. "In modern society, it is extremely difficult to live a calm life once information is posted and shared on the Internet, which should be considered when determining whether [the information] should be deleted." *The Japan Times* reported that Google intended to appeal Judge Kobayashi's order.

In April 2016, Bloomberg BNA reported that Ukraine's parliament, the Verkhovna Rada, was considering legislation that would update its civil code to create a right to be forgotten for its citizens. The law would permit Ukrainian citizens to demand the retraction and removal of online information that harms the "honor, dignity or business reputation of an individual." The bill also would allow users to request retractions electronically. Bloomberg BNA reported that both the Verkhovna Rada and the Ukrainian president must approve the law before it can take effect.

On May 1, 2016, *The Times of India* reported that a Delhi banker had submitted a plea to the Delhi High Court asking online search engines to remove personal details about him from their search results. In the plea, the banker alleged that an online search of his name resulted in links to websites containing details about a marital dispute between the banker and his wife from years earlier. The dispute was later resolved in court, and attorneys for the banker said that he and his wife were living happily together. As a result, the banker asked the Delhi High Court to order online search engines to remove the links to the details from their search results, according to *The Times of India*. In accepting the plea, Justice Manmohan of the Delhi High Court requested that India's Ministry of Communication and Information Technology, Google, and an Indian software developer brief the court on the issue of the right to be forgotten. The court also scheduled a hearing for September 2016 to consider the matter, according to a May 6 *CatchNews* report.

On May 2, 2016, the Korean Communications Commission (KCC), South Korea's telecommunications and internet regulatory agency, released its "Guidelines on the Right to Request Access Restrictions on Personal Internet Postings," which would allow South Korean consumers to request that website operators and search engine companies delete online content. "These [guidelines] are not legislated requirements but a strong start for the enforcement of the right to be forgotten in South Korea," a KCC spokesperson told *Bloomberg BNA* on May 9. The non-binding guidelines would require websites and search engines to delete digital content that individuals had posted and are unable to remove on their own.

The guidelines require users to submit applications containing the URL of the content they want removed, a reason why the content should be removed, and evidence of their identity. Website operators and search engines must authenticate the requester's identity prior to removal. The guidelines permit third parties to object to the deletion of content if they can prove that they uploaded the content in question. Additionally, the KCC's guidelines give individuals the ability to designate a family member who can exercise the right to be forgotten on their behalf after death. The KCC contended that the guidelines could also be enforced against foreign online companies if they offer Korean-language services to South Koreans. According to *Bloomberg BNA*, the KCC noted that the guidelines were "preliminary" and would probably be revised in the future. The guidelines went into effect in June 2016.

Casey Carmody
Silha *Bulletin* Editor

Supreme Court Issues Long-Awaited *Spokeo* Ruling

DATA PRIVACY

On May 16, 2016, the U.S. Supreme Court decided *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), vacating and remanding the U.S. Court of Appeals Ninth Circuit's decision holding that the lower court failed to properly analyze the "concreteness" requirement for establishing an injury-in-fact. Since the Ninth Circuit's decision in 2014, consumer protection and privacy advocates have expressed concerns about the implications that a Supreme Court ruling could have on similar suits involving procedural violations, including cases regarding the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., and the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710.

Spokeo involved the operator of an online "people search engine," Spokeo, Inc., which gathered personal information about individuals for users, including employers seeking to evaluate prospective employees. Information pertaining to the plaintiff Thomas Robins contained inaccuracies, misrepresenting his marital and employment status and inflating his income and level of education. These inaccuracies prompted Robins to file a class action suit against Spokeo, alleging violations of the FCRA. The FCRA requires consumer reporting agencies, such as Spokeo, to "follow reasonable procedures to assure maximum possible accuracy" of information within consumer reports. 15 U.S.C. § 1681e(b).

In 2011, the U.S. District Court for the Central District of California dismissed Robins' complaint for lack of Article III standing under the U.S. Constitution. Article III standing requires a plaintiff to demonstrate that he has suffered an injury-in-fact, which consists of the invasion of a legally protected interest which is concrete and particularized. The Ninth Circuit reversed the district court decision in 2014, holding that Robins had adequately alleged injury-in-fact to establish standing. (For more information on the Ninth Circuit decision, see "U.S. Supreme Court Accepts Review of *Robins v. Spokeo, Inc.*" in the Summer 2015 issue of the Silha *Bulletin*.)

In the U.S. Supreme Court's ruling, Justice Samuel Alito, writing for a 6-2 majority, vacated and remanded the Ninth Circuit decision, based on the lower court's failure to consider concreteness as a separate issue. The Court held that concrete injuries were *de facto* — that they must actually exist. In determining whether an intangible harm, such as that argued in *Spokeo*, is sufficient under Article III, Congress's judgment was both "instructive and important." Despite this deference to the legislature and noting that Congress "plainly sought to curb the dissemination of false information" with the FCRA, the Court held that Robins could not satisfy the concreteness requirement with a "bare procedural violation." Justice Alito illustrated this difference by arguing that an incorrect zip code or failure to provide the required notice would be a procedural violation of the FCRA, though would result in no concrete harm.

In a concurring opinion, Justice Clarence Thomas distinguished between applying the injury-in-fact requirement in private versus public actions. "Congress cannot authorize private plaintiffs to enforce public rights in their own names, absent some showing that the plaintiff has suffered a concrete harm particular to him," wrote Justice Thomas. "Robins has no standing to sue Spokeo, in his own name, for violations of the duties that Spokeo owes to the public collectively, absent some showing that he has suffered concrete and particular harm."

In a dissenting opinion, Justice Ruth Bader Ginsburg, joined by Justice Sonia Sotomayor, found "no utility" in remanding the case to the Ninth Circuit. Although the majority observed that Robins would fail if he alleged only a "bare" procedural violation, Justice Ginsburg argued that Robins' complaint goes beyond a bare procedural violation. "Robins complains of misinformation about his education, family situation, and economic status, inaccurate representations that could affect his fortune in the job market," wrote Justice Ginsburg.

U.S. Supreme Court observers have criticized the *Spokeo* decision, suggesting that the ruling contained inherently contradictory logic and lacked clear guidance for lower courts about how plaintiffs establish "concreteness" of injury. One such contradiction involves the role Congress has played in elevating intangible harms to concrete injuries, which the Court simultaneously acknowledged and ignored by still requiring a concrete injury "even in the context of statutory violation." In a May 17, 2016 post on LinkedIn's *Pulse* blog, Daniel Solove, the John Marshall Harlan Research Professor of Law at George Washington University Law School, argued that while the Court sought to restrict Congress's ability to establish concrete harms via statutory violations, it failed to create a sufficient test for determining when Congress is not permitted to elevate such violations to that level. Solove also noted that one of the examples proffered by the Court of an erroneous zip code could result in actual injury, because information about a zip code could reveal information regarding a person's income, ethnicity, or distance from workplace, potentially disqualifying the applicant in the eyes of potential employers.

In a June 22, 2016 commentary for *The Legal Intelligencer*, Reed Smith LLP attorney Richard L. Heppner Jr. wrote that merely citing procedural failures is no longer sufficient to establish standing, and that plaintiffs after *Spokeo* must now show that the defendant's conduct caused or increased the risk of harm. Heppner argued that despite this, *Spokeo* provided "little guidance for other 'increased risk' cases," particularly in areas of data misuse.

Legal observers have also suggested that cases most likely to be affected by *Spokeo* are those involving similar statutes where a procedural violation creates a private action. For example, in a June 17, 2016 commentary for *Forbes*, Greg Herbers, a staff attorney for non-profit legal organization The Washington Legal Foundation, argued that the VPPA is one such statute that could be subject to a renewed standing challenge post-*Spokeo*. The VPPA allows for private individuals to sue "video tape service providers" who disclose "personally identifiable information" to unauthorized persons. Because the VPPA allows for private actions based only on violation of the statute, such actions may require plaintiffs to establish that disclosure of the "personally identifiable information" created a concrete injury. Herbers argued the Supreme Court "clearly reminded circuit courts that standing analyses required a consideration of concrete injury to the plaintiffs."

Ronald Waclawski
Silha Research Assistant

Eighth Circuit Overturns Jesse Ventura's Victory in Libel and Unjust Enrichment Suit

DEFAMATION

In June 2016, the U.S. Court of Appeals for the Eighth Circuit overturned a jury decision in favor of former Minnesota Gov. Jesse Ventura who brought defamation and unjust enrichment claims against *American Sniper* author Chris Kyle's estate. *Ventura v. Kyle*, 2016 825 F.3d 876 (8th Cir. June 13, 2016). In overturning the decision, the three-judge panel for the Eighth Circuit focused its decision primarily on procedural matters and Minnesota law rather than First Amendment principles relating to defamation. However, the panel's decision left the door open for Ventura to continue to pursue his defamation claim against the Kyle estate. Many free expression advocates praised the outcome of the Eighth Circuit's decision but were disappointed that the panel did not consider substantive issues related to the First Amendment.

The dispute between Ventura and the Kyle estate began in January 2012 when William Morrow, an imprint of HarperCollins Publishers, published *American Sniper: The Autobiography of the Most Lethal Sniper in U.S. Military History*, by former Navy SEAL sniper Chris Kyle. The book quickly rose in popularity, reaching number one on *The New York Times'* bestsellers list within a month after publication. One subchapter in the book recounted an alleged 2006 incident between Kyle and an older celebrity Navy SEAL, identified only as "Scruff Face," at a bar in California. According to Kyle's account, Scruff Face had made disparaging remarks about the SEALs and said that the military unit "deserved to lose a few." Kyle wrote that he punched Scruff Face, who fell to the floor. Kyle also wrote that rumors had circulated that Scruff Face had a black eye while speaking at a SEAL graduation event the following day.

Although Kyle did not identify Scruff Face in print, he later named the person as Ventura during interviews while promoting the book. On Jan. 23, 2012, Ventura filed a complaint in the United States District Court for the District of Minnesota against Kyle, alleging claims of defamation, misappropriation, and unjust enrichment. Specifically, Ventura claimed that a Google search of his name resulted in millions of hits restating Kyle's alleged falsehoods. Ventura also alleged that Kyle's statements had injured his reputation as former governor and undermined future opportunities as a political candidate and commentator. Kyle was later shot and killed in February 2013 by another military veteran who was suffering from post-traumatic stress disorder. Kyle's wife, Taya, was appointed as executrix of Kyle's estate and became the defendant against Ventura's lawsuit.

In July 2014, the trial began between Ventura and Kyle's estate. In order to be successful on his defamation claims, Ventura, a public figure, was required to prove that Kyle had acted with actual malice, meaning that Kyle made his comments with knowledge of falsity or with reckless disregard for the truth, as required by *New York Times v. Sullivan*, 376 U.S. 254 (1964), and *Gertz v. Robert Welch Inc.*, 318 U.S. 323 (1974). During the trial, the testimony of witnesses for both Ventura and the Kyle estate disputed where the fight took place as well as whether the fight had actually occurred. Ventura's attorneys also provided photographs from that day after the alleged incident in which Ventura did not appear to be suffering from any physical repercussions of a fight. During jury deliberations in late July 2014, the attorneys for both Ventura and the Kyle estate agreed to accept a divided decision after the jury expressed doubt that they could reach a unanimous decision. On July 29, 2014, the jury arrived at an 8-2 decision in favor of Ventura, finding that he had proven his defamation claims. The jury awarded $500,000 in damages to Ventura on the defamation claim. The jury also found that the Kyle estate had been unjustly enriched due to Kyle's alleged fabrication and awarded $1,345,477 to Ventura. (For more information about the background of Ventura's claims and the trial, see "Jesse Ventura Awarded $1.8 Million for Libel and Unjust Enrichment" in the Summer 2014 issue of the Silha *Bulletin*.) Taya Kyle later sought a motion for judgment as a matter of law or for a new trial, which the district court denied. She then appealed the jury's decision.

On June 13, 2016, a three-judge panel for the U.S. Court of Appeals for the Eighth Circuit overturned the jury's decision. Writing for the 2-1 majority opinion, Judge William Riley declined to dismiss Ventura's defamation claims as a matter of law. Rather, the majority ruled that the decision must be overturned because Ventura's attorneys had made improper statements throughout the trial about HarperCollins' insurance coverage related to *American Sniper*. During the trial, Ventura's attorneys attempted to cast doubt on the testimony of two HarperCollins employees by asking about the publisher's insurance coverage. The attorneys suggested that the publisher had a direct financial interest in the outcome of the case because HarperCollins was paying for the Kyle estate's legal fees and had paid for the insurance coverage to protect against any legal claims arising from Kyle's book. During the trial's closing arguments, Ventura's attorneys suggested that HarperCollins' insurance company would be required to pay any monetary penalty for defamation.

Judge Riley wrote that the references to an insurance policy had a prejudicial effect against the Kyle estate because the jurors were likely to believe that an "impersonal deep-pocket insurer," rather than Taya Kyle, would be responsible for any financial penalty resulting from a defamation decision. As a result, the majority ruled that the Kyle estate received an unfair trial and remanded the defamation claim for a new trial. In a dissenting opinion, Judge Lavenski Smith disagreed with the majority's opinion, arguing that the Ventura attorneys' references to insurance policies had not prejudiced the jury. Judge Smith also wrote that Kyle's requests for a mistrial during the district court proceedings had not followed proper procedures, and therefore a new trial should not be granted on appeal.

As for the unjust enrichment claims, the three-judge panel ruled unanimously that the $1.3 million award should be vacated. Judge Riley wrote that under Minnesota law, "to prevail on a claim of unjust enrichment, a claimant must establish an implied-in-law or quasi-contract in which the defendant received a benefit of value that unjustly enriched the defendant in a matter that is illegal or unlawful." The panel held that Ventura's unjust enrichment claim failed because

the former governor did not have any type of contractual relationship with Kyle. "Although Ventura is correct that 'a quasi-contract will be imposed' where 'a benefit was conferred unknowingly or unwillingly,' we reject Ventura's assertion that Ventura conferred a 'benefit' on Kyle by Ventura's mere existence as a colorful figure who might inspire people to make up stories about him," Judge Riley wrote. As a result, the court overturned the judgment in favor of Ventura on the unjust enrichment claim.

Several legal practitioners and observers agreed with the Eighth Circuit panel's decision in Ventura's case, but were disappointed that the reasoning rested on technical and procedural grounds rather than First Amendment jurisprudence. In a June 16, 2016 interview with *Minnesota Lawyer*, First Amendment attorney Mark Anfinson said that he was frustrated that the Eighth Circuit decision avoided important Constitutional questions. "I was hoping that they would reverse the defamation claim as a matter of law, concluding that the evidence on the record was not sufficient to prove actual malice by clear and convincing evidence [as required by the First Amendment]," Anfinson said. "But they didn't touch that issue. Instead, they went to this highly esoteric debate about references to insurance coverage and when certain objections were made by the attorneys, which really wasn't very satisfying."

In a June 18 interview on WCCO radio's "Saturday Night with Esme Murphy," Director of the Silha Center and Professor of Media Ethics and Law at the University of Minnesota Jane Kirtley said that the Eighth Circuit panel's decision on the unjust enrichment claim would help curtail similar claims made by others in the future. "The unjust enrichment aspect was what really made this case something to cause media lawyers and journalists a lot of concern. If that claim had survived this appeal, you would have had a lot of potential for what I would characterize as crazy cases coming out of the woodwork," Kirtley said. "Public figures and other celebrities would say, 'Just because I exist as an interesting person, if you decide to write about me and you defame me or invade my privacy, I should be able to get some of the money you made off the story.' It might not be such a big deal for a news organization, but it certainly would be for somebody who writes a book that makes a lot of money, or a screenplay, or something like that."

Others have suggested that the appellate court's technical decision may have actually been a way to ensure greater free expression protections. In a June 14 commentary for *Bloomberg View*, Harvard University law professor Noah Feldman compared the Eighth Circuit's decision regarding Ventura with how Florida state courts have been handling professional wrestler Hulk Hogan's lawsuit against the now defunct celebrity and media gossip website *Gawker*. In March 2016, Hogan won a $140 million judgment on invasion of privacy claims against *Gawker*, which published a sex-tape of Hogan in 2012. (For more on Hogan's legal battle with *Gawker*, see "*Gawker* Faces $140 Million Judgment after Losing Privacy Case to Hulk Hogan" in the Winter/Spring 2016 issue of the Silha *Bulletin*, and "*Gawker* Shuts Down After Losing Its Initial Appeal of $140 Million Judgment in Privacy Case" on page 1 of this issue.)

"The appeals court [in *Ventura*] said in a 2-1 decision that the insurance questions were improper because no evidence had been admitted to prove that the book publisher had an insurance policy that would cover the costs. One judge dissented, arguing very plausibly that the brief mentions of the possible insurance policy wouldn't have prejudiced the jury," Feldman wrote. "But what the dissent effectively demonstrates is that the [Eighth] Circuit was trying to find a way to overturn the defamation verdict in the hope that it would make the case go away. To be sure, Ventura can sue again on his defamation theory in the district court. But he will now realize that the appeals court is against him, and it would probably be a waste of money for him to try again."

"The contrast couldn't be stronger between the Eighth Circuit's decision and the Florida state court that decided in favor of Hulk Hogan in his suit against Gawker — not to mention the intermediate state appellate court that upheld some aspects of the *Gawker* trial []. The Florida courts have so far failed to realize that *Gawker* should be protected by the First Amendment because the sex tape it posted, as unsavory as it may be, was relevant to Hogan's status as a public figure who had discussed his sex life repeatedly on Howard Stern's radio show," Feldman added. "The [Eighth] Circuit is showing what the Florida judges should be doing: using all legal means available to protect freedom of expression. In this sense, the Ventura appeal should be a model for the Hogan appeals yet to come."

On Aug. 2, 2016, the Eighth Circuit declined Ventura's request to rehear his case *en banc*. The Minneapolis *Star Tribune* reported on August 10 that Ventura intended to appeal the Eighth Circuit's decision to the U.S. Supreme Court. Ventura also said that he would seek another trial on his defamation claims if necessary. "I feel I'll win again," Ventura told the *Star Tribune*. "Every time I'm the major underdog, guess who comes and makes me the favorite? The people. The people will come and take me from underdog status to victory."

However, Kirtley had already cast doubt on the prospects of Ventura's appeal. "Ventura could file a *cert* petition to the U.S. Supreme Court on the [unjust enrichment] issue. But because it is based on an interpretation of Minnesota law, and not on the First Amendment, my guess is that the Supreme Court would have absolutely no interest in taking that aspect of the case," Kirtley said in the June 18 interview on "Saturday Night with Esme Murphy." "The Supreme Court is not in the business of interpreting state law unless it violates the Constitution in some way. That's not in play here. So the only option I see is . . . going back for a new trial at the district court level." In the August 10 *Star Tribune* story, Mitchell Hamline School of Law Professor Emeritus Joseph Daly said that a new trial might be likely because Ventura did not seem particularly motivated by a financial settlement. "The governor is fighting on principle, and it could be really hard to move them away from anything but a trial," Daly said.

As the *Bulletin* went to press, Ventura's attorneys had not submitted any formal filings regarding further appeals to the U.S. Supreme Court or for a potential re-trial.

Casey Carmody
Silha *Bulletin* Editor

2016 Presidential Candidates Present Challenges for Free Expression

During the 2016 presidential race, free expression advocates have raised concerns over comments and actions taken by Republican candidate Donald Trump and Democratic candidate Hillary Clinton regarding the press. In February 2016, Trump claimed that *The New York Times* and other media outlets were publishing false information with impunity and made suggestions that libel laws in the United States should be reformed. Throughout the summer of 2016, Trump continued to criticize reporters, calling them "dishonest" and "not good people," as well as revoking press credentials from several media outlets. Meanwhile, press advocates have criticized Clinton's campaign for limiting press access because she has avoided holding press conferences for several months. As a result, both candidates' actions have led several national journalists to speculate on potential challenges for the press under a Trump or Clinton White House administration.

FREEDOM OF PRESS

Trump Alleges News Organizations Deliberately Print False News, Suggests Changes in Libel Laws

On March 1, 2016, *Politifact* reported that during a February 28 appearance on "Fox News Sunday," Trump told host Chris Wallace that he believed news organizations often published false stories because they knew they would not be sued for libel. "I think it's very unfair when the *New York Times* can write a story that they know is false, that they virtually told me they know it's false, and I say, why don't you pull the story, and they say, we're not going to do that, because they can't basically be sued," Trump said during the show. "And you (Wallace) can't be sued because you can say anything you want, and that's not fair." Trump's comments came after he previously stated on February 26 that, as president, he would change libel law in the United States. "One of the things I'm going to do if I win . . . I'm going to open up our libel laws so when they write purposely negative and horrible and false articles, we can sue them and win lots of money," Trump said, according to *PolitiFact*.

In light of the comments, several media scholars and legal experts pushed back against Trump's assertions, explaining that the presidential candidate's thoughts appeared misguided. University of Michigan Law Professor Leonard M. Niehoff told *PolitiFact* on March 1 that Trumps claims about news organizations intentionally publishing false information were not correct under the law. "Under *New York Times v. Sullivan*, the type of knowing lie that Mr. Trump describes is not protected by the First Amendment," Niehoff said. Regarding libel laws, Director of the Silha Center and Professor of Media Ethics and Law at the University of Minnesota Jane Kirtley explained there are already ways for figures, like Trump, to take action against publications. "A public figure or public official must plead and prove actual malice," said Kirtley, citing *Sullivan*, in an interview with *PolitiFact*. "If he or she does, then yes, he or she could prevail, absent some other defense." Under *Sullivan*, public officials do have the ability to recover damages from a news organization for libelous statements, but they must first prove that the organization acted with actual malice, meaning that the organization made the statements with knowledge of falsity or with reckless disregard for the truth. *New York Times v. Sullivan*, 376 U.S. 254 (1964).

CNN reported on May 31, 2016 that Trump's criticism of the press continued during a contentious news conference held after news organizations questioned the candidate's claims that he raised $5.6 million for military veterans at an event earlier in 2016. However, Trump spent nearly 40 minutes criticizing and insulting reporters, both in general terms and individually. At different points, he called reporters "dishonest," "not good people," and among "the worst human beings" he has ever met, according to CNN. "I think the political press is among the most dishonest people that I have ever met, I have to tell you. I see the stories, and I see the way they're couched," Trump said during the press conference. CNN reported that Trump also went on to say that the combative nature toward the press would continue were he to become president. "Yeah, it is going to be like this," Trump said. "You think I'm gonna change? I'm not gonna change."

In a May 20, 2016 commentary for the *Columbia Journalism Review* (*CJR*), Committee to Protect Journalists Executive Director Joel Simon wrote that Trump's overly combative nature with journalists should raise concerns for press freedom. "Trump has promised that when he's president media companies like *The New York Times* and *The Washington Post* will have lots of 'problems' in the form of libel suits. 'We're going to open up libel laws, and we're going to have people sue you like you've never got sued before,' Trump said at Texas rally in February," Simon wrote. "Trump has variously denounced journalists as 'dishonest,' 'scum,' and 'sleaze.' This kind of overheated rhetoric could be dismissed, except that Trump supporters seem to take it as license to insult, attack, smear, and heckle journalists and harass them online."

Washington Post *Joins Several Organizations that Trump Bars from Covering Campaign Events*

On June 13, 2016, Trump went beyond simply criticizing the press when he announced that he had revoked *The Washington Post*'s press credentials to cover his campaign events. In a June 13 post on Twitter, Trump wrote, "Based on the incredibly inaccurate coverage and reporting of the record setting Trump campaign, we are hereby revoking the press credentials of the phony and dishonest *Washington Post*." In a subsequent post, Trump criticized a particular headline in the wake of the Orlando club shooting in June 2016. "I am no fan of President Obama, but to show you how dishonest the phony *Washington Post* is, they wrote, 'Donald Trump suggests President Obama was involved with Orlando shooting' as their headline. Sad!" Trump wrote on Twitter. *The Washington Post* reported on June 13 that Trump was referring to an article titled, "Donald Trump seems to connect President Obama to Orlando shooting." Trump accurately quoted the original headline, which the *Post* changed after Trump's tweet. However, the *Post* claimed that the newspaper changed the headline "on its own, before Trump's complaint," according to the June 13 story.

In a June 13 press release, the Trump campaign elaborated on his reasons behind pulling the *Washington Post*'s press credentials "We no longer feel compelled to work with a publication which has put its need for 'clicks' above journalistic integrity," the press release stated. "They have no journalistic integrity and write falsely about Mr. Trump. Mr. Trump does not mind a bad story, but it has to be honest. The fact is, *The Washington Post* is being used by the owners of Amazon as their political lobbyist so that they don't have to pay taxes and don't get sued for monopolistic tendencies that have led to the destruction of department stores and the retail industry."

On June 14, 2016, CNN Money reported that the revocation of the *Post*'s credentials was not the first instance of Trump adding a news organization to a credentials "blacklist." The Trump campaign revoked credentials from the *Des Moines Register* during the summer of 2015. CNN Money reported that at the time, then-campaign manager Corey Lewandowski issued a press release explaining the decision, stating, "We're not issuing credentials to anyone from *The Des Moines Register* based on the editorial that they wrote earlier in the week." CNN Money reported that the Trump campaign had also barred Univision from campaign events after candidate filed a lawsuit against the media company for cancelling the broadcast of his Miss USA Pageant in the wake of his controversial comments related to undocumented Mexican immigrants. Other organizations that the Trump regularly refused to provide credentials to included *Buzzfeed*, *Politico*, *The Daily Beast*, and *The Huffington Post*, according to CNN Money.

Noah Shachtman, executive editor of *The Daily Beast*, told CNN Money that his publication was blocked by the Trump campaign after publishing critical coverage of the candidate. "We were never a Trump favorite, but things got very frosty after we published a story last year about allegations that Ivana Trump made and later walked back about Donald Trump," Shachtman said. "[Tim Mak, who wrote the story] was the first of our reporters to be cut off . . . [and] by the time the New Hampshire primary rolled around, even our freelancers were getting cut off."

In a July 2016 press release, *Washington Post* Executive Editor Martin Baron criticized Trump's decision to block publications from obtaining credentials to cover his campaign. "Donald Trump's decision to revoke *The Washington Post*'s press credentials is nothing less than a repudiation of the role of a free and independent press," Baron said in the press release. "When coverage doesn't correspond to what the candidate wants it to be, then a news organization is banished."

However, on July 29, 2016, Trump's running mate, Indiana Gov. Mike Pence, who hosted a conservative talk radio show during the 1990s, told conservative radio host Hugh Hewitt during an interview that the Trump campaign was discussing lifting the press credential "blacklist," according to *The Washington Post*. "I have a long history, as you well know, Hugh, of advocating and defending for a free and independent press," Gov. Pence told Hewitt. "You know, I authored legislation in the Congress. We actually got it passed once or twice, to create, you know, the ability to keep confidential sources confidential. So we're going to have those conversations internally, and I fully expect in the next 100 days we're going to continue to be available to the media, whether they're fair or unfair." (For more information on federal shield laws that Gov. Pence sponsored, see "Shield Law Bills Introduced Again in U.S. House and Senate" in the Winter 2009 issue of the Silha *Bulletin*, "House Passes Federal Reporter Shield Law" in the Fall 2007 issue, "Proposed Federal Shield Law will go to House Floor; Justice Department and Big Business Offer Criticism" in the Summer 2007 issue, "Shield Law Update: New Federal Shield Bill Introduced" in the Spring 2006 issue, and "Federal Shield Law Debated in Hearings Before Senate Judiciary Committee" in the Summer 2005 issue.)

On Aug. 30, 2016, *Politico* reported that the Trump campaign did appear to be loosening restrictions it had placed on several news organizations. *The Washington Post*, *BuzzFeed*, *Politico* and *The Huffington Post* were all listed as part of the Trump campaign's press pool rotation, which involves news organizations combining reporting efforts by taking turns to report on Trump's activities on behalf of all of the organizations within the pool rotation. *Politico* reported that news organizations involved in the negotiations with Trump campaign over how the press pool rotation would operate demanded that only the news organizations, rather than the campaign, would determine which press outlets would have membership in the pool. "We are pleased to announce that after some start-and-stop negotiations with the Trump campaign, we are debuting our full print pool this week, starting with *BuzzFeed* today in Washington," read an e-mail, according to *Politico*, sent to the press poll by representatives of *The New York Times* and *Time* magazine, who are managing the press pool.

Critics Also Raise Concerns over Clinton Campaign's Limitations on Press Access

Alternatively, press advocates have also criticized Democratic candidate Hillary Clinton, for failing to hold regular press conferences to publicly answer journalists' questions. CNN Money reported on Sept. 1, 2016 that Clinton had not held a press conference during the entirety of 2016. Clinton last held a press conference on Dec. 4, 2015, according to CNN Money. However, *Politico* reported on July 10, 2016 that Clinton said during an interview with CNN reporter Jake Tapper that she believed that she was accessible to the press, noting that she has given nearly 300 interviews during 2016 alone. Clinton's running mate, U.S. Sen. Tim Kaine (D-Va.), also defended Clinton's availability to the press during a September 1 interview with CBS "This Morning." "You see Hillary take questions from reporters every day," he said. "I don't see what the massive difference is between a press conference and talking to the press everywhere you go. She talks to the press a lot. And I've been with her when she's talked to the press."

On Aug. 5, 2016, *The Huffington Post* reported that the Clinton campaign held what they called a press conference in which the candidate fielded questions from two journalists serving as moderators at a joint gathering of the National Association of Black Journalists (NABJ) and National Association of Hispanic Journalists (NAHJ). Clinton also took questions from three other journalists as well. MSNBC national correspondent Joy Reid, one the journalists who asked a question, said that the event was a good step forward for Clinton in an August 5 post on Twitter, writing "Kudos to #NABJNAHJ16 for nabbing that Hillary Clinton Q&A." However, Reid added in the same post, "Not quite a press conference, but the closest in a long while." Several other

Candidates, *continued on page 24*

Candidates, *continued from page 23*

journalists were more critical of the Clinton campaign, arguing that the event was not a press conference. "@NABJ/@NAHJ president describes today's event with Clinton as a large press conference. It is not," wrote CNN Reporter Dan Merica in an August 5 post on Twitter. That same day, Lisa Lerer, the national politics reporter for the Associated Press, also wrote on Twitter, "I would not exactly call a couple Qs from pre-selected journalists a press conference. #NABJNAHJ16."

In an August 18 post on *The Washington Post*'s political blog The Fix, columnist Chris Cillizza wrote that Clinton's refusal to hold a press conference was a problem. "It's beyond ridiculous that one of the two people who will be elected president in 80 or so days continues to refuse to engage with the press in this way. But she does sit-down interviews! And she did a 'press conference' with a moderator, um, moderating questions!" Cillizza wrote. "Not good enough. Not when you are running to be president of the United States. One of the most important things when someone is offering themselves up to represent all of us is that we get the best sense we can about how that person thinks on his or her feet, how they deal with unwanted or adversarial questions. Those two traits are big parts of doing the job of president in the modern world."

Observers Suggest Either Outcome of 2016 Election Could Be Troublesome for the Press

As a result of the issues raised by both major presidential candidates related to freedom of the press, several national writers discussed their concerns if either were to become president. In a July 14 *USA Today* op-ed, Carol Lee, the outgoing president of the White House Correspondents' Association (WHCA), together with incoming president Jeff Mason, wrote that they were "alarmed by the treatment of the press in the 2016 presidential campaign," focusing on both candidates in their critique of the 2016 presidential campaign. "The public's right to know is infringed if certain reporters are banned from a candidate's events because the candidate doesn't like a story they have written or broadcast, as Donald Trump has done," Lee and Mason wrote. "Similarly, refusing to regularly answer questions from reporters in a press conference, as Hillary Clinton has, deprives the American people of hearing from their potential commander-in-chief in a format that is critical to ensuring he or she is accountable for policy positions and official acts."

"The United States will not have a free press if its president gets to choose which journalists and which media organizations are allowed access to the executive branch. We will not have a truly free press and an informed electorate if the president doesn't believe he or she should be held accountable to inquiries from the media," they added. "It is a reporter's job to cut through the rhetoric from candidates, scrutinize whether their policy proposals would benefit Americans in the way they claim and question the viability of their promises. If we cannot do our job, then the American people cannot do theirs. That's why we are concerned both with the rhetoric directed at the media in this campaign and the level of press access to the candidates. Both Clinton and Trump can do better."

> "President [Barack] Obama campaigned on a promise to lead the 'most transparent' administration in American history but has failed to meet that commitment. Based on the candidates left in the race, there is a good chance the situation will get worse, not better, in the next administration. The question to be decided on Election Day is how much worse, and how quickly."
>
> **— Joel Simon, Executive Director, Committee to Protect Journalists**

In a June 15, 2016 commentary on *The Huffington Post*, Bill Blum, a lecturer at the USC Annenberg School of Communications, expressed similar concerns, writing, "As we head for the general election, the First Amendment — particularly, freedom of the press — is at risk." Blum noted that every generation faces "unique" press freedom concerns but argued that candidates in the 2016 election were particularly worrisome when it came to the press and widespread government surveillance. "This time, in the continuing shadow of 9/11 and the never-ending war on terror abroad and at home, the dangers come not only from the expanded operations of government agencies like the NSA and FBI, but from the ambitions of both presumptive presidential nominees — Donald Trump and Hillary Clinton — who seek control over the levers of mass surveillance and the coercive powers of the state," Blum wrote. "Whatever important differences they may have in other policy areas or in terms of personal style, temperament and experience, neither Trump nor Clinton can be counted on as an ally or partner in the struggle to preserve freedom of the press against excessive state surveillance. To protect a free and open press — to the extent it is still possible at all — we'll have to rely on ourselves, remaining ever skeptical of those in power, and, as the old saying goes, 'eternally vigilant.'"

In his May 20 commentary for *CJR*, the Committee to Protect Journalists' Simon suggested that neither Trump nor Clinton presented a good choice for widespread press freedom and government transparency in the future if elected. "President [Barack] Obama campaigned on a promise to lead the 'most transparent' administration in American history but has failed to meet his commitment," Simon wrote. "Based on the candidates left in the race, there is a good chance the situation will get worse, not better, in the next administration. The question to be decided on Election Day is how much worse, and how quickly."

Scott Memmel
Silha Research Assistant

Revenge Porn Remains Controversial Topic for State and Federal Legislatures

In May 2016, Minnesota Gov. Mark Dayton signed a bill that would criminalize "revenge porn," which is the online distribution of nude photos or other sexually explicit content depicting another person without consent. On June 20, 2016, Rhode Island Gov. Gina Raimondo vetoed a similar bill that was meant to outlaw the "unauthorized dissemination of indecent material." In Vermont, a judge dismissed charges brought against a woman for violation of the state's "revenge porn" law, enacted in 2015. Meanwhile, Congresswoman Jackie Speier (D-Calif.) introduced a bill on July 7, 2016 that would aim to make revenge porn illegal at the federal level.

ONLINE SPEECH

Minnesota Enacts Revenge Porn Statute

On May 19, 2016, Minnesota Gov. Mark Dayton signed HF 2741 into law, which created "civil and criminal penalties for the nonconsensual dissemination of private sexual images, commonly referred to as 'revenge porn.'" The law would also require prosecutors to show that an alleged perpetrator knew that the person depicted in the pictures believed the images would remain private and had not agreed to share the images any further. According to a May 3, 2016 *MinnPost* story, Minnesota's bill would make the act a gross misdemeanor or a felony, depending on the circumstances. Rep. John Lesch (DFL-St. Paul) introduced the bill, which passed the Minnesota Senate 62 to 3 on May 2, 2016 and 128 to 0 in the House of Representatives on May 16. (For more information on this law, see "Minnesota Legislature Considers Criminalizing 'Revenge Porn'" in the Spring 2016 Silha *Bulletin* and "Minnesota Court of Appeals Declares Defamation Statute Unconstitutional" in the Summer 2015 issue).

In an Aug. 16, 2016 post on his official Facebook page announcing an award from the Minnesota Coalition Against Sexual Assault for his work on the bill, Rep. Lesch argued that Minnesota's newly enacted revenge porn law was necessary in the digital media environment. "In this new age of digital information, we must be vigilant in observance and protection of privacy rights — especially when digital images are used to intimidate, harass, and embarrass," Rep. Lesch wrote. "Sexual crimes against intimate partners will not be tolerated in Minnesota."

Rhode Island Governor Vetoes Revenge Porn Bill

In Rhode Island, Gov. Gina Raimondo vetoed a bill, H7537, which aimed to "curb the dissemination of private sexual material over the internet," according to a June 21, 2016 story by *The Providence Journal*. The state Senate unanimously approved the bill on May 26, 2016 and the House voted 68 to 1 in favor of the bill on June 14. However, Raimondo voiced concerns that the bill could hinder free speech. "The bill is apparently intended to curb the dissemination of private sexual material over the internet, but its sweep is much broader," Gov. Raimondo wrote in her veto statement, according to the *Providence Journal*. "It could also cover works of art that depict the human body. And unlike virtually all other similar state statutes, H7537 does not include basic safeguards such as the requirement that 'intent to harass' be demonstrated for conduct to be criminal."

"The breadth and lack of clarity may have a chilling effect on free speech. We do not have to choose between protecting privacy rights and respecting the principles of free speech," added Gov. Raimondo in a letter to state legislators. "The right course of action is to follow the example of other states, and craft a more carefully worded law that specifically addresses the problem of revenge porn, without implicating other types of constitutionally protected speech."

The Rhode Island bill would have made a first offense a misdemeanor. If convicted, the offender would be subject to imprisonment up to one year, a fine of $1,000, or both, according to *The Herald News*. Repeated offenders would face a higher fine up to $3,000 and up to three years in prison. The legislation would have also created criminal penalties for those engaged in "sextortion," which, according to Attorney General Peter Kilmartin's office, was a new cybercrime where victims are extorted into paying money, or providing more photos or videos, in order to have embarrassing nude photos removed from website. The penalty for "sextortion" would have been up to five years in prison, a fine of up to $5,000, or both. Lawmakers in Rhode Island can override Raimondo's veto with a three-fifths vote in both the House and the Senate, but, as the *Bulletin* went to press, legislative leaders had not commented on whether they would call the Assembly back to do so.

Several Rhode Island legislators criticized Gov. Raimondo's decision to veto the bill. House Speaker Nicholas Mattiello issued a press release saying that he was "extremely disappointed" because the bill was part of a larger package of domestic-violence measures, according to a June 11, 2016 story by CBS-affiliate WPRI "Eyewitness News." "I am surprised because she never raised any concerns during the four months that it was under consideration by the House," Mattiello said in a press release.

Attorney General Kilmartin issued his own press release on June 21 that pushed back against Raimondo's concerns that the bill would raise free expression challenges. "I am confident that after review by our criminal, civil, and appellate units, as well as by the General Assembly, that we could have easily and successfully defended the constitutionality of the bill if challenged," he said in the statement. "This legislation protects victims who are being exploited, harassed, and stalked by individuals who willfully and intentionally post intimate photos and videos to exact revenge or cause humiliation. . . . I applaud the General Assembly for recognizing the need to update our laws to reflect the changing nature of crime due to advances in technology."

Executive director of the Rhode Island Coalition Against Domestic Violence Deb DeBare voiced her disappointment in an interview with WPRI "Eyewitness News," but also said she understood Raimondo's concerns that the bill was "overly broad" and would have been likely to face challenges in court. "So while I'm disappointed in the sense that there isn't a good solid piece of legislation that has now become law, I do have a commitment from the governor and

Porn, *continued on page 26*

Porn, *continued from page 25*

her policy staff to work toward a more tightly crafted piece of legislation for next session," DeBare said.

Raimondo and DeBare were not alone in their concerns over the bill. *The Providence Journal* reported that American Civil Liberties Union for Rhode Island Executive Director Steven Brown said that the bill lacked important elements protect free expression. "It is essential to recognize that this bill makes no mention of revenge or harassment, and contains no requirement that the dissemination of a photo cause harm or be intended to cause harm in order to violate the law," Brown said. "Rather, it is written so broadly that it could make criminals of people involved in neither revenge nor porn, and would have a direct impact on the First Amendment rights of the media. . . . That is why the Media Coalition, based in New York and consisting of national organizations like the American Booksellers Association, the Association of American Publishers, and the Motion Picture Association of America has . . . concern about the bill's potential impact on matters of legitimate news, commentary, and historical interest."

Vermont Judge Raises Constitutional Questions over Revenge Porn Statute

Meanwhile, a Vermont Superior Court Judge for Bennington County granted a defendant's motion to dismiss criminal charges on July 1, 2016, that were brought under the state's law criminalizing revenge porn. Decision on Motion to Dismiss, *Vermont v. Rebekah Van Buren*, No. 1144-12-15Bncr (Vt. Sup. Ct. Bennington Unit July 1, 2016). During the summer of 2015, Vermont enacted the law which "forbid[s] the distribution of sexually explicit images without the subject's consent." 13 V.S.A. § 2602(b)(1). In October 2015, prosecutors brought charges against Rebekah Van Buren, alleging that she had violated the state's revenge porn law. Van Buren accessed the Facebook account of her boyfriend and found that his ex-girlfriend had sent him nude photos despite no longer being in a relationship. Van Buren posted the nude photos without consent on her boyfriend's public page and identified the woman in the pictures. Van Buren later told police she posted the pictures "for revenge" and to harm the ex-girlfriend's reputation. After prosecutors brought charges under the revenge porn law, Van Buren filed a motion to dismiss, arguing that the statute was unconstitutionally vague both as applied and generally.

In granting Van Buren's motion, Vermont Superior Court Judge David Howard found that the photos at issue in the case were not obscene and therefore did not fall within a category of speech that has no First Amendment protection. Turning to the revenge porn law itself, Judge Howard wrote that statute raised constitutional concerns. "The possible overbreadth of this statute is a concern," he said in the opinion. "When criminal charges rest solely on acts protected by the constitutional right to free speech, the charges must be dismissed." Judge Howard's full opinion is available at https://assets.documentcloud.org/documents/2998410/State-v-VanBuren-1144-12-15-Bncr.pdf.

> "Technology today makes it possible to destroy a person's life with the click of a button or a tap on a cell phone. That is all anyone needs to broadcast another person's private images without their consent. The damage caused by these attacks can crush careers, tear apart families, and, in the worst cases, has led to suicide."
>
> **— Rep. Jackie Speier (D-Calif.)**

In an August 2 interview with Vermont alternative newspaper *Seven Days*, Van Buren attorney Albert Schaal Fox applauded the dismissal. "It's an accurate decision," he said after the case. "The statute as it's written is dangerously overbroad. I don't think anyone has come close to demonstrating the need for such an abridgment of First Amendment rights in Vermont. It's very much a case of the legislature addressing a problem that doesn't really have a demonstrated existence. To limit First Amendment speech rights without meeting that criteria of [obscenity], that has a chilling effect and is entering into an uncertain world of what is and isn't a crime and I think that's disturbing."

However, Auburn Watersong, associate director of public policy for the Network Against Domestic and Sexual Violence, told Vermont's *Valley News* in an August 1 interview that she believed the law was necessary to prevent cases of revenge porn, including the type at issue in Van Buren's case. "A rape culture would have us believe that victims, primarily women, do not have the right to privacy," Watersong told *Valley News*. She also said that the dissemination of revenge porn could also create risks for the physical safety of the victims, and that the public needed to recognize "how very dangerous these violations could be."

Bennington County state attorney Erica Marthage, who brought the charges against Van Buren, and Attorney General Bill Sorrell had jointly appealed the case to the Vermont Supreme Court, according to a Aug. 1, 2016 *Valley News* story. As the *Bulletin* went to press, the Vermont Supreme Court had yet ruled on the state's revenge porn statute.

Congresswoman Introduces Federal Revenge Porn Bill

As states were considering different types of "revenge porn" legislation, Rep. Jackie Speier (D-Calif.) also introduced federal legislation on July 14, 2016 that would criminalize revenge porn. The bill, titled the Intimate Privacy Protection Act, H.R. 5896, 114th Cong. (2016), would create criminal penalties for anyone who "knowingly uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to distribute a visual depiction of a person who is identifiable from the image itself or information displayed in connection with the image and who is engaging in sexually explicit conduct, or of the naked genitals or post-pubescent female nipple of the person, with reckless disregard for the person's lack of consent to the distribution." Violations of the law would result in criminal fines or up to 5 years imprisonment. The full text of the bill is available at https://www.congress.gov/bill/114th-congress/house-bill/5896/text.

"Technology today makes it possible to destroy a person's life with the click

of a button or a tap on a cell phone. That is all anyone needs to broadcast another person's private images without their consent. The damage caused by these attacks can crush careers, tear apart families, and, in the worst cases, has led to suicide," Rep. Speier said in a July 14 press release. "What makes these acts even more despicable is that many predators have gleefully acknowledged that the vast majority of their victims have no way to fight back. Celebrities and other high profile victims might be able to take on these predators in civil courts, but the average person can't afford that option. Even more disturbing is the number of victims who have mustered the courage and strength to pursue criminal charges, only to learn there is no law that protects them. My bill will fix that appalling legal failure."

In a July 18, 2016 commentary on *The Huffington Post*, University of Miami School of Law Professor Mary Anne Franks wrote that the Intimate Privacy Protection Act was a much needed privacy law. "The Intimate Privacy Protection Act does exactly what its title suggests: it recognizes that the right to privacy extends to sexual information," Franks wrote. "Numerous privacy laws protect the confidentiality of medical records, financial information, and many other forms of sensitive information. But existing laws offer much less protection for our most sensitive information: private photographs and videos of nudity or sexual activity. IPPA seeks to change that."

"The criticisms aimed at this bill are depressingly familiar. The pretense of First Amendment concerns, the trivialization of the harm inflicted, the limitless sympathy for perpetrators and the utter indifference to victims — these same tactics have long been used to criticize legislation against domestic violence, sexual assault, stalking, and sexual harassment," Franks added. "Perhaps the most disturbing claim made by critics of the bill is that sexual consent is ambiguous and that people should never be punished for recklessly disregarding it. That dangerous logic has helped create the sexual assault crisis we are experiencing today, and has greatly contributed to the phenomenon of nonconsensual pornography itself. Consent always matters, whether for the sexual activity is physical or virtual, and there is simply no excuse for disregarding it."

In an August 15 op-ed for *The New York Times*, Peter Thiel, billionaire tech investor and co-founder of online payment service company PayPal, praised the bill by drawing comparisons between it and his financing of professional wrestler Hulk Hogan's invasion of privacy lawsuit against Gawker. In March 2016, Hogan won a $140 million judgment against *Gawker*, who published a sex tape of Hogan in 2012. "This [bill] is a step in the right direction. Protecting individual dignity online is a long-term project, and it will require many delicate judgments," Thiel wrote. "We can begin on solid ground by acknowledging that it is wrong to expose people's most intimate moments for no good reason. That is the kind of clear moral line that *Gawker* and publishers like it have sought to blur. But they can't do it if we don't let them." (For more on Hogan's legal battle with *Gawker*, see "*Gawker* Faces $140 Million Judgment after Losing Privacy Case to Hulk Hogan" in the Winter/Spring 2016 issue of the Silha *Bulletin*, and "*Gawker* Shuts Down After Losing Its Initial Appeal of $140 Million Judgment in Privacy Case" on page 1 of this issue.)

However, Electronic Frontier Foundation (EFF) staff attorney Lee Tien criticized the bill, especially its definition of revenge porn, according to a July 14 *U.S. News & World Report* story. "It defines revenge porn in a way that doesn't match very well with what revenge porn actually is. It's reaching stuff that's not actually the problem," Tien said. Tien expressed concerns that the bill could chill free expression if businesses decided to withdraw content for fear that it is revenge porn, even if it is not. "It's never a good idea to create a rule that could go pear shaped if you can do a better job," he said.

In a July 14, 2016 blog post on *Defending People*, Mark Bennett, a Houston criminal defense lawyer, echoed the concerns about the unconstitutionality of the bill. "The Intimate Privacy Protection Act of 2016 is a content-based restriction on speech, unconstitutional under current Supreme Court case law. In order for the Supreme Court to uphold it, it would have to recognize a category of historically unprotected speech that includes nonconsensual pornography," Bennett wrote. "IPPA's advocates have written a presumptively unconstitutional statute. They have not suggested a path to constitutionality. They address a problem that has not been overwhelming state criminal-justice systems. Perhaps there are better uses for Congress's time."

The American Civil Liberties Union (ACLU) has repeatedly opposed similar state laws, including an Arizona statute in July 2015, according to the *The Huffington Post*. In Arizona, the ACLU brought a federal lawsuit against the state arguing that its revenge porn statute was overbroad and put booksellers, photographers, publishers and librarians at risk of felony charges for publishing images fully protected under the First Amendment, according to *The Hill* on July 15, 2015. The ACLU later settled the lawsuit with the state, which included terms that barred state prosecutors from bringing charges under the revenge porn statute. "You shouldn't need a permission slip to post images of horrific torture from Abu Ghraib or the 'Napalm Girl' photograph that contributed mightily to changing American attitudes about the Vietnam War," Lee Rowland, an ACLU staff attorney, wrote in a July 10, 2015 blog post on the ACLU of Northern California's website. "These iconic images are obviously a far cry from 'revenge porn,' in which a person maliciously invades a former lover's privacy." The ACLU had not provided specific comment about the Intimate Privacy Protection Act as of early September 2016.

As the *Bulletin* went to press, the Intimate Privacy Protection Act had been referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, but no further action had been taken.

Scott Memmel
Silha Research Assistant

Data Breaches Continue to Plague Social Networking Websites, Government Agencies, and News Organizations

DATA PRIVACY

Throughout 2016, private companies, government bodies, and media organizations faced data breaches and cyberattacks. In May 2016, news organizations reported that a large-scale data breach of social networking service LinkedIn was much larger than initially suspected. Data breaches at other social networking sites also raised concerns among cybersecurity experts after user names and passwords were found for sale on illegal online marketplaces. Meanwhile, federal investigators alleged that Russian agents were behind a series of cyberattacks against the Democratic National Committee (DNC), the National Security Agency (NSA), and *The New York Times*.

LinkedIn Data Breach From 2012 Larger than Expected; Social Media Sites Suffer Series of Mega Breaches

In June 2012, social networking service LinkedIn was the target of a large-scale hack that resulted in the disclosure of approximately 6.5 million users' encrypted passwords in an online Russian forum. However, more recent reports have suggested that the breach may have been larger than expected. In May 2016, *Motherboard* reported that a hacker by the name "peace_of_mind" (or "Peace") attempted to sell data from the 2012 LinkedIn data breach — which contained 167 million account login credentials, and the e-mails and passwords of 117 million LinkedIn users — on a dark web illegal marketplace called "The Real Deal."

In a May 18, 2016 post on the *LinkedIn Official Blog*, LinkedIn Chief Information Security Officer Cory Scott confirmed the data for sale was genuine user information, noting that LinkedIn was "taking immediate steps to invalidate the passwords of the accounts impacted" and encouraged users to enable two-step verification as well as use stronger passwords.

LinkedIn's breach is just one in a string of social media megabreaches to have surfaced during 2016. On May 31, 2016, *Time* magazine reported that Myspace had been the victim of a hacking incident that resulted in a significant data breach. The Myspace breach resulted in the unauthorized access to personal information, including e-mail addresses, usernames, and encrypted passwords associated with approximately 360 million user accounts that were created prior to June 11, 2014. Other data breaches involving social media websites that surfaced in 2016 includes microblogging website *Tumblr*, which suffered a breach that exposed more than 65 million unique e-mail addresses and encrypted passwords, as well as adult dating website *Fling*, which suffered a breach that exposed approximately 40 million users' e-mail addresses, usernames, plain text passwords, and IP addresses, according to separate May 2016 stories by *Motherboard*.

> "[Myspace] didn't protect passwords with much rigor prior to 2013, meaning that if you use the same username and password combo on any other sites today as you did for social networking in 2007, you're at risk."
>
> **— *Wired* reporter Brian Barrett**

Motherboard reported on May 27 that the LinkedIn and Myspace passwords were originally "hashed," a process that converts the actual password to a series of letters and numbers, using an algorithm that is weak and easy for hackers to crack. An anonymous operator for *LeakedSource*, a hacked data search engine, told *Motherboard* that he had cracked "90% of the [LinkedIn] passwords in 72 hours." Tumblr passwords were encrypted using the same technique, but were additionally "salted," whereby additional random data is added to the password, making it difficult for hackers to crack, according to a May 30 *Motherboard* story.

As of August 2016, *HaveIBeenPwned*, a website that allows internet users to check whether their personal data has been compromised by a data breach, listed the Myspace, LinkedIn, Tumblr, and Fling data breaches as among the top 10 largest breaches the site has analyzed. *Ars Technica* reported on May 31 that data from all four of the social media megabreaches were available for sale by Peace on the dark web marketplace.

Experts also noted that in addition to amount of information exposed, the breaches also posed problems because of how long ago some of the incidents actually occurred. In a May 31, 2016, blog post, *HaveIBeenPwned* founder Troy Hunt explained that his analysis of the Myspace data breach suggested it happened around 2008. As a result, users who no longer use the compromised websites may not realize that their information has been exposed. In a May 31 commentary, *Wired* reporter Brian Barrett explained that the age aspect to the breach could create serious security problems for users. "It's unlikely that anyone will break into your zombie [Myspace] page; the company has invalidated user passwords for all affected accounts, and didn't store credit card or other financial info anyway," Barrett wrote. "The bigger worry, though, is that [Myspace] didn't protect passwords with much rigor prior to 2013, meaning that if you use the same username and password combo on any other sites today as you did for social networking in 2007, you're at risk."

Cyberattacks Target U.S. Political Campaigns and Organizations During Election Year

In the midst of the U.S. presidential campaign during late July 2016, news outlets began reporting that the U.S. Democratic National Committee (DNC) computer systems were hacked. According to a July 29, 2016 story by *The New York Times*, Federal Bureau of Investigation (FBI) officials told U.S. House of Representative and Senate intelligence committees that the agency

has "virtually no doubt that the Russian government was behind the theft." Early reports of the breach suggested that law enforcement officials initially believed that compromised information was limited to the private e-mail accounts of more than one hundred party officials and groups as well as documents from the Democratic Congressional Campaign Committee, the fundraising arm of the DNC. On Aug. 10, 2016, the *Times* reported that further investigations suggested that information tied to the Democratic Governors' Association might have also been affected.

On July 29, *The New York Times* reported that early analyses by CrowdStrike, a private cybersecurity firm, pointed to two Russian-based groups involved in the cyberattack: The Federal Security Service (FSB) and the Main Intelligence Directorate (or GRU). The compromised DNC information was later leaked to several news publications in June 2016 by a hacker who referred to himself as "Guccifer 2.0." On July 27, 2016, the *Times* reported that Crowdstrike and other technology specialists were unsure at the time whether Guccifer 2.0 was a lone hacker or a false persona created by Russian intelligence officials. On July 22, 2016, a day prior to the start of the Democratic National Convention, WikiLeaks also published a significant number of documents on its website that were stolen in the DNC hack, including 19,252 e-mails and 8,034 attached files.

The DNC was not the sole target of cyberattacks during the 2016 election cycle. *The Washington Post* reported on June 14, 2016 hackers had attempted several attacks that targeted groups associated with both major 2016 U.S. presidential campaigns, as well as several Republican political action committees. Reuters reported on Aug. 12, 2016 that U.S. intelligence officials had informed top congressional leaders that the Democratic Party was being targeted, but the congressional leaders were unable to warn the targets due to the classified nature of the information.

The 2016 attacks were not the first time presidential candidates have been targeted for cyberattacks during an election year. In November 2008, then-Senator and Democratic presidential candidate Barack Obama's and Republican presidential candidate John McCain's campaign computer systems were the targets of a Chinese-based cyberattack, but the resulting damage appeared minimal despite the fact that hackers downloaded large quantities of information related to policy positions, according to a Nov. 7, 2008 *Financial Times* story.

However, Skyhigh Networks CEO Rajiv Gupat suggested in a July 28 commentary for *Forbes* that WikiLeaks' timing of the publication and the substance of the leaked documents seem to suggest that hackers are seeking to influence the U.S. presidential election. The fallout from leaked documents was embarrassing for Democratic presidential candidate Hillary Clinton's campaign and the DNC, resulting in the resignation of several high profile DNC members, including chairwoman Debbie Wasserman Schultz. In the same commentary, Gupta said the hack "sets a new precedent and draws into question the US government's ability to deter state-sponsored cyberattacks on even the most sensitive government and political operations." But Gupta noted that attributing cyberattacks to their source, even with substantial evidence, can be difficult, particularly in light of the United States' own cyber-espionage efforts.

> "What makes this attack [on the Democratic National Committee] very different — and crosses the line — is the Russian team's decision to dump the Clinton campaign's opposition strategy on the public Web."
>
> **— Dave Aitel, CEO, Immunity, Inc.**

Gupta and others have suggested that the leak should be distinguished from traditional acts of espionage. In a June 17, 2016 commentary for *Ars Technica*, Immunity, Inc. CEO Dave Aitel argued that the breach and disclosure of DNC data was not traditional espionage, but more akin to an act of cyberwarfare. "What makes this attack very different — and crosses the line — is the Russian team's decisions to dump the Clinton campaign's opposition strategy on the public Web," Aitel wrote.

In addition to political campaigns, the FBI released information regarding the possible hacking of state election offices, suggesting a direct involvement in election tampering. On Aug. 29, 2016, *The Washington Post* reported that hackers had targeted voter registration systems in Illinois and Arizona. *Politico* reported on August 29 that any access to registration information "could allow hackers to digitally alter or delete registration information, potentially denying people a chance to vote."

In a Sept. 2, 2016 interview with *Bloomberg News*, Putin denied Russian involvement in the DNC hack but said that the leak was beneficial to the public. "The important thing is the content was given to the public," Putin said. On Sept. 5, 2016, *The Wall Street Journal* reported that Clinton suggested that the Russian government was trying to interfere with the election in an effort the get her opponent, Republican presidential candidate Donald Trump, elected president. However, *The Wall Street Journal* also reported that federal investigators could not determine whether Russian hackers were actually trying to influence the election or merely attempting to gather intelligence.

Leaked Data Probably Contains Power NSA Hacking Tool

On Aug. 15, 2016, *Ars Technica* reported that a hacking group referring to itself as the Shadow Brokers claimed to have hacked the servers of Equation Group, a highly sophisticated technology and hacking contractor employed by the U.S. National Security Agency (NSA). Alongside the blog post taking credit for the hack, the Shadow Brokers posted samples of code used in the production of malware built and used by the NSA. On Aug. 16, 2016, *The Washington Post*, citing unnamed NSA personnel from the agency's hacking division, the Tailored Access Operations (TAO), reported that the posted files appeared legitimate and contained several NSA-related hacking tools dating back to 2013 that could take control of firewalls, networks, and exfiltrate or modify information.

In the August 15 story, *Ars Technica* editor Dan Goodin noted that the Shadow Broker group's disclosures about NSA hacking tools occurred less than a month after another unidentified

Breaches, *continued on page 30*

Breaches, *continued from page 29*

hacker, Guccifer 2.0, published information gained from a hack of the Democratic National Committee's (DNC) computer system. Goodin suggested that, taken together, the leaks "represent a major broadside against US interests, although it's impossible to directly connect the people behind the two online personas."

The specter of Russian involvement with the Shadow Brokers leak was seen by some as a geopolitical move in response to United States' intelligence agencies attributing Russia with involvement in the DNC leak weeks earlier. In a series of Aug. 16, 2016 Twitter posts, Edward Snowden, a former-NSA contractor and whistleblower on the agency's mass surveillance efforts worldwide, wrote that "[c]ircumstantial evidence and conventional wisdom indicates Russian responsibility" and that the Shadow Brokers leak looks like someone was "sending a message that an escalation in the attribution game could get messy fast." (For more information about Snowden's disclosure of NSA documents to the public, see "Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone and Internet Communication" in the Summer 2013 issue of the Silha *Bulletin*, "Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms" in the Fall 2013 issue, "NSA Surveillance Practices Prompt Reforms and Legal Challenges Throughout All Government Branches" in the Winter/Spring 2014 issue, "Fallout from NSA Surveillance Continues One Year after Snowden Revelations" in the Summer 2014 issue, "Two Years after Snowden Revelations, National Security Surveillance Issues Still Loom" in the Summer 2015 issue, and "NSA Telephony Metadata Collection Program Remains Controversial Even after It Ends" in the Fall 2015 issue.)

***FBI Investigates Possible Hack of* The New York Times**

On Aug. 23, 2016, CNN reported that the Federal Bureau of Investigation (FBI) was investigating whether Russian hackers were behind a series of cyber attacks targeting U.S. news organizations. CNN's report, citing unidentified government officials associated with the investigation, did not specifically identify the news organizations involved in the inquiry but noted that the FBI's investigation focused on an attack targeting *The New York Times*. The unnamed officials told CNN that investigators, although not certain, thought there was a high probability that Russian intelligence operatives were behind the attacks on news organizations' servers over the course of several months.

Later that day, *The New York Times* reported that its Moscow bureau had indeed been the target of a cyberattack. However, *Times* spokeswoman Eileen Murphy said that there was no evidence that the attack was successful. "We are constantly monitoring our systems with the latest available intelligence and tools," Murphy said. "We have seen no evidence that any of our internal systems, including our systems in the Moscow bureau, have been breached or compromised." The *Times*, also citing unnamed government officials, disputed CNN's claims that the FBI's investigation extended to other news organizations.

CNN reported that U.S. intelligence agencies believed that the cyberattack on the *Times* showed that Russian spy agencies were attempting to gather intelligence from a wide range of sources involved in the American political system. The *Times* noted that U.S. officials had also blamed Russian hackers for cyberattacks carried out in 2016 against the Democratic National Committee. U.S. investigators told CNN that foreign intelligence hackers viewed news organizations as valuable cyberattack targets because reporters retain contact information as well as sensitive communications and unpublished works from government sources.

In an Aug. 24, 2016 interview with the *Christian Science Monitor*, Reporters Without Borders' head of the Eastern Europe & Central Asia desk Johann Bihr said that claims that Russian hackers had attacked news organizations were unsurprising because of the widespread surveillance that Russia conducts domestically. "The Russian surveillance system is absolutely extensive," Bihr said. "[Russia's principal intelligence agency, the Federal Security Service,] has access to the servers of each and every internet server provider at the regional level, so it's quite easy for them to intercept any communication."

Reporters Without Borders ranked Russia 148 out of 180 countries in its World Press Freedom Index 2016. "What with draconian laws and website blocking, the pressure on independent media has grown steadily since Vladimir Putin's return to the Kremlin in 2012," Reporters Without Borders wrote in its description of Russia for the 2016 ranking. "Leading independent news outlets have either been brought under control or throttled out of existence. While TV channels continue to inundate viewers with propaganda, the climate has become very oppressive for those who question the new patriotic and neo-conservative discourse or just try to maintain quality journalism."

Ronald Waclawski
Silha Research Assistant

Critics Raise Privacy Concerns Over *Pokémon Go*

DATA PRIVACY

On July 6, 2016, mobile app developer Niantic Inc. released *Pokémon Go*, a free "augmented reality" game in which players attempt to capture virtual monsters called Pokémon, in the United States in both Apple's and Android's mobile apps stores. The game makes the monsters appear on users' screens as if they were appearing in the users' same real-world location. It also requires users to travel to various locations in order to capture Pokémon. The gaming app quickly gained popularity when millions of users downloaded the app in the United States and countries across the world as the game was released internationally. However, some observers began raising concerns over *Pokémon Go*'s privacy and data access settings. Such concerns led to privacy advocates and government officials calling upon Niantic to explain its data collection and use practices.

On July 11, 2016, *CNET* reported that cybersecurity blogger Adam Reeve had discovered that iOS users had given Niantic "full access" to their Google accounts when using such accounts to sign up to play *Pokémon Go*. Full account access, according to Google, meant that Niantic was able to "see and modify nearly all information in [an] account." Later reports suggested that the amount of information that Niantic could actually access may have been limited, but observers could not be certain because Google had not provided specific details over what the "full account access" designation. The discovery that Niantic could potentially have more access than necessary to information found in users' Google accounts led to significant outcry from the public and press. On July 12, 2016, Niantic released an update to *Pokémon Go* that limited access permissions to allowing the company to see only users' Google User IDs and e-mail addresses.

In a July 11 statement to *Ars Technica* after the news about access permissions broke, Niantic said that it had not accessed users' information. "We recently discovered that the *Pokémon Go* account creation process on iOS erroneously requests full access permission for the user's Google account. However, *Pokémon Go* only accesses basic Google profile information (specifically, your user ID and e-mail address) and no other Google account information is or has been accessed or collected," Niantic said. "Once we became aware of this error, we began working on a client-side fix to request permission for only basic Google account information, in line with the data we actually access. Google has verified that no other information has been received or accessed by *Pokémon Go* or Niantic."

Others also expressed concerns that Niantic might be collecting and sharing too much information from users through *Pokémon Go*. According to the app's privacy policy, Niantic wrote that it will "collect and store information about your (or your authorized child's) location when you (or your authorized child) use our App and take game actions that use the location services made available through your (or your authorized child's) device's mobile operating system, which makes use of cell/mobile tower triangulation, wifi triangulation, and/or GPS." The privacy policy also noted that it would share collected information with various third parties that administer various services or for research and analysis purposes. The policy said that the sharing of personally identifiable information (PII) with third parties will only happen in limited circumstances, but the policy never specifically defines what the company considers to be PII. The privacy policy indicated that it was last updated on July 1, 2016.

In a July 14 interview with *Politifact*, cybersecurity expert and Binary Defense Systems founder David Kennedy said that the third-party sharing provisions should raise concerns. "With Google, it's a well-established service. Facebook is a well-established service, with terms and conditions you can read," Kennedy said. "These third-party applications could be selling your name, your address, your phone number, your contact list, what you're browsing — directly tied to your name." Kennedy also told *Politifact* that he would not be downloading the game.

Recognizing several potential data privacy concerns, U.S. Senator Al Franken (D-Minn.) sent a letter to Niantic Chief Executive Officer John Hanke on July 12 asking the CEO to describe how *Pokémon Go* collected, used, and shared users' data. "I am concerned about the extent to which Niantic may be unnecessarily collecting, using, and sharing a wide range of users' personal information without their appropriate consent," Sen. Franken wrote in the letter. "I believe Americans have a fundamental right to privacy, and that right includes an individual's access to information, as well as the ability to make meaningful choices, about what data are being collected about them and how the data are being used. As the augmented reality market evolves, I ask that you provide greater clarity on how Niantic is addressing issues of user privacy and security, particularly that of its younger players."

Others also expressed concerns over the types of data that Niantic was collecting from children. In a July 19 letter to Niantic, Common Sense, an independent non-profit organization that focuses on issues involving children's use of media, asked the company to clarify its privacy policies and practices related to *Pokémon Go*. "Parents must be the ones who decide which games their children play and what is acceptable use of their data — decisions parents cannot make when privacy policies are vague and business models profit off players in multiple, and often opaque, ways, such as via confusing in-app purchases and targeted ads seamlessly incorporated into a game," Common Sense founder and CEO James P. Steyer wrote in the letter. "Niantic, and other app developers, need to make it easy for parents to understand what apps do, how game play works, and how data is collected and shared."

"[Common Sense urges you to] enable users, particularly parents acting on behalf of their kids, to easily opt-out of information sharing that is not integral to the game," Steyer added. "For example, the Children's Online Privacy Protection Act (COPPA) requires that parents have the option to prevent sharing of their children's personal information with third parties. This is an essential protection for children, who should not have a marketing profile built on them as the price of playing a game."

On July 22, 2016, the Electronic Privacy Information Center (EPIC) called on the Federal Trade Commission (FTC) to investigate Niantic's data privacy practices. "When Niantic released Pokemon GO, the company

Pokémon, *continued on page 32*

Pokémon, *continued from page 31*

granted itself 'full access' to the accounts of users who signed up for the game with a Google account," EPIC wrote in a letter to FTC Chairwoman Edith Ramirez. "At no time did Niantic request user permission for full access to Google accounts; users simply logged in to the app via their Google account without receiving any additional information about what will be accessed. During this time, all users' full accounts were at risk of hacking and data breach. The FTC has previously found similar practices to be unfair or deceptive."

"Niantic's unlimited collection and indefinite retention of location data violate the data minimization requirements under the Children's Online Privacy Protection Act (COPPA), which requires providers to 'retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which information was collected.' Niantic does not disclose how long location information is retained or what purpose this retention fulfills," EPIC added. "The Pokemon GO app raises complex and novel privacy issues that require close FTC scrutiny. Niantic's disappointing history with respect to consumer privacy further underscores the need for FTC oversight. The FTC should (1) investigate whether Niantic's data collection and retention practices are consistent with [Fair Information Practices (FIPs)]; (2) prohibit Niantic's policies that are inconsistent with FIPs as unfair or deceptive trade practices; and (3) investigate Niantic's ongoing COPPA violations." As the *Bulletin* went to press, the FTC had not publicly responded to EPIC's requests.

Overseas, Niantic faced various challenges over data privacy and security practices related to *Pokémon Go*. On July 13, the National Society for the Prevention of Cruelty to Children (NSPCC), a UK charitable organization dedicated to child protection, called on Niantic to further delay the release of *Pokémon Go* in the UK, which had been halted due to server-related issues, so that the company could address privacy concerns. "Given Pokémon's already massive popularity with children, the NSPCC is concerned that basic safety standards appear to have been overlooked. . . . I urge you to urgently reassess your app and its security and safety features," NSPCC CEO Peter Wanless wrote in a letter to Nintendo UK, which maintains ownership rights over the Pokémon brand. "We all have a responsibility to ensure that children are protected and as creators of a game with substantive reach, you have a weighty responsibility to protect your young users. . . . I'm asking you to use this opportunity to reassess [Pokémon Go's] safety and ensure you have security and reporting functions which will still allow children to play but, crucially keep them safe when they do." Niantic released Pokémon Go in the United Kingdom the following day despite the NSPCC's concerns.

On July 20, *Fortune* reported that the Federation of German Consumer Organizations (VZBZ) threatened to sue Niantic under Germany's privacy and consumer protection law if the company did not amend 15 clauses in Pokémon Go's terms of service and privacy policy. VZBZ was particularly concerned with provisions in which Niantic claimed that it had the right to share users' data with third parties. "We think there is not a high enough level of consent in the use of data — these extended rights of giving users' data away to third parties in circumstances, which are not sufficiently described," VZBZ legal policy officer Heiko Dünkel told *Fortune* in an interview.

The German consumer group said that Niantic's claims that it could revise its terms of service at any time as well as the fact the policies' language was difficult for ordinary citizens to comprehend violated Germany's consumer protection law. VZBZ gave Niantic until August 9 to comply with its requests. If Niantic failed to do so, the group said it would file a cease-and-desist letter in German court. On August 17, VZBZ updated an earlier press release, stating that it had been in contact with Niantic attorneys to discuss privacy concerns. The consumer group said it would delay any legal action until its correspondence with Niantic was completed.

On Aug. 9, 2016, the Ireland's Office of the Data Protection Commissioner published detailed guidance for individuals and organizations about Irish law related to the collection of locational data from mobile apps and other types of online technology. Bloomberg BNA reported that the Commissioner's Office issued the guidance in response to the popularity of *Pokémon Go*. The office's guidance for individuals included: being aware that mobile apps, websites, and public Wi-Fi networks may collect location data when in use; becoming familiar with mobile phone settings that let users manage the types and amount of data that can be collected form the phone; learning about personal rights related to data processing; and being aware that companies must typically ask for consent prior to collecting and using personal data. The Data Protection Commissioner's Office guidance also reminded organizations that: locational data is likely to identify individuals and is therefore considered person data under Irish data protection laws; data controllers are required to minimize the amount of personal data that they collect, process, and retain; and informed consent is necessary to obtain prior to collecting data in order to comply with the law.

In a press release accompanying the documents, the Irish Data Protection Commissioner's Office explained that the guidance it was providing would help individuals' protect their rights. "Location data is any information which links an individual to a particular place including information about where a person currently is, or where they were at some point in the past. Technology such as smart phones has made it easier than ever before for individuals to be located. Organisations use this data to offer personalised services, such as navigation apps or location-specific news content on websites," the office wrote in the press release. "Aimed at both individuals and organisations, our guidance will assist individuals in understanding how information relating to their location is collected and processed, and provides clarity to organisations on their obligations regarding such data. The overriding principle of the guidance centres on the protection of the individual's right to data privacy."

Casey Carmody
Silha *Bulletin* Editor

Department of Defense Revises Law of War Manual after Criticisms from Journalistic Community

When the Department of Defense (DoD) issued its new "Law of War Manual" (Manual) in June 2015, several news organizations and press advocacy groups quickly criticized the way the manual defined "journalists" and "newsgathering activities," and called on the government to make revisions to the text. Among the concerns with the first version of the Manual were passages suggesting that journalists could be considered "unprivileged belligerents," meaning hostile individuals that did not qualify for combatant immunities or a "prisoner of war" status and could be detained indefinitely; that if a journalist disclosed information about combat operations, military officials would have the authority to consider that the journalist was "taking a direct part in hostilities"; advising journalists to carry "appropriate identification" to protect them from being viewed as spies; and that journalists' work might be subject to prior review by military officials. These descriptions and definitions prompted significant criticism from the journalistic community, which argued that several sections of the Manual could create dangerous situations for reporters covering wartime operations. (See "Department of Defense's New Law of War Manual Brings Calls for Revisions from Journalistic Community" in the Fall 2015 issue of the Silha *Bulletin*.)

NEWSGATHERING

In response to the criticisms, the DoD announced in a July 22, 2016 press release that it had made "substantial revisions" to its sections regarding reporters and journalistic activity. The press release explained that the DoD had worked with several journalists and press advocacy groups to make the changes. In a July 22 post on its website, the Committee to Protect Journalists (CPJ), one of the groups that the DoD consulted, wrote that the changes included: the inclusion of statements describing the important role that journalists play in covering combat operations; clarifications that engaging in newsgathering does not constitute taking part in direct hostilities, which would have removed military members' obligations to provide protection; and an explanation that military members needed to make an effort to "distinguish between the activities of journalists and the activities of enemy forces" so that journalists are not mistaken for combatants. *The Huffington Post* reported on July 22 that the DoD also removed passages that compared newsgathering to spying, as well as suggestions that journalists should seek permission from "relevant authorities" prior to gathering information.

However, Section 4.24.2.2 of the Manual continues to restrict other types of journalistic activities, noting that journalists have no special right to enter "areas of military operations without the consent of the State conducting those operations." The same section explained that security measures may also be taken to "reduce the risk of disclosure of sensitive military information, including numbers of military personnel, types of on-hand equipment, unit locations, and plans for future operations." Additionally, the *Christian Science Monitor* reported on July 22 that journalists could still be considered "unprivileged belligerents" if they are part of "non-state armed groups" carrying out propaganda or other media activities. The *Christian Science Monitor* noted that this phrasing left significant room for varying interpretations. The updated version of the Manual is available at http://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf.

The CPJ praised the updates to the Manual in its July 22 post. "The new language is a seismic shift for the U.S. military. This affirmation of journalists' right to report armed conflicts freely and from all sides is especially welcome at a time when governments, militias, and insurgent forces around the world are routinely flouting the laws of war," CPJ Senior Adviser for Journalist Security Frank Smyth said, according to the CPJ post. "The Law of War Manual's original language would have risked more journalistic imprisonments by putting most of the burden on the journalist to avoid behavior that could be construed as a hostile act. The revised language seems to put more of the burden on military commanders to distinguish between the journalistic and enemy activities."

In a July 22 press release on its website, Reporters Without Borders (RSF), another organization the DoD consulted during the revision process, stated that it was pleased to learn that provisions referring to spying and censorship had been removed. In Section 4.24.1, the revised version clarifies the international legal principle that journalists, particularly those who are embedded with U.S. military forces, are protected as civilians under the law of war, stating, "Journalists do not form a distinct class of persons under the law of war, but instead receive protection through the general protections afforded civilians." RSF U.S. Director Delphine Halgand said the clarification would provide greater protections for journalists. "We welcome today's revisions to the Law of War Manual and that the DOD for addressing RSF's concerns," said Halgand in the press release. "We hope that this update will help to improve the safety of journalists covering conflict, a profession that becomes increasingly dangerous every day."

In the government's July 22 press release, DoD General Counsel Jennifer O'Connor said that the revisions should clarify the military's approach to working with journalists covering combat operations. "After the manual's release last year, DoD lawyers heard concerns brought forward by media organizations and engaged in a productive, thoughtful dialogue with journalists that helped us improve the manual and communicate more clearly the department's support for the protection of journalists under the law of war," O'Connor said. "The department's mission is to defend the very freedoms that journalists exercise. We have learned a lot during this process, and the department and the manual are better off for the experience." The *Christian Science Monitor* also reported on July 22 that DoD officials said that they were open to further revisions to the Manual in the future, if necessary.

Elaine Hargrove
Silha Center Staff

State Legislatures, Courts Consider Media Law Issues

During the summer of 2016, several states confronted legal questions that raised important issues for media law policy within their jurisdictions. The issues included Minnesota lawmakers considering a bill that would establish protections for individuals' likenesses, the Minnesota Court of Appeals ruling that a statute criminalizing "grooming" was unconstitutional, and states adopting laws outlining procedures for police body camera footage.

STATE LAW UPDATES

Minnesota Lawmakers pulls the PRINCE Act Amidst Opposition

In the wake of the April 2016 death of Minnesota-based recording artist Prince, Minnesota Rep. Joe Hoppe (R-Chaska) introduced the Personal Rights in Names Can Endure Act (PRINCE Act), H.F. 3994, on May 9, 2016 that would have created a property right in a person's name, voice, image, or likeness for up to 50 years after they die. CNN Money reported on May 10 that the law would have established a property right for all citizens, not just celebrities. However, the Minneapolis *Star Tribune* reported on May 19 that Rep. Hoppe elected to withdraw the bill in response to widespread concerns over its language.

On April 21, 2016, *The New York Times* reported that Prince Rogers Nelson, better known simply as Prince, was found dead in an elevator at Paisley Park, his home and recording studio in Chanhassen, Minn. He died without a will, a spouse, or any children to name as heirs, according to the *Times*. On April 21, *Spin* magazine reported that besides the value of his name alone, Prince also left a vault of unreleased music. The *Star Tribune* also reported on May 18 that representatives handling Prince's estate were concerned about others profiting off of Prince, including through unauthorized T-shirts with his image.

In response to all of these concerns, Rep. Hoppe, whose legislative district includes Paisley Park, introduced the PRINCE Act on May 9, near the end of Minnesota's 2016 legislative session. In a May 9 interview with Minnesota Public Radio (MPR), Rep. Hoppe said that the bill was intended "to recognize the right of publicity postmortem." More specifically, the bill would grant celebrities greater leverage to restrict the unauthorized use of their likeness. According to a May 16 story by *MinnPost*, the bill would create a statutory property right "in a person's name, voice, signature, photograph, or likeness." Under the bill, that right is automatically passed on to heirs for a minimum of 50 years, and for an indefinite period afterwards so long as the heirs continue to enforce that right.

In a May 9 interview with MPR, Joel Leviton, the Bremer Trust attorney appointed to oversee Prince's estate, was a vocal supporter of the PRINCE Act. "We're talking about your name, we're talking about your image, we're talking about a photograph of you," Leviton said. "We're talking about anything that identifies you." In a May 9 interview with CBS-affiliate WCCO, Sen. Bobby Joe Champion (DFL-Minneapolis), who introduced the PRINCE Act in the Minnesota Senate, said that the bill was needed to help give artists greater control over their images. "We just wanted to make sure that that property right was created and that the heirs and estates would have control over any commercial exploitation or any usages of it," Sen. Champion said.

> "The way it's written, the law is broad enough to drive a truck through. If someone wants to throw a Prince dance party, they can expect a cease and desist letter from an attorney."
>
> **— Attorney Blake Iverson**

However, others were critical of the language of the PRINCE Act. Minneapolis attorney Blake Iverson told *MinnPost* on May 16 that he was troubled by a provision in the bill that allowed litigants, if successful, to collect attorney fees from anyone found liable for infringement. "This law is essentially a cash grab for attorneys," he told *MinnPost*. Iverson was also concerned at what the law would cover, such as any purple coat, which was one of Prince's signature looks. "The way it's written, the law is broad enough to drive a truck through," said Iverson. "If someone wants to throw a Prince dance party, they can expect a cease and desist letter from an attorney."

In May 11 op-ed for the *Star Tribune*, University of Minnesota Professor of Law William McGeveran argued that the bill conflicted with the First Amendment. "As first drafted, currently written, the PRINCE Act contained a very narrow, limited free-speech exception for news, public affairs and sports reports. When critics like me immediately pointed out that this narrow rule probably violated the First Amendment, the bill was changed to add a laundry list of other types of art and commentary," McGeveran wrote. "These 11th-hour additions are based on old media and do not mention, for example, video games or websites. There has been no time to consider what else might have been overlooked. Moreover, even the improved PRINCE Act still would require case-by-case adjudication in court, which would be an expensive and difficult undertaking for any artist or author defendant sued by the celebrity's estate. And celebrities and their heirs can threaten suit whenever they choose. That prospect would scare many people away from exercising legitimate speech rights in the first place."

In the May 16 *MinnPost* story, Director of the Silha Center and Professor of Media Ethics and Law at the University of Minnesota Jane Kirtley argued that the act was largely unnecessary. "Existing intellectual property law would most likely address most of the legitimate concerns about Prince," Kirtley said. *MinnPost* also reported that although Minnesota does not have a written law protecting a living person's right of publicity, federal courts had already held that Minnesota would recognize a right to publicity for living persons. If adopted, the PRINCE Act would have made Minnesota the sixteenth state with a state statute

that codified a common law protection of an individual's privacy into a form of intellectual property, according to *MinnPost*.

Kirtley also raised concerns over the fair use exceptions for media coverage and artistic representation. "Celebrities can and will use right of publicity laws to try to stop reporting about things that they want to keep secret, even if those things might arguably be matters of public interest," Kirtley told *MinnPost*. "A publisher may be embroiled in expensive litigation for years, and even if it wins in the end, will have lost a lot of money in the process. . . . Most users won't have those kinds of resources, so will be chilled from engaging in this kind of speech."

Although the Minnesota House of Representatives' Civil Law and Data Practices Committee approved the bill on May 12, 2016, Rep. Hoppe chose to withdraw the bill in order to consider the concerns raised by opponents over the bill's language, according to a May 18 *Star Tribune* story. Rep. Hoppe said he planned to rework the bill and intended to reintroduce it during Minnesota's 2017 legislative session.

Minnesota Court of Appeals Finds Anti-Grooming Law Unconstitutional

On June 20, 2016, the Minnesota Court of Appeals ruled that a statute preventing predators from luring children into sexual encounters online was unconstitutional. *Minnesota v. Muccio*, 881 N.W.2d 149 (Minn. App. 2016). The three-judge panel for the Minnesota Court of Appeals held that the law's language was unconstitutionally overbroad and had the potential to chill protected free speech. Attorneys for the state of Minnesota are considering an appeal to the Minnesota Supreme Court.

Enacted in 2007, Minnesota's "Solicitation of Children to Engage in Sexual Conduct; Communication of Sexually Explicit Materials to Children," criminalized the act of "grooming." Minn. Stat. § 609.352. Minnesota Public Radio (MPR) reported on June 20, 2016 that grooming involves sexual predators engaging in online conversations with children and exposing them to pornographic material in an attempt to acclimate the child towards a sexual encounter. Under Minnesota's anti-grooming statute, a person over the age of 18 who used the internet, phone, or computer system to solicit sex by "engaging in communication with a child or someone the person reasonably believes is a child, relating to or describing sexual conduct" was guilty of a felony. The statute defined a child as anyone who was age 15 or younger.

On June 20, 2016, the Minneapolis *Star Tribune* reported that the case at hand arose in November 2014 from online conversations between Krista Muccio, a 43-year-old Dakota County middle-school lunchroom assistant, and a 15-year-old student. The student's father found images depicting naked women and female genitals on his son's iPad and reported it to law enforcement authorities. Upon investigation, law enforcement officials discovered that the pictures originated from Muccio's Instagram account and were sent to the student via direct message. When police executed a search warrant, they found that Muccio and the student had held sexually explicit conversations and exchanged explicit photographs through social media accounts, according to the *Star Tribune*.

> "[Although] the statute's aim is laudable, the law is unconstitutionally overbroad because the 'restriction goes well beyond that interest by restricting the speech available to law-abiding adults.'"
>
> **— Judge Peter M. Reyes, Minnesota Court of Appeals**

In April 2015, prosecutors brought charges against Muccio in the District Court for Dakota County, alleging one count of felony communication with a minor describing sexual conduct in violation of Minnesota's anti-grooming statute and another count for possessing pornographic work involving a minor in violation of the state's child pornography statute. Muccio then filed a motion requesting that the trial judge dismiss the grooming charge, arguing that the statute was unconstitutional. The judge agreed and dismissed the charge, ruling that the law was facially overbroad and violated the First Amendment's protections of free expression. State prosecutors then appealed the district court's decision to the Minnesota Court of Appeals.

On June 20, 2016, a three-judge panel for the Minnesota Court of Appeals upheld the lower court's ruling, finding that parts of the state's anti-grooming were "facially overbroad in violation of the First Amendment because it prohibits a substantial amount of protected speech." In writing for the unanimous panel, Judge Peter M. Reyes' opinion focused on the wording in Subdivision 2a(2) of the statute, which stated "A person 18 years of age or older who uses the Internet, a computer, computer program, computer network, computer system, an electronic communications system, or a telecommunications, wire, or radio communications system, or other electronic device capable of electronic data storage or transmission to commit any of the following acts, with the intent to arouse the sexual desire of any person, is guilty of a felony . . . : engaging in communication with a child or someone the person reasonably believes is a child, relating to or describing sexual conduct." Minn. Stat. § 609.352, subd. 2a(2). In particular, the panel criticized the wording "arouse the sexual desire of any person." Judge Reyes wrote that the language potentially risked criminalizing protected speech between two adults who have a right to engage in sexually arousing interactions online. In other words, the court determined that the statute could criminalize any situation in which an adult wished to "arouse the sexual desire of any person" in an online conversation, not just in the case of conversations with children, said Director of the Silha Center and Professor of Media Ethics and Law at the University of Minnesota Jane Kirtley in an interview with the *Star Tribune* on June 20.

The court also focused on the wording "engaging in communication . . . relating to or describing sexual conduct" within the statute. The court acknowledged that speech directly related to criminal conduct was not entitled to First Amendment protections. However, Judge Reyes

State Law, *continued on page 36*

State Law, *continued from page 35*

wrote that the anti-grooming statute criminalized speech that was not "integral to criminal conduct." Instead, the statute criminalized speech that was "one step removed" from conduct because the type of speech that the statute prohibits "precedes the solicitation of criminal sexual conduct by sexual predators," meaning that there was not an absolute guarantee that criminal activity would follow such speech.

The panel also found that the statute was unconstitutionally overbroad because it had the potential to criminalize protected speech. Judge Reyes gave one example of a "music video producer [who] creates a video with sexually explicit depictions or lyrics, with the intent to arouse the sexual desire of some person who views or listens to the video, places that video on social media, and a child age 15 or younger sees or hears it." The court concluded that this act, among others protected by the First Amendment, would be criminalized under the statute. The appellate court also dismissed the state's arguments that the statute could be narrowly construed in order to prevent it from being struck down because it would require the appellate court to add language not already included in the statute. Finally, Judge Reyes rejected the state's arguments that the statute was a constitutional content-based regulation, finding that the statute was not sufficiently narrowly tailored to serve the state's compelling interest in protecting children. Judge Reyes wrote that although "the statute's aim is laudable, the law is unconstitutionally overbroad because the 'restriction goes well beyond that interest by restricting the speech available to law-abiding adults.'"

John Westrick, who represented the Muccio in the case, applauded the decision. "The Legislature tries to criminalize conduct before it's criminal," Westrick told the *Star Tribune* on June 20. "I understand [the state's] desire to protect the children, I really do. But prosecutors need to show intent to commit a crime. It doesn't fly in this case. . . . I believe the public is the winner with this ruling." Kirtley also told the *Star Tribune* that the appellate court's decision would have a major impact on Minnesota law because the opinion clearly stated that it was permissible for individuals to engage in speech that could potentially sexually arouse someone else, even if that person might be a child. Kirtley noted that the statute's definitions of criminal conduct were overly broad, thus making the statute unconstitutional.

The *Star Tribune* also reported that Dakota County Attorney James Backstrom, one of the attorneys representing the state in the case, said that the Minnesota Supreme Court should decide the constitutionality of the statute and that he planned to appeal the decision. State Sen. Ron Latz, (DFL-St. Louis Park), chairman of the Minnesota Senate Judiciary Committee, said that he had not read the ruling yet but was surprised that the appellate court couched its decision so deeply in First Amendment jurisprudence. He also acknowledged that laws regulating speech are difficult to draft. "There is always a gray area with legislation that tries to address potential criminal risk compared to actual harm," Sen. Latz said.

In July, state attorneys filed a petition for further review with the Minnesota Supreme Court. On Aug. 23, 2016, the Supreme Court granted the state's petition. As the *Bulletin* went to press, the Minnesota Supreme Court had not yet scheduled oral arguments.

Minnesota and North Carolina Governors Sign Police Body Camera Legislation

On May 31, 2016, Minnesota Gov. Mark Dayton signed SF 498, which established regulations for the use of police body camera technology within the state. The Minneapolis *Star Tribune* reported on May 31 that the Minnesota law requires that most footage captured by police body cameras would remain private. However, the law permits some body cam videos to be released to the public in situations when the camera captures altercations resulting in "substantial bodily harm" or when individuals depicted in the footage chooses to allow the video to be publicly available. Meanwhile in North Carolina, Gov. Pat McCrory signed a similar law, HB 972, on July 11, 2016, which allows law enforcement agencies to keep officer-worn body camera footage from the public unless ordered to release the footage by a court, according to a July 11 ACLU press release. Like Minnesota's statute, the North Carolina bill does not presume that body camera footage is publicly available under the law.

In February 2015, Sen. Ron Latz (DFL-St. Louis Park) introduced SF 498 in the Minnesota Senate, which aimed to establish uniform guidelines for how police departments within Minnesota must handle body camera footage because approximately 40 police departments were already using such devices, according to a May 24 Minnesota Public Radio (MPR) story. However, the bill was initially tabled during Minnesota's 2015 legislative session but was considered once again during the 2016 session.

In its final form, the bill contained several provisions on how police departments in Minnesota should handle officer body camera footage. Significantly, the bill classified all footage captured by body cameras as private or nonpublic data. The bill did include several circumstances in which the video could be made public, including footage capturing instances when police officers have fired their weapons during the course of their duties, when there is "the use of force by a peace officer that results in substantial bodily harm," or when a subject in the footage requests that it be made publicly accessible so long as an investigation involving the footage is complete. In situations when footage will be made publicly-available, anyone depicted in the video who is not a police officer can decide whether they want to be identifiable. If people do not want to be identified, they may elect to have their faces blurred and voices distorted in the video, according to a May 17 *City Pages* story. The *Star Tribune* reported on May 10 that police officers depicted in the video could also choose to redact their own images in situations when footage will be made public. Additionally, the bill allowed police to withhold footage that was "clearly offensive to common sensibilities," but does not define what that term means.

The bill also permitted individuals to pursue court actions to compel the disclosure of any body camera footage that a department retains. In such situations, individuals seeking the footage must notify the department retaining the footage, as well as the subjects depicted in the videos, about the requests for public disclosure. State district courts have the authority to determine whether the footage

in question should be released in its entirety or only in part. When considering whether to make footage publicly available, the bill required judges to consider whether the benefit of releasing the footage outweighed any harm of making the footage public. The bill also mandated that judges view the footage in private before making a decision.

The bill required police departments that use body cameras to post a written policy that governs the departments' use of such technology on their website. Police departments must solicit comments on their policies from the public before any equipment is purchased or used within a department. *City Pages* reported that the bill would permit police departments to create their own rules about when the cameras would need to be capturing footage, what consequences officers would face for violating department policies, and designating the department officials tasked with collecting, withholding, and editing the footage.

Throughout the course of the legislative process, the bill was the subject of extensive lobbying efforts by both government transparency advocates and law enforcement officials. Open government advocates argued that the bill's provisions were too favorable to law enforcement officials because of the presumption that camera footage was private. During a May 10 House Civil Law and Data Practices Committee hearing on the bill, Minneapolis City Council Member Linea Palmisano expressed concerns that the footage from the cameras will not be used properly and that the city was not equipped to deal with public data requests. "I want this data to be usable," said Palmisano, according to a May 10 *Star Tribune* story. "If we aren't managing the data from a body camera program and making it accessible, it's of zero worth. And I think we are about to get snowed [under] in terms of how we might catalog this type of data and be able to go and access it."

During the same hearing, National Association for the Advancement of Colored People (NAACP) Minneapolis Chapter President Nekima Levy-Pounds expressed concerns over provisions in the bill that would have permitted offices to review footage prior to filing official incident reports and that more time should be taken to consider the bill. "It weighs too heavily in favor of the perspective of law enforcement at a time in which trust by the African-American communities and other communities of color in law enforcement is at an all-time low," she said, according to the *Star Tribune*. "At the end of the day, it's more important to take the time and do this right than to hastily enact legislation that is going to cause more harm than good." The clause allowing officers to review footage prior to submitting incident reports was later removed by the legislature after Gov. Dayton said he would not sign a bill containing such a provision.

> "[Minnesota's police body camera bill] weighs too heavily in favor of the perspective of law enforcement at a time in which trust by the African-American communities and other communities of color in law enforcement is at an all-time low. At the end of the day, it's more important to take the time and do this right than to hastily enact legislation that is going to cause more harm than good."
>
> **— Nekima Levy-Pounds, President, the Minneapolis Chapter, NAACP**

Despite the significant opposition during the May 10 hearing, the committee chose to adopt the bill on an 11 to 2 vote, with many observers suggesting that the overwhelming support stemmed from law enforcement officials' significant lobbying efforts related to the bill. In a May 10 interview with the *Star Tribune*, Minnesota Police and Peace Officers Association Executive Dennis Flaherty acknowledged the role of law enforcement lobbying in the legislative process. "We try to develop relationships with lawmakers from both sides of the aisle, and I think we're fortunate in that most of the legislators want to certainly hear our message," said Flaherty. Ben Feist, a lobbyist for the American Civil Liberties Union (ACLU) of Minnesota, also noted that police groups have a "tremendous amount of influence" in most of the legislation his organization views as important.

The Minnesota Senate adopted the police body camera bill on May 2, 2016 on a 47 to 14 vote before it moved to consideration in the Minnesota House. The House adopted the bill on May 16 on a 95 to 33 vote with an amendment that removed the provision allowing officers to review footage prior to submitting incident reports. As a result, the House and Senate held a conference committee to reconcile the Senate bill and amended House bill. Upon reaching a compromise, both the Minnesota Senate and House voted to pass the bill on May 21. Gov. Dayton signed the bill on May 31, 2016.

Upon the governor's signature, Sen. Latz said that, despite transparency advocates' criticisms, the bill was a success because it favored individuals' privacy. "Community organizations look at the big picture, but that may conflict with the agenda of an individual who is on a recording," Sen. Latz told the St. Paul *Pioneer Press* in a May 31 interview. "I'd rather leave it in the hands of the individual." However, NAACP President of St. Paul Jeff Martin said that the bill ultimately focused more on law enforcement interests rather than police accountability, which should have been the focus of the bill. "We seem to have forgotten what led us to this point," Martin told the *Pioneer Press* in the same story. "If our opinion doesn't count, then let's get ready for the real fight, which will be in court."

Others also agreed that the negotiations over the use of police body cameras were not settled upon Gov. Dayton's decision to sign the bill. In a May 31 interview with MPR, Rep. Dan Schoen (DFL-St. Paul Park) said that he expected that amendments to the law would be introduced during Minnesota's next legislative session. "This is a conversation we should continue to have," Schoen said. "[The law as it is now is] going to make it very possible for any law enforcement agency that wants to adopt body

State Law, *continued on page 38*

State Law, *continued from page 37*

cameras to go ahead and do so. That's the most important achievement here."

Meanwhile in North Carolina, Gov. Pat McCrory signed HB 972 on July 11, 2016, which created legal distinctions for different types of footage captured by law enforcement officers. On July 12, the *Christian Science Monitor* reported that under the law, both body camera footage and dash camera footage are not considered part of the public record. Instead, law enforcement agencies have the discretion whether to disclose the footage to people who were recorded, according to an ACLU of North Carolina July 11 press release. *The Huffington Post* reported on July 14 that Gov. McCrory may have been motivated to sign the bill in response to a series of police-involved shootings throughout the United States during 2016.

CNN reported on July 13 that under the newly enacted law, North Carolina police departments could consider withholding law enforcement-captured footage from the public if such a disclosure would reveal information of a "highly sensitive personal nature"; if the disclosure "may harm the reputation or jeopardize the safety of a person"; if disclosure would create "a serious threat to the fair, impartial, and orderly administration of justice"; or if withholding release was necessary to protect an active or inactive investigation, criminal or internal.

According to July 1 *PolitiFact* story, the bill differentiates between the "disclosure" and the "release" of body camera footage. The "disclosure" of footage is only available to the people seen or heard in the video. These individuals are allowed to watch the video, but cannot show it to the general public or make any copies. However, they are not guaranteed the ability to see the footage because it is still up to law enforcement to decide whether to disclose the video. For example, police agencies can withhold the footage if they feel it requires so much secrecy that even the people in the footage cannot see it, according to *PolitiFact*.

The "release" of body camera videos meant that the footage would be made available to the general public. Under the law, individuals, including reporters, who believe that body camera footage should be publicly released would be required to seek a court order compelling disclosure of the footage. Individuals would also need to petition a court in situations when law enforcement officials deny requests for footage in "disclosure" situations. Prior to any footage being released, local district attorneys, the head of the agency that captured the video, and any officer whose image is seen or voice is heard in a video must be notified that footage may be publicly released and must be given the opportunity to testify about the footage in court, according to *Politifact*.

Upon signing the bill, Gov. McCrory said the new law established new standards that would promote "uniformity, clarity and transparency" for law enforcement recordings within North Carolina. However, government transparency advocates criticized several of the new law's provisions. In a July 1 interview with *Politifact*, Raleigh-based public records attorney Mike Tadych explained that the law created significant barriers for individuals who want to make law enforcement footage publicly available. Tadych argued that the law maintains that judges are allowed to release only footage that has been specifically described during court proceedings. The attorney argued that such a task would be difficult when no one in the public would have been able to see the video before it was released. "I don't know how in the world, without knowing what's on it, you would be able to say you know what's on it," Tadych said.

In a July 11 press release, Susanna Birdsong, Policy Counsel for the ACLU of North Carolina also criticized the law because of the difficult steps needed to be taken in order to make body camera footage publicly available. "Body cameras should be a tool to make law enforcement more transparent and accountable to the communities they serve, but this shameful law will make it nearly impossible to achieve those goals," said Birdsong, in the press release. "People who are filmed by police body cameras should not have to spend time and money to go to court in order to see that footage. These barriers are significant and we expect them to drastically reduce any potential this technology had to make law enforcement more accountable to community members."

The North Carolina law will go into effect on Oct. 1, 2016.

Scott Memmel
Silha Research Assistant

Free Expression Controversies on College Campuses to be Topic of 31st Annual Silha Lecture

From "culturally offensive" Halloween costumes to protests over controversial speakers to "trigger warnings" in classrooms, debate over freedom of expression only seems new to America's college campuses. These and similar issues have roiled higher education for decades. Randall L. Kennedy, the Michael R. Klein Professor of Law at Harvard Law School, will revisit key disputes that are likely to continue to challenge First Amendment principles when he presents "The Politics and Law of the Culture Wars in American Higher Education, 1950-2020" at the 31st Annual Silha Lecture on Oct. 3, 2016.

SILHA CENTER EVENTS

During the past year, free expression advocates have found themselves in conflict with civil rights and student protestors on college campuses across the United States. In Connecticut, a campus newspaper faced the loss of student funding in October 2015 after printing a controversial op-ed criticizing the protest tactics of Black Lives Matter, an organization dedicated to drawing attention to and combatting institutional racism against black individuals in the United States. Black Lives Matter supporters argued that the campus newspaper had perpetuated racism on campus. In a separate November 2015 incident, activists who were protesting the University of Missouri administration's handling of several racist incidents at the institution blocked a student photographer on assignment for a national news organization from taking pictures at a makeshift tent encampment on the campus quad. The activists claimed that the student photographer was violating a "safe space" free from journalists despite the encampment being in a public location. (For more on these conflicts between protestors and the press, see "Journalists, Newspapers Clash with Activists on College Campuses, Raising First Amendment Issues" in the Fall 2015 issue of the Silha *Bulletin*.)

In a Nov. 27, 2015 op-ed essay for *The New York Times* titled "Black Tape at Harvard Law," Professor Kennedy argued that activists should fully consider outcomes when presenting legitimate claims of victimhood. In particular, Professor Kennedy responded to activists who argued that when vandals defaced photographs of African-American law school professors by placing black tape over their faces, it constituted a "racial hate crime." He wrote that although the taping was disturbing to many, the motive of those who vandalized the photos was unclear. Although acknowledging that the action may have been racist, he argued that "there is a need to calibrate carefully its significance." Noting that incidents like the one at Harvard Law inspired "difficult but earnest and probing conversations," he suggested that "in the long run, reformers harm themselves by nurturing an inflated sense of victimization." The complete essay is available at http://www.nytimes.com/2015/11/27/opinion/black-tape-at-harvard-law.html.

The author of numerous books and articles, Professor Kennedy is uniquely qualified to discuss race relations in the United States. His books include *For Discrimination: Race, Affirmative Action, and the Law* (2013), *The Persistence of the Color Line: Racial Politics and the Obama Presidency* (2011), *Sellout: The Politics of Racial Betrayal* (2008); *Interracial Intimacies: Sex, Marriage, Identity, and Adoption* (2003), and *Nigger: The Strange Career of a Troublesome Word* (2002). In 1998, he was awarded the 1998 Robert F. Kennedy Book Award for *Race, Crime and the Law*.

Professor Kennedy attended Princeton University, Oxford University, and Yale Law School, followed by clerkships with Judge J. Skelly Wright of the United States Court of Appeals for the District of Columbia Circuit and with United States Supreme Court Justice Thurgood Marshall. He is also a member of the American Law Institute, the American Academy of Arts and Sciences, and the American Philosophical Society. Professor Kennedy currently teaches courses on civil rights and civil liberties, Constitutional law, and race and law at Harvard.

The 31st Annual Lecture begins at 7:30 pm at Cowles Auditorium in the Hubert H. Humphrey Center on the West Bank of the University of Minnesota Twin Cities campus. A selection of Professor Kennedy's books will be available for sale, with a book signing following the Lecture. The Silha Lecture is free and open to the public. No reservations or tickets are required. Parking is available in the 19th and 21st Avenue ramps. Additional information about directions and parking can be found at www.umn.edu/pts.

The Silha Center for the Study of Media Ethics and Law is based at the School of Journalism and Mass Communication at the University of Minnesota. Silha Center activities, including the annual Lecture, are made possible by a generous endowment from the late Otto Silha and his wife, Helen.

Silha Center Staff

Silha Center for the Study of Media Ethics and Law
School of Journalism and Mass Communication
University of Minnesota
111 Murphy Hall
206 Church Street SE
Minneapolis, MN 55455
(612) 625-3421

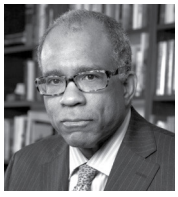
Non-profit Org.
U.S. Postage
PAID
Twin Cities, MN
Permit No. 90155

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

The Politics and Law of the Culture Wars in American Higher Education, 1950-2020

PROFESSOR RANDALL KENNEDY, HARVARD LAW SCHOOL

From "culturally offensive" Halloween costumes to protests over controversial speakers to "trigger warnings" in classrooms, debate over freedom of expression only *seems* new to America's college campuses. These and similar issues have roiled higher education for decades. Randall Kennedy will revisit key disputes that are likely to continue to challenge First Amendment principles.



Randall Kennedy is Professor of Law at Harvard Law School. He attended Princeton University and Yale Law School. He clerked for Judge J. Skelly Wright and Justice Thurgood Marshall. His most recent books are *The Persistence of the Color Line: Racial Politics and the Obama Presidency* and *For Discrimination: Race, Affirmative Action, and the Law.* He is a member of the American Law Institute, the American Academy of Arts and Sciences, and the American Philosophical Society.

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

31ST ANNUAL SILHA LECTURE

- MONDAY, OCTOBER 3, 2016
- 7:30PM
- COWLES AUDITORIUM
  HUBERT H. HUMPHREY SCHOOL
  OF PUBLIC AFFAIRS
  UNIVERSITY OF MINNESOTA
  WEST BANK
- FREE & OPEN TO THE PUBLIC;
  NO RESERVATIONS NEEDED

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW

SCHOOL OF JOURNALISM
& MASS COMMUNICATION
COLLEGE OF LIBERAL ARTS
UNIVERSITY OF MINNESOTA