Debates Continue Over Net Neutrality as FCC Nears Decision on an “Open Internet”

During the summer and fall of 2014, federal policymakers and regulators continued to debate the role of “net neutrality” in managing Internet communication. The principle of net neutrality is based on the idea that the government should require Internet service providers (ISPs) to treat all Internet traffic the same. Net neutrality principles prevent ISPs from speeding up, slowing down, or blocking the delivery of lawful Internet data based on type of content, financial arrangements, users, or web sites. In the United States, the rules for net neutrality stemmed from a 2010 Federal Communications Commission (FCC) order, In re Preserving the Open Internet, 25 F.C.C.R. 17905 (2010). The order had several provisions, including mandates for ISPs to affirmatively disclose information about Internet speed, terms of use, and management practices; anti-blocking measures that prohibited ISPs from preventing consumers from receiving lawful Internet content except for reasonable management reasons; and anti-discrimination rules, which prevented ISPs from speeding up the delivery of certain Internet content. The FCC has also previously stated that its “Open Internet” order would ban “pay for priority” arrangements, which the Commission said would limit Internet openness by allowing large content providers like Google and Netflix to pay ISPs for quicker delivery of content.

However, in January 2014, the U.S. Court of Appeals for the D.C. Circuit struck down the anti-blocking and anti-discrimination provisions of the FCC’s “Open Internet” order. Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014). A three-judge panel held that although the FCC could regulate Internet service providers, the Commission had exceeded its statutory authority with its 2010 order. Specifically, the FCC had previously classified broadband service providers as “information service providers” rather than “telecommunication carriers” for the purposes of regulation. As a result, the court held that the FCC could not impose several of the common carrier requirements for “telecommunication carriers” under Title II of the Telecommunications Act onto the broadband Internet service providers. After the appellate court’s decision, FCC Chairman Tom Wheeler, who was appointed by President Barack Obama in 2013, said that the Commission would not seek to appeal the decision but would promote net neutrality through other means. (For more on the court of appeals decision and early reaction to the decision, see “D.C. Circuit Strikes Down FCC ‘Net Neutrality’ Rules” in the Winter/Spring 2014 issue of the Silha Bulletin.)

FCC Proposes New “Open Internet” Rules

On May 15, 2014, The New York Times reported that the FCC had voted 3-2 to seek public comment on newly-proposed Open Internet rules. Protecting and Promoting the Open Internet, GN Docket No.14-28, 29 FCC Rcd 5561 (2014). The FCC’s proposed rules would allow content providers, such as Facebook or Netflix, to pay ISPs for guaranteed “fast lane” service to deliver content more rapidly to Internet subscribers. The rules also prohibited ISPs from knowingly slowing down the delivery of data from content providers who declined to pay for upgraded service. The Times reported that the FCC’s proposed Open Internet rules contained provisions that would prohibit ISPs from blocking lawful web content, require ISPs to explain to consumers how web traffic is managed, and create an ombudsperson position who would act as an advocate on behalf of the public in discussions about Internet regulation. The proposal also sought comments on whether ISPs should be re-classified as “common carrier” under Title II of the Telecommunications Act, rather than “information service providers,” which would allow for greater regulation.

The vote to open the proposed rules to public comment passed along a party-line vote with the three Democratic-appointed commissioners voting in favor and the two Republican-appointed commissioners voting against the plan. Despite their support for seeking comment from the public, the two Democratic commissioners, Jessica Rosenworcel and Mignon Clyburn, suggested that the proposed rule could still be improved, the Times reported. “I support network neutrality,” said Rosenworcel, according to the Times. “But I believe the process that got us to this rule making today is flawed. I would have preferred a delay. I think we moved too fast, to be fair.”

In contrast, Republican Commissioner Michael O’Rielly argued that the proposed rule would exceed the FCC’s statutory authority. The premise for imposing net neutrality rules is fundamentally flawed and rests on a faulty foundation of make-believe statutory authority,” said O’Rielly. Republican Commissioner Ajit Pai suggested that Congress was better suited to making decisions about net neutrality. “A dispute this fundamental is not for us, five unelected individuals, to decide,” Pai said, according to the Times. “Instead, it should be resolved by the people’s elected representatives, those who choose the direction of government, and those whom the American people can hold accountable for that choice.”

FCC, continued on page 3
Inside This Issue

1  Debates Continue Over Net Neutrality as FCC Nears Decision on an “Open Internet”  
   Cover Story

6  “Drone Journalism” Presents Possibilities But Faces Legal Obstacles  
   Journalism Technology

9  Supreme Court Considers Whether Facebook Posts Can Constitute “True Threats”  
   Online Speech

11  Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberties  
   Press Freedom

13  Problems Continue for News Coverage of Ferguson Shooting after Grand Jury Decision  
   News Media Challenges

16  Federal Investigators’ Deceptive Use of Media Raises Concerns  
   Law Enforcement Conflicts

18  Dissemination of Hacked Online Photos Demonstrates Challenges of Digital Privacy  
   Privacy

20  Government Surveillance Critics Target Broad Authority of Executive Order 12333  
   National Security

21  Tenth Circuit Dismisses Claims That News Program Violated Broker’s Civil Rights, Allows Defamation Claims to Proceed  
   Defamation

24  Law Enforcement, Tech Companies Clash on Built-In Privacy Features  
   Privacy

25  29th Annual Silha Lecture Examines the Right to Access Government Information in the Wake of National Security and Privacy Concerns  
   Silha Center Events

27  Silha Center Co-Sponsors Forum on Ethics of “Pointergate”  
   Broadcast
   Silha Center Events

---

**Silha Center Staff**

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

**Casey Carmody**  
Silha Bulletin Editor

**Alex Vlisides**  
Silha Research Assistant

**Sarah Wiley**  
Silha Research Assistant

**Elaine Hargrove**  
Silha Center Staff
FCC, continued from page 1

The FCC’s May 15 vote did not create any binding rules related to Internet regulations. Rather, the vote immediately opened a time period for the public to comment on the FCC’s proposal, which was originally targeted to last until July 15. After the first deadline, the public then had until September 10 to file comments in response to initial discussions of the proposal. The Times reported that Chairman Wheeler specifically stated during the Commission’s hearing that the vote was seeking public comment. “We are dedicated to protecting and preserving an open Internet,” said Wheeler. “What we’re dealing with today is a proposal, not a final rule. We are asking for specific comment on different approaches to accomplish the same goal, an open Internet.”

FCC Receives Significant Response to Net Neutrality Proposal

During the comment period, The Washington Post’s Soraya Nadia McDonald reported on June 4 that the FCC had received more than 45,000 comments on June 2 alone, which crashed the FCC’s online commenting system. McDonald suggested that the surge in comments probably resulted from a June 1 commentary by comedian John Oliver on his show, “Last Week Tonight,” that airs on HBO. In his 13-minute commentary, Oliver gave net neutrality a comedic spin, but also encouraged viewers to submit comments in support of net neutrality rules on the FCC’s web site, which was displayed on the screen during the conclusion of the segment. The Post reported that the FCC was having trouble managing the amount of traffic it received the following day, with issues remaining unresolved until the early evening. The “Last Week Tonight” video can be seen at https://www.youtube.com/watch?v=fpbOEoRrHyU.

On June 18, Bloomberg BNA reported that Sen. Patrick Leahy (D-Vt.) and Rep. Doris Matsui (D-Calif.) introduced the Online Competition and Consumer Choice Act. The legislation would require the FCC to ban financial deals between ISPs and content providers that would allow for priority service of content delivery. The bill also would prohibit ISPs from prioritizing the traffic of their own content, applications, or services. “Americans are speaking loud and clear,” Sen. Leahy said in a June 17 statement. “They want an Internet that is a platform for free expression and innovation, where the best ideas and services can reach consumers based on merit rather than based on a financial relationship with a broadband provider.” The bill had three co-sponsors, including Rep. Henry Waxman (D-Calif.), Rep. Anna Eshoo (D-Calif.), and Sen. Al Franken (D-Minn.). No Republicans chose to co-sponsor the legislation. Congressional aides also told BNA that the bill should be viewed as a political message rather than legislation that would actually be enacted.

On July 15, The New York Times reported that the FCC had received approximately 780,000 comments from the public on the proposed rules prior to the initial comment deadline ranging from a single line of text to entire legal briefs on the proposed rules. Because of the number of comments, the FCC extended the initial deadline by three days. The Times also reported that a sample of the comments submitted to the FCC seemed heavily skewed toward preserving the principles of net neutrality. Many of the comments argued that the FCC’s proposed rules did not go far enough. The Times story also noted that the standard-form nature of many of the submissions indicated that several of the comments appeared to be from different interest groups’ popular “get-out-the-comments” advocacy efforts encouraging the public to participate in the debate.

Internet content providers and ISPs also provided comments to the FCC before the extended July deadline. The Times reported that the Internet Association, an industry group that represents technology and media companies with members including Netflix, Amazon, and Google, submitted comments suggesting that without new rules, ISPs would discriminate among different types of content. “Unlike consumers, broadband Internet access providers have a horse in the race — whether it is their affiliated content or which content provider will pay the most for the enhanced or prioritized access,” the Internet Association wrote. In contrast, AT&T’s comment argued that the government’s attempt at imposing new rules for the Internet was problematic, according to the Times. “In no other area of the economy does the government ban voluntary market transactions (here, for example, quality-of-service enhancements) specifically in order to prevent those with superior resources from offering better services to their own customers,” AT&T wrote in its submitted comments. On August 15, the FCC released a public notice extending the reply comment period from the originally scheduled deadline of September 10 to September 15.

On September 2, the Sunlight Foundation, a nonpartisan nonprofit advocating for open government, released a report on the content of about 800,000 public comments from the initial commenting period. Using an automated computer analysis, the organization determined that less than one percent of the comments were “clearly opposed to net neutrality.” The remaining 99 percent of comments advocated for the FCC to adopt net neutrality principles or did not take a definitive stance one way or the other. The Sunlight Foundation found that at least 60 percent of the comments were some type of form letter that commenters had used from an organized campaign. The Foundation noted that although form letters made up the majority of comments, “this is actually a lower percentage than is common for high-volume regulatory dockets,” which suggested that many individuals were making an effort to personalize their submitted comments. The organization also noted that at least 200 comments were from law firms working on behalf of their clients. The Sunshine Foundation’s report and the data it used for analysis can be found at http://sunlightfoundation.com/blog/2014/09/02/what-can-we-learn-from-800000-public-comments-on-the-fccs-net-neutrality-plan/.

Several large technology companies staged online protests on September 10, just days before the end of the second round of comments on the FCC’s proposed Internet rules. According to a September 10 article by online technology magazine The Verge, Netflix, Tumblr, and Kickstarter, among several others, displayed “spinning wheels” on their web sites. The wheels suggested that the web site was taking a long time to load, which the companies argued would be a regular occurrence if the FCC did not adopt net neutrality regulations. The protesting content
tent providers also provided information to web site users that encouraged them to submit a comment to the FCC or to contact their local congressperson.

On September 17, National Public Radio reported that at the close of the September 15 deadline, the FCC had received approximately 3.7 million comments on the proposed Open Internet rules. The number of comments for the proposed rules was greater than any other previous FCC rule proposal. The comments on net neutrality beat the previous record set by the public’s outcry after Janet Jackson’s “wardrobe malfunction” during the 2004 Super Bowl halftime show. The FCC received approximately 1.4 million messages from the public after the 2004 incident.

**FCC Considers Regulating Mobile Broadband under Net Neutrality Principles**

In a September 15 article, *The New York Times* reported that the FCC was holding roundtable discussions to determine whether net neutrality regulations should include cellular Internet services accessed on mobile devices. The Commission’s 2010 Open Internet Order as well as the new May 2014 proposal targeted only ISPs that provided wired Internet services to customers. Mobile Internet providers had previously been exempt due to the technical limitations of their services. The *Times* wrote that Wheeler had told attendees at the annual convention of CTIA – The Wireless Association, the largest trade group of the mobile phone industry, that “there have been significant changes in the mobile marketplace since 2010.” The *Times* reported that in 2014, nearly 120 million Americans had subscriptions to the fastest mobile broadband services as compared to only 200,000 subscribers in 2010. Wheeler said that any new proposals regulating the Internet would need to account for the changes in how Americans access Internet data. However, the FCC’s discussions at the roundtable meetings were not part of any official policymaking processes. Rather, the meetings were merely advisory discussions for members of the Commission.

In the same story, Gene Kimmelman, the president and chief executive of consumer advocacy organization Public Knowledge, told the *Times* that Wheeler’s comments were “a shot across the bow” for the mobile wireless Internet industry. “We’ve sensed for a while the F.C.C. [sic] is looking to beef it up on the wireless side,” Kimmelman told the *Times*. “There’s less of a difference between wireless and wireline than there was five years ago.”

However, Meredith Atwell Baker, a former FCC commissioner and chief executive of CTIA – The Wireless Association, told the *Times* that wireless Internet companies should be treated differently because they rely on the public spectrum, which has limited capacities as compared to the opportunities to continually build more wired Internet infrastructure. “The growth of smartphones and LTE [the fastest wireless broadband Internet] — and the constant change in our ecosystem — is the clearest evidence that we should retain a mobile-specific approach, because it has worked so well for consumers,” said Baker.

In an interview for a September 24 Bloomberg BNA story, Consumer Federation of America Research Director Mark Cooper also argued that the FCC should consider technological differences between wired Internet and wireless mobile broadband before imposing net neutrality rules on the wireless industry. “Could the FCC do a better job on network neutrality for wireless? Certainly,” said Cooper. “Should they more fully recognize the role of mobile communications in the 21st century communications network? Absolutely. But don’t tell me mobile is a substitute for wireline. It’s not.”

**FCC Considers Hybrid Approach to Net Neutrality**

On October 30, *The Wall Street Journal* reported that Wheeler was considering alternatives to the FCC’s May proposal. Wheeler’s new proposal aimed to split ISPs’ broadband services into two distinct categories. The first category would be a retail service, which would involve consumers paying ISPs for Internet access. Under this category, the FCC would exercise less regulatory control, which would allow ISPs to provide consumers with specialized Internet services or to experiment with pricing based on the amount of Internet data consumers use. The second category is a back-end service, which focuses on ISPs’ relationships with content providers. The FCC would classify ISPs as “common carriers” for the purposes of back-end services between broadband Internet companies and content providers. Reclassification as a “common carrier” under Title II of the Telecommunications Act would allow the FCC to regulate financial deals between an ISP and Internet content providers.

*The Wall Street Journal* reported that Wheeler’s developing hybrid plan stemmed from proposals submitted by the Mozilla Foundation, a non-profit that advocates for Internet openness, and the Center for Democracy and Technology. The organizations believed that the advantage of the hybrid approach to net neutrality would mean that the FCC was not completely reversing previous decisions to deregulate the broadband Internet industry, which might place the agency “on firmer legal ground.” However, an FCC spokeswoman did not explicitly confirm that the new proposal was the leading idea at the Commission. Rather, she told *The Wall Street Journal* that the agency was still weighing all possibilities related to reclassification options.

After news of the possible plan leaked, *The Washington Post* reported in an October 31 story that both consumer groups and ISPs expressed concern over the hybrid proposal. Jonathan Banks, a public policy executive for USTelecom, told the *Post* that an FCC decision to reclassify services between ISPs and content providers as a “common carrier” relationship under Title II would draw a legal challenge. “I think they’ll certainly hear from the broadband industry that, from our perspective, Title II is Title II and we would feel compelled to challenge any sort of Title II in court,” Banks said.

In an October 31 press release, Public Knowledge President Kimmelman also expressed concern that the hybrid approach could still allow for financial deals between ISPs and content providers for better services. “[P]olicy is not made through leaked articles. Reports of allowing inappropriate paid deals between ISPs and [content] providers is worrisome,” Kimmelman said in the press release. “As the FCC clarifies how their Title II framework works, it is critical that the Chairman explains how it will protect the core tenets of an open Internet that consumers expect and businesses require. This includes, but is not
limited to, explaining what sort of prioritization is allowed and if allowed, why that level of prioritization is not harmful.”

**President Obama, Republican Critics Weigh In on Net Neutrality**

During much of 2014, President Obama remained largely absent from the debates over net neutrality regulations. However, on November 10, the White House released an online video statement in which Obama called on the FCC to reclassify ISPs as “common carriers” under Title II of the Telecommunications Act in order to enforce net neutrality rules. “In plain English, I’m asking [the FCC] to recognize that for most Americans, the Internet has become an essential part of everyday communication and everyday life,” Obama said in the video. In addition to the video, the White House released a written statement from the President that called for the FCC to establish “bright-line” rules that would prohibit ISPs from blocking legal online content and from intentionally slowing or speeding up the delivery of Internet content, require increased transparency about Internet services, and ban paid prioritization for content delivery. The written statement also called for the rules to be applied to mobile broadband Internet services.

In both the video and written statements, Obama acknowledged that the FCC had the sole authority to decide on net neutrality rules but stressed that the Commission should consider the public comments on the issue. “The FCC is an independent agency, and ultimately this decision is theirs alone. But the public has already commented nearly four million times asking the FCC to make sure that consumers, not the cable companies, get to decide what sites they use,” Obama said in the video statement. “Americans are making their voices heard and standing up for the principles that make the Internet a powerful force for change. As long as I’m President, that’s what I’ll be fighting for, too.” Obama’s video and written statements are available at http://www.whitehouse.gov/net-neutrality.

The response to Obama’s call for the FCC to reclassify ISPs as “common carriers” under Title II of the Telecommunications Act was mixed. Among the critics of the President’s suggestion for reclassification were Republican Congressional leaders. In a November 10 statement, House Speaker John Boehner (R-Ohio) said that the President’s proposed net neutrality regulations would stifle Internet innovation as well as hinder the economy. “It’s disappointing, but not surprising, that the Obama administration continues to disregard the people’s will and push for more mandates on our economy,” Speaker Boehner said in the statement. “An open, vibrant Internet is essential to a growing economy, and net neutrality is a textbook example of the kind of Washington regulations that destroy innovation and entrepreneurship.”

In a November 13 op-ed in The Washington Post, Sen. Ted Cruz (R-Texas) also criticized the President’s proposal for reclassification. He suggested that regulations on Internet businesses would slow entrepreneurial efforts in technology industries and harm consumers. “[N]et neutrality is Obamacare for the Internet,” Sen. Cruz wrote. “It would put the government in charge of determining Internet pricing, terms of service and what types of products and services can be delivered, leading to few choices, fewer opportunities and higher prices.”

However, Sen. Al Franken (D-Minn.) pushed back against Sen. Cruz’s claims that the FCC’s establishment of net neutrality rules would create new regulations on the Internet. In a November 16 interview, Sen. Franken told Candy Crowley on CNN’s “State of the Union” that “[Cruz] has it completely wrong and he just doesn’t understand what this issue is.” Sen. Franken argued that net neutrality rules would not implement any new programs. Rather, the regulations would ensure that all Internet traffic would continue to be treated as equal. “We’ve had net neutrality the entire history of the Internet,” Sen. Franken told Crowley. “This is about re-classifying something so that it stays the same. This would keep things exactly the same that they’ve been.”

In a November 10 interview with The Verge, Columbia Law School Professor Tim Wu, who coined the term “net neutrality” in 2003, also agreed with the President’s proposal to reclassify ISPs as “common carriers” under Title II. “I think [Obama’s proposal] was bold and courageous and, in some ways, just obvious,” Wu said. “But sometimes, it takes someone who’s not deeply embedded in the game to say this is the obvious thing to do.” He suggested that the FCC would be best suited to fully choose a side in the net neutrality debate because trying to please everyone might prove to be challenging, especially after Obama indicated his support for reclassification. “If [the FCC] stay[s] in the middle, they’re kind of naked right now — there’s no one there with them,” Wu said. “It’s not like Congress is gonna help out. Congress is going to be against any version of the net neutrality rule, [and] the tech companies are against any compromise. Sometimes, the middle can end up being a very dangerous place.”

— Tim Wu, Professor, Columbia Law School

“If [the FCC] stay[s] in the middle, they’re kind of naked right now — there’s no one there with them. It’s not like Congress is gonna help out. Congress is going to be against any version of the net neutrality rule, [and] the tech companies are against any compromise. Sometimes, the middle can end up being a very dangerous place.”

CASEY CARMODY
SILHA BULLETIN EDITOR

5
“Drone Journalism” Presents Possibilities But Faces Legal Obstacles

Some journalists looking for a new or cheaper way to gather information have begun to look to the skies. Advances in remotely controlled aerial devices, known as “drones” or “unmanned aerial vehicles,” give journalists new possibilities for covering stories and capturing images. With drones already being used by the U.S. government in warfare, border protection, ecological surveying, and law enforcement, private citizens and companies are hoping to take advantage of drone capabilities. But citizens and journalists hoping to use drones to gather information will need to navigate an uncertain legal environment. Some states have passed laws regarding drones, but these laws vary wildly and some regulate only government drone use. Meanwhile, the Federal Aviation Administration (FAA) is responsible for federal drone regulation policy but has not yet issued drone-specific regulations. Recent litigation has also questioned whether the FAA has authority to regulate some uses of drones. In sum, drones offer tantalizing possibilities for journalists but such use remains legally problematic.

Media, Researchers and Advocates Explore “Drone Journalism”

Despite the legal obstacles, journalists and researchers have been exploring the potential of drone journalism. The Schools of Journalism at the University of Missouri and the University of Nebraska have each established drone journalism research programs. Nebraska’s Drone Journalism Lab launched in November 2011 with a mission to provide resources for students to build and test drones for journalistic use as well as to research the emerging ethics and strategies of drone journalism. In July 2013, both programs received cease-and-desist letters from the FAA requiring them to stop all outdoor drone flights. Each stopped drone testing and applied for a Certificate of Authorization (COA) from the FAA, the authorization legally required for public entities to operate a drone. Both applications are still pending, and the programs have had to refocus efforts on more theoretical and policy research rather than experimenting with actual drone flights.

CNN and Georgia Institute of Technology also announced a joint research initiative on how media organizations can use drones safely and effectively. In a June 23, 2014 press release, CNN senior vice president David Vigilante said the project is intended to “accelerate the process for CNN and other media organizations to safely integrate this new technology into their coverage plans.” The initiative plans to report its findings to the FAA in hopes of promoting journalist-friendly regulations by the agency.

Meanwhile, the FAA has aggressively pursued those using private drones without authorization. A spate of unapproved drone flights over public crowds, such as at sporting events during the summer and fall of 2014, prompted the FAA to clarify its regulations. Citing safety concerns posed by unauthorized drones flying over crowded areas, on Oct. 27, 2014, the FAA published a public notice expanding the existing ban on private flights of unmanned vehicles over sporting events with more than 30,000 attendees. The regulation would require approval from both the FAA and the licensed broadcaster of the sporting event in order to authorize the drone flight. Violation of the regulation could carry criminal prosecution, including up to one year of jail time. According to a Nov. 9, 2014 article by The Washington Post’s Craig Whitlock, the notice is “the first time the agency has explicitly stated that reckless drone pilots could wind up behind bars.” Pepperdine Law Professor Gregory McNeil wrote in an Oct. 31, 2014 article for Forbes that “the ban is allegedly for national security purposes, which means that arguable justification may even trump future safe uses of drones — even by the media.”

On Sept. 25, 2014, the FAA announced the first private drone use to receive authorization, The agency granted regulatory exceptions to six film companies to use drones to record television and film. The FAA will not require COAs, which may signal the beginning of a less rigid approach to authorizing drone use. But the FAA emphasized that the flights would take place in controlled set environments and the drones were subject to extensive safety approval. “We are thoroughly satisfied these operations will not pose a hazard to other aircraft or to people and property on the ground.” The administration said it was still considering more than 40 exception applications by other private entities. Secretary of Transportation Anthony Foxx told reporters on September 25, that “[t]oday’s announcement is a significant milestone in broadening commercial use” of drones.

The exemptions are particularly significant because they lay out for the first time the parameters that the FAA will require a private drone operator to observe. According to Sept. 25, 2014 article on DroneJournalism.org, these exemptions are the FAA’s first indication to private operators of “what can fly, when it can fly, when it can fly, how it can be flown, and who can fly it.” The pervasive restrictions of the exceptions require, among many other things, that the drones operate only in a “sterile” environment, with no unauthorized person within 1000 feet and receive advance permission from local FAA authorities. The drones can also only be operated in daylight with a line of sight between the operator and the drone.

Although they were tailored specifically to the six film companies’ operations, the FAA’s requirements could present insurmountable obstacles if applied to drone journalism. Journalists hoping to capture newsworthy public events live, for instance, would likely collide with provisions on both advance permission and proximity to unauthorized persons. The University of Missouri Drone Journalism Program expressed similar concerns after it applied for a COA, stating in an Aug. 21, 2013 blog post that it expects the restrictions imposed by a COA “will make ‘drone journalism,’ as we’ve come to know it, all but impossible.” Because drones can fly “only within a predetermined, relatively small,
contiguous space,” journalists’ “ability to travel and respond to events (key attributes of field reporting) will be entirely curtailed.” Requiring a “sterile” environment may make the operation of drones in public, and particularly in crowded, urban spaces, impracticable.

Journalists Face Evolving, Uncertain Legal Landscape

The FAA is the only federal agency currently regulating drones. In 2012, Congress passed the FAA Modernization and Reform Act, under which the FAA must “provide for the safe integration of civil unmanned aircraft systems into the national airspace system” by Sept. 30, 2015. After this act, the FAA has maintained that until it has regulations in place, all commercial drone use in U.S. airspace needs to be explicitly permitted by the agency. Any domestic drone use, private or public, must apply for and receive FAA approval.

The FAA has reiterated that its mission is air safety. In the Nov. 14, 2013 statement on the establishment of six drone test sites around the country, the FAA emphasized that the testing was meant to explore how drones can be integrated safely into the national airspace and not “the scope of data that can be collected” by drones. Despite the introduction of several bills, Congress has not passed legislation governing drone use since the 2012 FAA Act.

However, in March 2014, an administrative law judge found that the FAA does not have the authority to regulate “model” drone use. In Huerta v. Pirker, Docket No. CP-217 (NTSB Mar. 6, 2014), available at http://www.ntsb.gov/legal/pirker/Pirker-CP-217.pdf, the judge dismissed a $10,000 FAA fine for recklessly operating a drone. The judge found that model drones are not “aircraft” subject to FAA regulation.

Other drone proponents seized on the Pirker decision as an opportunity to advocate for unregulated drone use. In response to letter demanding it cease drone operations, Texas Equusearch, a non-profit search-and-rescue group, challenged the FAA’s authority to regulate their drone use. On July 18, 2014, the U.S. Court of Appeals for the D.C. Circuit dismissed the challenge, but on the basis that the FAA’s letter had no legal authority. Tex. Equusearch Mounted Search and Recovery Team v. Fed. Aviation Admin., Case No. 14-1061 (D.C. Cir. July 18, 2014). Although the court declined to rule on the FAA’s broader authority to regulate, it essentially rendered the agency’s tactic of issuing cease and desist letters to drone users legally powerless.

Meanwhile, a coalition of media companies filed an amicus brief with the NTSB in opposition to FAA regulation while the Pirker case was pending appeal before the National Transportation Safety Board (NTSB). The coalition, including the Associated Press, The New York Times, Reporters Committee for Freedom of the Press and many others, argued that the FAA’s current categorical ban on drone use for newsgathering is unconstitutional. The amici argued that, contrary to FAA statements that media use is the type of “business purpose” that allows drone regulation, “[t]he FAA’s position is untenable as it rests on a fundamental misunderstanding about journalism. News gathering is not a ‘business purpose.’ It is a First Amendment right.”

In addition to challenging the FAA’s authority, the amici also challenged its methods. The brief argued the FAA’s letters constituted an “ad hoc cease-and-desist enforcement process,” which created “an impermissible chilling effect on the First Amendment newsgathering rights of journalists.”

On November 18, 2014, the NTSB reversed the decision in Pirker, ruling that the FAA did have authority to regulate model drones. Huerta v. Pirker, Order No. EA-5730 (NTSB Nov. 18, 2014), available at http://www.ntsb.gov/legal/pirker/5730.pdf. The court acknowledged the amici making First Amendment arguments on behalf of drone use, but declined to reach the more complex constitutional questions. Instead, the case could be decided on a narrower issue: model drones are “aircraft” for the purposes of federal aviation law, and thus are within the regulatory jurisdiction of the FAA. The decision can be appealed, but no appeal had been filed as the Bulletin went to press.

University of Washington professor and drone expert Ryan Calo argued that the case left important First Amendment questions unanswered. If the FAA is restricting some people’s use while allowing others, they will need to justify these distinctions, particularly where they burden newsgathering, Calo told ArsTechnica for a Nov. 18, 2014 article. If the FAA is restricting drone use for those “with legitimate reasons in the public interest — like, journalists filming protests — but allowing others that are not — like surveying people’s land or making a movie — [that] doesn’t make sense.”

However, Holland & Knight attorneys Jameson B. Rice, Joel E. Roberson, and Christine N. Walz wrote in a December 10 news alert post on the firm’s web site that members of the U.S. House of Representatives Committee on Transportation and Infrastructure’s Subcommittee on Aviation were pushing FAA officials to adopt regulations of drones.

“If you have a news organization hovering over a protest and videoing, that’s really valuable for the First Amendment.”

— Professor Margot Kaminski, Yale Law School

overseas,” the attorneys wrote. “[T]his was described as stifling innovation and creating a competitive disadvantage.”

According to the attorneys, FAA officials explained that although the Administration planned to release some minor proposals governing the private use of drones before the end of 2014, a final comprehensive rule would not likely be in place until 2017 or later.

Although the FAAs implementation of drone regulations has been slow moving, many state legislatures have debated the proper scope of drone use. Fifteen states have passed laws restricting drone use and 29 more have had drone bills introduced. However most of these laws address drone use by law enforcement, often imposing warrant requirements in some instances where police used drones to gather evidence. Only five states have laws that regulate private drone use. These are the laws with which prospective drone journalists would need to comply.

Louisiana, Texas and Wisconsin have established criminal laws for various uses of drones, while Idaho and Oregon have created civil causes of action. The Texas law broadly criminalizes private drone use but includes a list of exceptions for acceptable private use. Acceptable uses include surveying utilities, scholarly research, real estate evaluation and several others. The Wisconsin law takes a different approach, making it a misdemeanor offense to record a
Drones, continued from page 7

person with a drone where they have a “reasonable expectation of privacy.” The Louisiana law, the most recent state law, passed in July 2014, makes it a crime to photograph or record a person’s property via drone without their consent.

The Idaho and Oregon laws do not criminalize use, but rather allow private plaintiffs to sue over privacy or trespass violations involving drones. The Idaho law specifically and solely targets the fruits of surveillance, prohibiting the publicizing of images or video of private property recorded by a drone. The Oregon law focuses on drone use more generally, allowing property owners to sue a person who operates a drone less than 400 feet above their property.

These laws pose significant challenges for journalists seeking to use drones. Although they vary in their approach to drone regulation, each could potentially restrict some newsgathering activity. Significantly, none of these laws contains an exception for newsgathering or reporting.

Several of these laws have prompted objections based on First Amendment grounds. For instance, although the Texas law provides many exceptions for specific drone uses, none would allow media to use drones for newsgathering. Margot Kaminski, a scholar at Yale Law School, believes that the Texas law may be struck down for violating the First Amendment. “If you have a news organization hovering over a protest and videoing cops beating protesters, that’s really valuable for the First Amendment,” she told The Washington Post in a June 18, 2013 article on behavior that would likely violate the Texas law. While “there’s really not all that much out there that shows how the First Amendment and privacy law are supposed to intersect,” Kaminski believes the Texas law is “likely to end up with a ruling that says this doesn’t pass First Amendment muster.” According to a June 3, 2013 article by the Electronic Frontier Foundation’s Dave Maass, the Texas law “manages to mess up both sides of the table by allowing cops to use drones without a warrant while also hampering the press’ ability to use drones in newsgathering.”

The Idaho law, which specifically bans drone surveillance of “farm, dairy, ranch or other agricultural industries,” may violate the First Amendment rights of animal rights groups, which the law seems specifically targeted to restrict. Efforts to restrict drone use in this way may be in response to the work of journalists like Will Potter, who raised $75,000 through the online fundraising site Kickstarter to purchase drones to surveil and report on large farms and ranches. According to a July 22, 2014 article on AllGov.com, Potter invested in drones because more traditional undercover reporting from inside such facilities has been outlawed by so-called “ag-gag” laws. (For more on the conflict between journalism and “ag-gag” laws, see “States Consider Banning Undercover Recording at Agricultural Operations” in the Summer 2011 issue of the Silha Bulletin.) According to Timothy B. Lee in a June 18, 2013 Washington Post article, there is a “good chance” that the law’s provisions “violate the First Amendment rights of animal rights advocates.” But the Idaho law also bans recording with drones more broadly. The ACLU’s Allie Bohn wrote in an April 24, 2013 article that, “Idaho’s restrictions are so broad that they would likely prohibit a news station from using a drone to gather information for their traffic report absent written consent of everyone on the road.”

According to Vice staff writer Jason Koebler in an April 28, 2014 article, the Louisiana law is “by far the most stringent anti-drone law passed in the United States so far.” Brenden Shulman, a drone law expert, told Vice that the law may violate the First Amendment because the law “seems to discriminate against using a specific technology, namely drones, rather than target the offensive conduct that is of concern, which appears to be the surveillance of private areas.” The law’s sponsor, state Sen. Dan Claitor (R-Baton Rouge), responded to other lawmakers’ First Amendment criticisms, saying that journalists “believe they have a noble purpose but [a] noble purpose does not override my property rights.”

Because the FAA continues to broadly ban drone use, there have been no reports of enforcement of these state laws. If no one is prosecuted under the laws, it is unlikely that any plaintiff would have standing to challenge the laws for an alleged constitutional deficiency. In addition, parts of state drone laws may be preempted by federal drone laws, meaning states could not enforce those parts of the laws. But assuming the FAA will eventually release regulations allowing private drone use, these state laws, which vary greatly in states that have enacted them, will govern individuals’ use of drones. For the foreseeable future, drone journalism remains in an environment of multi-faceted legal uncertainties.

ALEX VLSIDES
SILHA RESEARCH ASSISTANT

The Bulletin is also available online at http://www.silha.umn.edu/news/

Archived issues of the Bulletin are available online at http://www.silha.umn.edu/news/bulletinarchive.html
Supreme Court Considers Whether Facebook Posts Can Constitute “True Threats”

On Dec. 1, 2014, the U.S. Supreme Court heard oral arguments in *Elonis v. United States*, which considered how courts should define what types of statements can constitute a “true threat.” True threats occupy one of the few categories of expression not safeguarded by the First Amendment. The U.S. Supreme Court first carved out a limited exception to First Amendment protection for true threats of physical violence in *Watts v. United States*, 394 U.S. 705 (1969).

The case presented the question of whether the convictions for threatening another person in violation of 18 U.S.C. § 875(c), which prohibits individuals from transmitting interstate communications that contain a threat to injure others, were unconstitutional. The case will play a significant role in future cases that determine what constitutes a true threat in online communication. The decision could also have implications for music lyrics.

The case arose from Anthony Elonis’ postings on Facebook, directed at his ex-wife, federal law enforcement officials, and elementary school children, among others. For example, Elonis posted on Facebook in 2010: “There’s one way to love you but a thousand ways to kill you. I’m not going to rest until your body is a mess, soaked in blood and dying from all the little cuts.” On Dec. 8, 2010, federal authorities arrested Elonis for posting the threatening Facebook messages and charged him with violating 18 U.S.C. § 875(c).

During the trial in federal district court in Philadelphia, Elonis argued that he never intended the posts to be threats. Rather, he has argued that he was writing lyrics that imitated violent and disturbing lyrics in rap music. Elonis testified at trial that rapper Eminem particularly influenced him. However, Elonis’ ex-wife testified during the trial that she took the statements seriously. She testified, “I felt like I was being stalked. I felt extremely afraid for mine and my children’s and my families lives.” She also explained that the lyrical form of the statements did not make her take the threats any less seriously. A jury convicted Elonis on four of the five charged counts of transmitting threatening communications, and sentenced him to 44 months imprisonment followed by three years supervised release. Elonis has already served more than three years in prison for his conviction.

Elonis appealed the conviction to the United States Court of Appeals for the Third Circuit, arguing that the trial court had incorrectly instructed the jury on the standard of what constitutes a true threat. *United States v. Elonis*, 730 F.3d 321 (3d Cir. 2013). The trial court judge had told the jury to use an objective reasonable person standard to determine a true threat. The jury instructions read, “a statement is a true threat when a defendant intentionally makes a statement in a context or under such circumstances wherein a reasonable person would foresee that the statement would be interpreted by those whom the maker communicates the statement as a serious expression of an intention to inflict bodily injury.” Elonis argued that instead the government must prove that he subjectively intended to threaten another person.

The Third Circuit upheld the convictions on Sept. 19, 2013, reasoning that limiting the definition of true threats to only those statements where the speaker subjectively intended to make a threat would fail to protect individuals from “the fear of violence” and the “disruption that fear engenders,” because it would protect speech that a reasonable speaker would understand to be threatening. The U.S. Supreme Court agreed to hear the case and granted certiorari on June 16, 2014.

The U.S. Supreme Court’s review of the decision will settle a split between the subjective intent standard that the Supreme Court has been using for decades and a standard similar to the objective test allowed by the Third Circuit. The Supreme Court heard oral arguments on June 1, 2016.

“Online and electronic communications, which eliminate the inflections and expressions that give meaning to words, reduce speakers’ ability to detect and correct misimpressions.”

— *Brief of Anthony Elonis Before the U.S. Supreme Court*

Ninth Circuit adopted in *United States v. Cassel*, 408 F.3d 633 (9th Cir. 2005), and the objective listener standard utilized by the majority of the other circuits, including the Third Circuit. The majority of circuits currently reject the subjective intent requirement and hold that statements that are reasonably construed as threats by the listener are not given First Amendment protection and are punishable. However, the Ninth Circuit, as well as the highest state courts in Massachusetts, Rhode Island, and Vermont, require proof of the speaker’s subjective intent to threaten before the government can punish a speaker.

Elonis’ arguments for a subjective intent standard was largely based on the last time the U.S. Supreme Court addressed the true threat doctrine in *Virginia v. Black*, 538 U.S. 343 (2003). (For more on the Black decision, see “*Virginia v. Black*” in the Summer 2003 issue of the Silha Bulletin.) In Black, the Court upheld a Virginia law banning threats expressed through cross burning. However, the Court struck down a portion of the law that made burning a cross itself a prima facie proof of intimidation and held that the state must prove an intent to intimidate existed. The Court defined true threats as “statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.” Elonis posited that the decision in Black required that the prosecution prove that a defendant subjectively intended to threaten the victim.

Furthermore, Elonis’ brief argued that the objective listener standard “would impose criminal liability on a vast array of first-person revenge fantasies that have always been staples of popular culture.” His brief highlighted that such sentiments have been commonplace in rap music and that however hateful or offensive, those songs are entitled to full First Amendment protection. Elonis argued that the lyrics he posted are no different.

Several free speech advocate groups filed amicus briefs with the Supreme Court, including the Reporters Commit-
ee for Freedom of the Press, the Student Press Law Center, and the American Civil Liberties Union. In its brief, the ACLU argued that proof of subjective intent was required to ensure that protected speech is not chilled by the fear of criminal prosecution. Another amicus brief, filed by the Marion B. Brechner First Amendment Project, sought to provide the Court with the history and conventions of rap music. The organization highlighted rap music’s “heavily stigmatized artistic and often political” nature.

On the prosecution side, several victims’ rights organizations, including the National Center for Victims of Crime and the Criminal Justice Legal Foundation, among others, filed amicus briefs. In its brief, the National Network to End Domestic Violence argued that “requir[ing] proof of a subjective intent to threaten will make it more difficult to protect victims of abuse from threats of violence made by their current and former intimate partners, who increasingly use easily accessible but sophisticated technology to track their victims and to threaten them wherever they are.”

The online context in which Elonis made the statements was also an important factor in the case. Elonis argued that an objective listener standard was inadequate when dealing with the atmosphere of social media sites. Elonis’ brief argued that “online and electronic communications, which eliminate the inflections and expressions that give meaning to words, reduce speakers’ ability to detect and correct misimpressions.” In addition, Elonis maintained that modern media allowed personal reflections intended for a small audience or no audience to be viewed widely by people who are unfamiliar with the context of the statements and thus may interpret the statements much differently than the speakers intended.

Many legal commentators have observed that the Supreme Court has never considered a threats case involving either online social media or messages conveyed in a controversial form of artistic expression like rap music. In a May 24, 2014, Forbes article, law professors Clay Calvert, Erik Niels and Charis Kubrin explained that “information posted to social media sites is often disseminated and displayed in ways that users do not control or even understand, profoundly complicating attempts to determine a person’s intent in posting something or a ‘reasonable’ person’s interpretation of it. Context becomes further complicated when a so-called threat is a lyric from a musical genre that often privileges highly exaggerated, confrontational and violent rhetoric.” The legal scholars also noted that there is a growing subset of cases that has emerged in which the act of writing violent rap lyrics itself has become a crime when they are uploaded to social media sites and interpreted by authorities as “true threats.”

“Context [of social media posts] becomes further complicated when a so-called threat is a lyric from a musical genre that often privileges highly exaggerated, confrontational and violent rhetoric.”
— Law Professors Clay Calvert, Erik Niels and Charis Kubrin

Lawyers are urging the Supreme Court to provide guidance to lower courts on how to identify true threats in the context of social media. In a March 28, 2014 article in Pennsylvania newspaper The Morning Call, Robert Richards, director of the Pennsylvania Center for the First Amendment at Penn State, commented on the complexity of determining whether statements made on social media constitute true threats. “Problems in identifying the nature of statements made via social media arise from the inability to judge body language or inflection. Unlike a letter or an email that is addressed specifically to a person, posts on social media may simply be left for anyone to find and sought out or discovered accidentally by the subject,” Richards said. “People use [social media] to say all kinds of things but they may not be directing it to a particular individual. They’re just venting their feelings.”

However, other commentators have suggested that the Court’s future decision may be less than clear. In an Oct. 8, 2014 post on FindLaw’s U.S. Third Circuit blog, attorney Mark Wilson wrote that “Elonis is free to post to Facebook for ‘therapeutic’ reasons, but there will be a point where those posts — admit-
Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberties

On Sept. 25, 2014, The New York Times reported that President Barack Obama announced during a White House press conference that U.S. Attorney General Eric Holder had chosen to resign from his position. The Times noted that Holder's resignation did not come as a surprise as he had previously said that he planned to leave the position before the end of 2014. Obama appointed Holder to the position in 2008, and commentators have suggested that Holder will leave a mixed legacy. Many have applauded Holder's work on civil rights, voting rights, and racial justice, but suggested that his handling of First Amendment and surveillance issues has been problematic.

In particular, Holder’s critics focused on the Department of Justice’s (DOJ) unprecedented use of the Espionage Act of 1917, 18 U.S.C. § 793, to pursue leakers of government secrets. In a Nov. 25, 2014 article for the Columbia Journalism Review, Kelly O’Brien pointed out that Holder’s Justice Department has used the World War I-era law as a basis to prosecute former government employees and contractors accused of leaking government information. “The fact that outgoing Attorney General Eric Holder has prosecuted more people under the Espionage Act than all previous attorneys general combined is an inescapable legacy of his time in office,” wrote O’Brien. He argued that the aggressive prosecution of leaks is one policy that the outgoing administration could have reversed, and that it would be more difficult for journalists to uncover government misconduct.

The numerous prosecutions under the Espionage Act have not only threatened journalists’ sources but also journalists themselves, according to O’Brien. With the Espionage Act, Holder chose a tool that could potentially be very dangerous to journalists, because it is vague enough to criminalize all kinds of information dissemination,” O’Brien wrote. In a September 25 editorial, The New York Times also noted that the DOJ’s pursuit of leakers during Holder’s tenure had led “prosecutors [to] seize[] phone and email [sic] records of journalists who were doing their jobs.” In 2013, the Times reported that the Department of Justice secretly seized the phone records of Associated Press reporters who wrote a 2012 story about a foiled terrorist plot to bomb a Yemeni airliner. That same year, The Washington Post also reported the Department of Justice had named Fox News reporter James Rosen as a co-conspirator during a leak investigation of a State Department official in order to obtain e-mails from Rosen’s Google account.

At the time of the revelations, Silha Professor of Media Ethics and Law and Silha Center Director Jane Kirtley told

“You really have to go back to the Nixon administration. I’m aghast to see how relentlessly this administration and the Justice Department have been pursuing [leaks].”

— Professor Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law

Critics have also pointed to Holder’s handling of efforts to subpoena New York Times journalist James Risen as a troubling aspect of the attorney general’s legacy. Risen became the focus of the DOJ after he published classified information about a failed Central Intelligence Agency (CIA) plan to undermine Iran’s nuclear program in his 2006 book, State of War. The DOJ has claimed that the source of Risen’s information was Jeffrey Sterling, a former CIA employee who was charged under the Espionage Act for allegedly disclosing confidential information. The DOJ subpoenaed Risen, claiming that it needed the journalist’s testimony to pursue the prosecution of Sterling. However, Risen has repeatedly refused to disclose any information about the sources of his information.

The DOJ’s aggressive pursuit of Risen’s testimony under Holder has led to a lengthy court battle over whether Risen can claim a journalist’s privilege to withhold information. The Supreme Court declined to hear Risen’s case in June 2014, which allowed a decision from the U.S. Court of Appeals for the Fourth Circuit ordering Risen to testify to stand. The New York Times had previously reported in May 2014 that Holder had told journalists that “no reporter who is doing his job is going to jail” in reference to Risen. (For more information on the background of Risen’s case, see “Update: Supreme Court Declines to Hear Reporter’s Privilege Cases” in the Summer 2014 issue of the Silha Bulletin, “Reporters Struggle to Claim Privilege to Avoid Testifying About Confidential Sources” in the Fall 2013 issue, and “Judges Rebuke Government on Leak Prosecutions” in the Summer 2011 issue.)

In discussing the DOJ’s conflicts with journalists under the existing attorney general, Freedom of the Press Foundation Executive Director Trevor Timm suggested in a September 26 post on the organization’s blog that Holder had created many problems for the press. “Holder will leave behind a complex and hotly debated legacy at the Justice Department on many issues, but one thing is clear: he was the worst Attorney General on press freedom issues in a generation, possibly since Richard Nixon’s John Mitchell pioneered the subpoenaing of reporters and attempted to censor the Pentagon Papers,” Timm wrote.

The Washington Post reported on October 10, 2014 that Assistant U.S. Attorney James Trump had hinted that the government intended to subpoena Risen again during Sterling’s trial beginning in 2015. The Post also noted that Trump did not indicate what kind of penalties the government would seek if Risen refused to testify. Risen has previ-
Attorney General, continued from page 11

Roses Award,” named for Richard Nixon’s secretary who erased many Watergate tapes, for worst open government performance by a federal agency. (For more on Holder’s promises of transparency, see “Obama’s Policies Promote Openness; Some Secrecy Persists” in the Spring 2009 issue of the Silha Bulletin.)

Reflecting on Holder’s resignation in a Sept. 25, 2014 article for The Daily Beast, law professor and member of the President’s Review Group on Intelligence and Communication Technologies Geoffrey Stone contended that Holder had been one of the most liberal members of Obama’s administration for many civil rights causes, such as equal rights for gays and lesbians as well as challenging voter-ID laws. “On a range of other terrorism-related issues, however, Holder has defended the legality of programs and positions that civil libertarians deplore,” Stone wrote. “These include, among others, approval of investigations and prosecutions of government employees and contractors who leak classified information, approval of the issuance of subpoenas directed at journalists who publish leaked classified information, … approval of the NSA’s telephone metadata program, [and] approval of the use of the state-secrets privilege to shield the secrecy of classified national security programs.” (Stone was the 2006 Silha lecturer. For more information about his lecture, see “Geoffrey Stone Predicts First Amendment will Protect Journalists from Prosecution at 21st Annual Silha Lecture” in the Fall 2006 issue of the Silha Bulletin.)

On Nov. 8, 2014, The New York Times reported that Obama announced the nomination of Loretta E. Lynch, a federal prosecutor from Brooklyn, N.Y., to replace Holder as attorney general. Prior to the announcement, however, Timm offered advice for the new head of the Justice Department in his September 26 post. “The next attorney general, whoever it is, will have a lot of issues on his or her plate,” wrote Timm. “But better respecting the rights of reporters and the First Amendment should be at the top of that list.”

As the Bulletin went to press, U.S. Senate confirmation hearings for Lynch’s nominations had not yet begun.

Silha Bulletin Editor Casey Carmody contributed to this story.

ALEX VLISIDES
SILHA RESEARCH ASSISTANT

Please visit the Silha Center online. Our home page is http://www.silha.umn.edu/

Our events page is http://www.silha.umn.edu/events/
Problems Continue for News Coverage of Ferguson Shooting after Grand Jury Decision

On Nov. 24, 2014, St. Louis County Prosecuting Attorney Robert McCulloch announced that a grand jury had chosen to not indict police officer Darren Wilson for fatally shooting Michael Brown, an unarmed 18-year-old African American. The Aug. 9, 2014 shooting sparked scores of protests in Ferguson, Mo., a suburb of St. Louis. Clashes between demonstrators and local police authorities drew the attention of several local and national new organizations, which sought to cover the tension between a predominantly black community with law enforcement authorities who were primarily white. During the coverage of the Ferguson protests in August, several journalists were arrested during law enforcement attempts to manage the large and increasingly violent protests. The arrests of journalists prompted several press advocacy organizations to call for Ferguson law enforcement authorities to recognize the First Amendment rights of news organizations to gather news. (For more information about the arrests of journalists in Ferguson, see “Journalists Arrested During Protests in Missouri; Journalist Abroad Face Dire Situations” in the Summer 2014 issue of the Silha Bulletin.)

However, law enforcement officials continued to struggle with attempts to manage media during the course of the grand jury proceedings that began on Aug. 20, 2014. News organizations were also criticized for how they handled the coverage throughout the several months after Brown’s death.

Leaks about Grand Jury Proceedings Create Problems for Government Officials

On October 1, The Washington Post reported that the St. Louis County prosecutor’s office was investigating accusations of grand jury misconduct because information about the proceedings was allegedly posted on Twitter. Several Twitter users alerted the prosecutor’s office after seeing another user, who was identified as Susan Nichols, post a message that said she was a friend of a member of the grand jury who had explained that evidence against Wilson was not enough to warrant an arrest. Nichols quickly deleted the post after several users alerted her that the proceedings of grand jury are supposed to be secret, but not before another Twitter user captured a screenshot of the Tweet that he submitted to the Post. Spokesman Ed Magee told the Post that the prosecutor’s office was “looking into the matter.” However, the following day, the Associated Press (AP) reported that Nichols had told investigators that her Twitter account had been hacked. The prosecutor’s office told the AP that they did not have any evidence to “suggest information in the post was credible.” The St. Louis Post-Dispatch also reported on October 30 that McCulloch released a statement that an investigation into the Twitter post indicated that Nichols account was hacked and that she was not connected to anyone on the grand jury.

Reports of false information on Twitter were not the only challenges that prosecutors faced in ensuring the secrecy surrounding the grand jury proceedings. On October 23, The Washington Post reported that a variety of information provided to the grand jury that supported Wilson’s account of events had been leaked to several different news outlets, including the New York Times, the St. Louis Post-Dispatch, and The Washington Post. The Post reported that many of the leaks focused on Wilson’s testimony before the grand jury in which he defended his actions during the August 9 shooting. Wilson’s testimony indicated that he had feared for his life before he fatally shot Brown. On October 22, the Post-Dispatch reported on the contents of the official autopsy of Michael Brown that prosecutors gave to the grand jury. The Post-Dispatch also published photos of the full report, which was stamped “not for secondary release.” The St. Louis newspaper did not disclose how it obtained the report.

The Washington Post reported in its October 23 story that both officials from the St. Louis County prosecutor’s office and Wilson’s legal team denied being the source of the grand jury leaks. In an October 24 post on the Gateway Journalism Review’s web site, Southern Illinois University School of Journalism Director William Freivogel speculated that the leaks could possibly have come from officials in the U.S. Department of Justice. Freivogel noted that many of the stories based on the information leaks “were written by the newspapers’ Justice Department reporters in Washington.” He observed that The New York Times “attributed [its] information to ‘government officials briefed on the federal civil rights investigation’ — not the state criminal investigation.” Freivogel suggested that members of Congress who had been briefed on the federal investigation potentially could have been the source of the leaks.

In an October 23 story, CBS News cited an unnamed Department of Justice official who complained that Attorney General Eric Holder was critical of the news accounts of the grand jury proceedings. Holder called the leaks a “selective flow of information” that were “inappropriate and troubling” during agency meetings, according to CBS News. St. Louis Public Radio reported the same day that St. Louis County Executive Charlie Dooley released a statement criticizing the leaks of the grand jury proceedings to news outlets. “The orchestrated leaks regarding the work of the grand jury reviewing the Michael Brown shooting are unbelievable and certainly do not inspire confidence in this process or the office of the prosecuting attorney,” Dooley said in the statement.

However, St. Louis Public Radio also reported that former St. Louis County Police Chief Tim Fitch had told a local radio station that officials might have leaked information to prepare the public for the possibility that the grand jury would choose to not indict Wilson. “[The leaks are aimed] to start getting some of the facts out there to kind of let people down
Ferguson, continued from page 13

slowly,” Fitch said, according to St. Louis Public Radio.

Pathologist Challenges Quotes in News Accounts of Autopsy Report

Others also criticized the way news organizations covered the grand jury proceedings. In particular, Dr. Judy Melinek, an independent pathologist who the Post-Dispatch quoted in its October 22 story on Brown's autopsy reports, objected to the way the newspaper reported her comments from an interview. The Post-Dispatch quoted Melinek as saying the autopsy report “supports the fact that this guy is reaching for the gun, if he has gunpowder particulate material in the wound.” The newspaper added that she said, “If he has his hand near the gun when it goes off, he’s going for the officer’s gun.” The newspaper also reported that Melinek described how the bullet wounds indicated that Brown might have been lunging toward Wilson. Other news organizations, such as the AP and The Washington Post, picked up the Post-Dispatch’s report as well as Melinek’s quotes.

In an October 22 appearance on MSNBC’s “The Last Word,” Melinek told host Lawrence O’Donnell that the Post-Dispatch had taken her statements out of context by not acknowledging that several other scenarios could have explained Brown’s wounds. “What happens sometimes is when you get interviewed and you have a long conversation with a journalist, they’re going to take things out of context. I made it very clear that we only have partial information here,” Melinek said. “I’m not saying that Brown going for the gun is the only explanation. I’m saying the officer said he was going for the gun and the right thumb wound supports that.” Melinek and O’Donnell also discussed alternative scenarios that did not include Brown reaching for Wilson’s gun but could still be consistent with the findings in the autopsy report.

Roy Malone wrote in an October 31 post for the Gateway Journalism Review that news organizations responded to Melinek’s criticisms differently. Malone noted that The Washington Post quickly added an editor’s note clarifying that “Melinek had said the autopsy ‘supports Officer Darren Wilson’s statement that brown was reaching for the gun but that other scenarios are possible.’”

St. Louis County Police Targeted Media in “No-Fly Zone” Request

On November 2, the AP reported that it had obtained audio recordings through a Freedom of Information Act request that indicated local law enforcement authorities’ requests to the Federal Aviation Administration (FAA) for a no-fly zone around Ferguson was intended to limit media coverage of protests. The FAA imposed flight restrictions on 37 square miles surrounding the Ferguson area during 12 days in August. Local police officials had previously stated that they made the requests for safety purposes rather than to hinder media coverage.

The AP reported that the day after the flight restrictions were imposed, FAA officials had trouble with managing how commercial airlines and police helicopters might operate in the no-fly zone while prohibiting others. In a recorded telephone conversation, an FAA manager explained that the St. Louis County Police “finally admitted [the requested order] really was to keep the media out.” The story also noted that a manager in the FAA’s Kansas City office said that law enforcement officials “did not care if [the Administration] ran commercial traffic through this [temporary flight restriction] all day long. They didn’t want media in there.”

The AP story also recounted that local police officials had said on several occasions that the only purpose for the flight restrictions was for safety. Brian Schellman, a St. Louis County police department officer, had told NBC News on August 12 that aircrafts were in danger of being hit by gunfire. “On Sunday night our police helicopter came under fire on 3 or 4 occasions, so we requested that the FAA put up a no-fly zone for the safety of pilots who would be in the area,” Schellman told NBC News. However, the telephone recordings that the AP obtained indicated that an FAA manager said that the descriptions of shots fired at the police helicopter were unconfirmed “rumors.”

The AP reported that one FAA official at the Administration’s command center had asked FAA authorities in Kansas City whether the flight restrictions were actually intended as safety precautions. “So are [the police] protecting aircraft from small-arms fire or something,” the Administration command center official asked in the recordings, according to the AP. “Or do they think they’re just going to keep the press out of there, which they can’t do.”

Upon learning of the AP’s revelations, press advocacy organizations were critical of the flight restrictions imposed around Ferguson. On November 4, Lee Rowland, an American Civil Liberties Union staff attorney, told CNN that the flight restrictions hindered the press’ ability to inform the public. “It’s very troubling to the ACLU and it should be extremely troubling to anyone in the public who wants to get news about what their government is up to,” Rowland said. “This was a no-fly zone targeted at the media and it appears it was not for safety purposes. If indeed the air restrictions were only to keep the media out, it is a constitutional violation of the freedom of the press.”

In a November 7 press release, Society of Professional Journalists (SPJ) National President Dana Neuts also criticized St. Louis County law enforcement agencies for using flight restrictions to hinder news organizations. “If other law enforcement agencies follow the example of media relations set in Ferguson, freedom of the press, guaranteed by the First Amendment, will be further eroded.”

“If other law enforcement agencies follow the example of media relations set in Ferguson, freedom of the press, guaranteed by the First Amendment, will be further eroded.”

— Dana Neuts, President, Society of Professional Journalists
agencies across the country to ensure the public’s right to know, but law enforcement agencies must be willing to meet us halfway.”

**News Organizations Criticized over Ferguson Coverage**

In a November 25 story, *Washington Post* media critic Erik Wemple wrote that one of news organizations’ biggest critics of the coverage of the Ferguson grand jury proceedings was St. Louis County Prosecutor Robert McCulloch. “The most significant challenge encountered in this investigation has been the 24-hour news cycle and its insatiable appetite for something, for anything to talk about, following closely behind with the non-stop rumors on social media,” McCulloch said during the November 24 press conference announcing the grand jury’s decision. McCulloch also criticized news organizations for releasing secret grand jury information because it could have influenced eyewitness accounts of the shooting. Wemple pushed back against the prosecutor’s criticisms of news organizations, however. He noted that McCulloch himself conceded that most witnesses appearing before the grand jury testified prior to news organizations publishing the autopsy report and accounts of Wilson’s testimony, which meant that media reports would not have affected witnesses. “So no harm done then?” wrote Wemple. “The grand jury got to hear its testimony free of leaked information, and the public got an early and accurate summation of the case.”

Wemple suggested that McCulloch’s claims more likely stemmed from his frustration over being blamed for several of the disclosures about the grand jury proceedings. Kimberly Kindy, one of the co-writers of *The Washington Post*’s story about the leaked testimony of Wilson, told Wemple that it was “pretty clear that [the officials from the prosecutor’s office] were frustrated with the leak stories. People were asking if the leaks were coming from them.”

News organizations also faced criticisms for their coverage of the protests after the announcement that the grand jury chose to not indict Wilson. In a November 25 episode of WNYC’s “On the Media,” host Bob Garfield criticized cable news organizations for not providing larger context to depictions of violent protests. “TV has a checkered history of letting de-contextualized images define events,” Garfield said. Although some television hosts, such as CNN’s Anderson Cooper attempted to provide context, Garfield explained that “it didn’t stop CNN, or its competitors, from showing us the same dozen burning buildings and same dozen burning cars for hours and hours, leaving the impression of a whole town consumed in an orgy of arson.”

Garfield explained that the vast majority of the Ferguson area remained peaceful after the grand jury announcement. However, *Baltimore Sun* television critic David Zurawik told Garfield during an interview that cable news organizations deserved some credit for their coverage of the protests. “Cable was there. Cable bore witness to [the protests],” Zurawik said. “You know, the networks didn’t. So give [cable news outlets] credit for that. They were there. Most of them committed major resources. They had the cameras there, and the cameras showed us a lot.” Zurawik also commended Cooper for his efforts at providing effective reporting throughout the evening by consistently asking correspondents to provide contextual information about their reporting.

In contrast, *Slate* senior writer Josh Voorhees criticized CNN’s coverage of the Ferguson protests in a November 25 post, noting that the cable channel’s reporters focused on talking about themselves. “On-camera interviews with protesters or community leaders were scarce at best, as was confirmation of many of the rumors that were mentioned on air, ranging from anecdotes about gunshots to one about a protester reportedly having a heart attack,” Voorhees wrote. “In their stead were a half-dozen CNN reporters wandering the streets, recounting what was personally happening to them and their colleagues. Among the many exchanges between the CNN contributors was Van Jones and Don Lemon talking about the latter’s gas mask not being on tight enough, and reporters warning other reporters to stay safe. Jake Tapper, clad in a CNN jacket, narrated as he walked toward a flaming trashcan to confirm that it was, in fact, a flaming trashcan.”

In a December 4 post for the *Gateway Journalism Review*, Terry Ganey criticized national media coverage of Ferguson more broadly. He argued that news organization accounts since Brown’s death on August 9 focused more on reporting a compelling narrative rather than factual news. “Journalists are supposed [to be] unbiased and blind to their own prejudices. They are required to be guided by facts,” Ganey wrote. “But in the case of the death of Michael Brown, it seemed as though the view of many journalists was that the police officer would have to prove he was innocent.”

Ganey noted that the news organizations focusing on such a narrative created expectations for viewers and readers that Wilson would be indicted, which ultimately never occurred. “The problem with the narrative was that it failed to take into account the facts of the case, and how the law authorizes a police officer to use lethal force in certain circumstances,” Ganey wrote. “In the end, after listening to some 60 witnesses, the grand jury concluded that Darren Wilson acted legally within his authority and did what many other police officers would do in the same circumstances.”

However, Ganey argued that the focus of national attention on Brown’s death had raised important points about distrust between the black community and the police, focused on discussions about the economic struggles of African Americans, and prompted Missouri Governor Jay Nixon to create a commission that will study “the root causes of Michael Brown’s death.” But Ganey suggested that national news organizations will ignore these important developments in the future. “Since the national media has moved on, the commission’s work will be explained and covered by local reporters,” Ganey wrote. “On Facebook, Lisa Eisenhauer, a [Post-Dispatch] editor, posted that long after the live trucks and celebrity anchors have pulled out, the newspaper will be telling the world what happened and why because ‘this is our community.’”

**Casey Carmody**

**SILHA BULLETIN Editor**
Federal Investigators’ Deceptive Use of Media Raises Concerns

Recent Drug Enforcement Agency (DEA) and Federal Bureau of Investigation (FBI) actions have raised concerns regarding undercover operations on the Internet. In one case, a DEA agent used information gathered from an arrestee’s cell phone to create a Facebook page for investigative purposes. In another situation, FBI officials posed as Associated Press (AP) journalists and created a fake news story in order to track a suspect.

**DEA Uses Woman’s Information to Create Fake Facebook Page for Investigation**

On Oct. 7, 2014, The Washington Post reported that the Justice Department said that it will review federal law enforcement practices regarding the use of fake social media profiles following an incident in which a federal agent used a woman’s photographs to create a Facebook account under her name as part of a drug investigation. Sondra Arquiett of Watertown, N.Y., sued the Drug Enforcement Administration (DEA), alleging intentional infliction of emotional distress and that the agent’s actions deprived her of several Constitutional amendments. Arquiett v. U.S., Timothy Sinnigen, 7:13-cv-752 (N.D.N.Y. 2014).

In her complaint, Arquiett contended that her pictures were retrieved from her cellphone after she was arrested in July 2010 on drug charges. During the arrest, law enforcement agents seized Arquiett’s cell phone, among other personal items. A month later, Timothy Sinnigen, a DEA agent, used personal information from Arquiett’s phone to create a Facebook account in her name as a way to identify other suspects.

The Post reported that U.S. Attorney Richard S. Hartunian explained in court papers that Sinnigen had used Arquiett’s information to create a Fakebook profile page, falsely posed as her and posted images from her phone on the page. Sinnigen also admitted that he had used the account to send a “friend request” to a wanted fugitive. However, Hartunian argued that Arquiett “implicitly consented by granting access to the information stored in her cellphone and by consenting to the use of that information to aid in … ongoing criminal investigations,” according to the Post.

Arquiett argued in her complaint that she suffered “fear and great emotional distress.” She also claimed that she was put in danger because Sinnigen’s fake Facebook page made some people think that she was willfully cooperating in Sinnigen’s drug investigation. The page had several photos of Arquiett, including one showing her in a bra and underwear. Sinnigen also posted photographs of her son and niece, who are both minors. According to an October 8 story in the Syracuse, N.Y. Post-Standard, Arquiett believed the page would be removed from Facebook after Sinnigen had admitted that he created the page in her name in 2010. However, the Post-Standard reported that Facebook had only removed the false profile page citing a “violation of community standards” on Oct. 7, 2014 after news broke about the case. Arquiett also did not indicate whether she had contacted Facebook prior to the page’s removal.

In an Oct. 6, 2014, BuzzFeed News article, privacy experts expressed concern with the DEA’s investigation tactics. “The technologies we have now are enabling all sorts of new uses. There are a whole bunch of new things that are possible, and we don’t have the rules for them yet.”

— Neil Richards, Professor, Washington University School of Law

“Facebook has long made clear that law enforcement authorities are subject to these policies,” Sullivan wrote. “We regard DEA’s conduct to be a knowing and serious breach of Facebook’s terms and policies.”

**FBI Agents Impersonate Associated Press to Capture Bomb-Threat Suspect**

On Oct. 28, 2014, the Seattle Times reported that the FBI acknowledged it created a fake AP news article in order to lure a suspect into downloading secret software onto his computer. According to documents the Seattle Times obtained from the Electronic Frontier Foundation (EFF), a digital rights advocacy organization, the FBI’s investigation began in the spring 2007 when Timberline High School in Lacey, Wash. received bomb threats by e-mail, on paper and on a bathroom wall, which caused the school to be evacuated. When local police were struggling to identify the source of the threats, they asked the FBI’s field office in Seattle for assistance.

FBI agents determined that if the suspect clicked on an online link that was embedded in computer malware, they could pinpoint his location. In the documents from the EFF, the agents discussed sending the suspect an e-mail in the style of the Seattle Times that contained the headline “Technology savvy student holds Timberline High School Hostage.” However, in a November 6 letter to the editor of The New York Times, FBI Director James Comey admitted that an agent, posing as a reporter for the
AP, began conversing with the suspect online. The agent asked the suspect to review a draft of an article on the bomb threats in order to be sure that the suspect was portrayed accurately. When the suspect clicked on the link to the fake draft, malware was secretly downloaded to his computer, which enabled agents to track his location and eventually arrest him. The 15-year-old suspect later pleaded guilty to making bomb threats. A 61-year-old suspect later pleaded guilty to making bomb threats. In a written statement, Frank Montoya Jr., the FBI’s special agent in charge in Seattle, had told the Seattle Times on October 28 that the technique is used “in very rare circumstances.”

Several news organizations and public figures were critical of the FBI’s investigation techniques after the Seattle Times report. On October 30, Senate Judiciary Chairman Patrick Leahy (D-Vt.), sent a letter to U.S. Attorney General Eric Holder expressing concerns about the tactic. “When law enforcement appropriates the identity of legitimate media institutions, it not only raises questions of copyright and trademark infringement but also potentially undermines the integrity and credibility of an independent press,” wrote Leahy.

On Nov. 7, 2014, Kathleen Carroll, the AP’s executive editor told The New York Times that “the [FBI] agent knew that the AP was a credible organization, or he would have not said ‘I am a reporter for The AP.’ And by using that credibility, he tarnished it.” Aly Colon, the Knight Professor in Journalism Ethics at Washington and Lee University, agreed with Ms. Carroll in the Times article. “This certainly undermines the position of all journalists who are trying to do their work as an independent source of information,” Mr. Colon said.

Press advocacy organizations condemned the FBI’s actions as well. In an October 28 post on the Freedom of the Press Foundation’s website, Executive Director Trevor Timm reflected on how frequently such tactics might be used. “The FBI and Justice Department owe some answers to news organizations and the public: How often have they impersonated news organizations to send malware to suspects? What other news organizations have they pretended to be?

And how do they prevent innocent readers from clicking on these links?” Timm asked.

In a November 7 statement, Carlos Lauria, the Committee to Protect Journalists’ senior program coordinator for the Americas, was also critical of the FBI’s decision to create fake news stories. “We are greatly concerned by the news that an FBI agent posed as a journalist and call for an immediate review of the policies that led to this action,” said Lauria. “Having federal agents pose as journalists not only threatens the credibility of a news organization — its most prized asset — but also erodes the perceived independence of the media.”

In response to objections from press organizations and the public, FBI Director Comey defended the practice in his November 6 letter to The New York Times. Comey wrote that the “technique was proper and appropriate under Justice Department and FBI guidelines at the time. Today, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate.” Comey went on to write, “every undercover operation involves ‘deception,’ which has long been a critical tool in fighting crime. The FBI’s use of such techniques is subject to close oversight, both internally and by the courts that review our work.” Comey also noted that the FBI had no intention to publish the article and that no one but the suspect ever interacted with the fake journalist or saw the falsified article.

On Nov. 10, 2014, Gary Pruitt, president and CEO of the AP, sent a letter to Attorney General Eric Holder and Comey demanding assurances from the Justice Department that the FBI will never again impersonate a member of the news media. Pruitt also demanded to know who authorized the 2007 impersonation, what process was followed for its approval, how the requirements to impersonate the media are different from seven years ago, and whether such operations are still being carried out. “In stealing our identity, the FBI tarnishes that reputation, belittles the value of the free press rights enshrined in our Constitution and endangers AP journalists and other newsgatherers around the world.”

“In stealing [the AP’s] identity, the FBI tarnishes that reputation, belittles the value of the free press rights enshrined in our Constitution, and endangers AP journalists and other newsgatherers around the world.”

— Gary Pruitt, Associated Press President and CEO

The Society of Professional Journalists (SPJ) also sent a letter to the U.S. Department of Justice on Nov. 3, 2014 stating that the FBI’s tactics hindered journalists’ ability to uphold their responsibilities as granted by the First Amendment. “The FBI’s impersonation of the Associated Press is a clear violation of the First Amendment, and its impact reaches far beyond AP. The FBI undermined the credibility of all journalists and news organizations by overextending its authority at a time when media credibility is already fragile,” said SPJ President Dana Neuts in the letter. SPJ also encouraged journalists across the country to open constructive dialogue with law enforcement officers in their communities to come to a better understanding of their respective roles in serving the public.

Sarah Wiley
Silha Research Assistant
Dissemination of Hacked Online Photos Demonstrates Challenges of Digital Privacy

Two recent high profile cases of hackers stealing photos from online databases have highlighted the difficulty of maintaining privacy in an online environment. In late August 2014, several nude photos of celebrities were posted to two online message boards, 4chan and Reddit, after hackers breached Apple’s online data storage service called iCloud. In a separate October incident, anonymous users on 4chan posted links to several photos that had been collected from a mobile app for sharing photos. Both incidents drew widespread concern and criticism from digital privacy commentators over posting stolen nude photos online and the protections for digital data.

Stolen Nude Celebrity Photos Raise Criticisms over Apple’s iCloud Services

On Aug. 31, 2014, The Washington Post reported that anonymous individuals had posted hundreds of pictures of nude celebrities on the online message boards of 4chan and Reddit. Many of the photos appeared to be taken by the celebrities themselves. Immediate questions over the authenticity of the photos dissipated when the publicist for actress Jennifer Lawrence, one of the celebrity’s whose photos was posted online, confirmed via a press release that the pictures were of Lawrence. However, many other celebrities also released statements saying that photos of them were digitally altered and not genuine pictures of themselves. The Post reported that the stolen photos included pictures of celebrities such as Kim Kardashian, Rihanna, Kate Upton, and Kirsten Dunst, among others.

The posting of the photos drew immediate widespread condemnation from several celebrities and publicists for the victims of the stolen photos. In the August 31 press release confirming the authenticity of the photos, Lawrence’s publicist wrote that the distribution of the hacked images was a “flagrant violation of privacy” and suggested that authorities would prosecute anyone who posted the photos of Lawrence. Perez Hilton, a celebrity blogger who often posts risqué pictures of celebrities, initially posted the stolen photos of Lawrence on his website only to take the images down later. In a September 1 video on his blog, Hilton apologized for posting the pictures of Lawrence. Hilton also noted that many people had told him that the posting of the photos was akin to sexual assault because celebrities did not give consent to the dissemination of their pictures. As a result, he vowed not to post any more stolen nude images.

Other celebrities also likened the stolen pictures to sexual assault. In September 1 posts on Twitter, actress Lena Dunham, who was not a target of hackers, wrote that the anonymous users posting the photos had violated the privacy of the targeted celebrities. “The way in which you share your body must be a CHOICE. Support these women and do not look at these pictures,” wrote Dunham. “Seriously, do not forget that the person who stole these pictures and leaked them is not a hacker: they’re a sex offender.”

The Post also reported on September 1 that the anonymous posters of the nude photos claimed that they had stolen the pictures appearing online from celebrities’ iCloud accounts. Initially, security experts raised concerns over the security of iCloud and were unsure how the photos may have been stolen from the celebrities’ accounts. The Post reported several ways that hackers could have stolen photos, including resetting passwords after guessing the answer to a security question, taking advantage of a flaw in a “Find My iPhone” application that would grant access to iCloud data, or hacking another person who had been privately collecting nude pictures of celebrities.

On September 4, Apple CEO Tim Cook told The Wall Street Journal that Apple was updating security policies related to its iCloud services. The updated changes included sending notifications to users when a device logs into their iCloud account for the first time, when someone attempts changing the account’s password, or when stored data is uploaded to a new device.

However, independent security researcher Ashkan Soltani told The Wall Street Journal that Apple’s security updates might not be effective because the notification “will do little to actually protect consumers’ information since it only alerts you after the fact.” Soltani also suggested that Apple had not focused on security measures that would protect user’s private information. “There’s a well-understood tension between usability and security,” Soltani told The Wall Street Journal. “More often than not, Apple chooses to err on the side of usability to make it easier for the user that gets locked out from their kid’s baby photos than to employ strong protections for the high-risk individuals.”

“More often than not, Apple chooses to err on the side of usability to make it easier for the user that gets locked out from their kid’s baby photos than to employ strong protections for the high-risk individuals.”

— Ashkan Soltani, Independent Security Researcher

Digital Photos Stolen from Snapchat Photo Collection Tool

On Oct. 10, 2014, The New York Times reported that anonymous users on 4chan had claimed that they had stolen as many as 200,000 pictures from Snapchat, a smartphone application that allows users to share photos that are automatically deleted after a short period of time. The anonymous 4chan posters claimed that they had accessed the photos by breaching the servers of Snapsave, an application that allowed users to save Snapchat photos before the image disappears. On October 12, The Guardian reported that a website had gone live where anyone could download the more than 13 gigabytes worth of stolen Snapchat content.

In the October 10 story, the Times reported that a spokesman from Snapchat confirmed in a statement that the content was not stolen from the company’s servers. “We can confirm that Snapchat’s servers were never breached and were not the source of these leaks,” the spokesman said in the statement.
Snapchatters were victimized by their use of third-party apps to send and receive Snaps, a practice that we expressly prohibit in our Terms of Use precisely because they compromise our users’ security.”

On October 17, Times reporter Mike Isaac wrote that the founders of Snapsaved had said that they initially set up their service as an experiment to prove that Snapchat photos could be saved. Users could download the Snapsaved app and enter their usernames. The app would send any of the users’ received messages on Snapchat to the Snapsaved servers. Users could then log-on to the Snapsaved website to examine the messages and photos they had received. The founders told Isaac that they had collected about 13 gigabytes worth of Snapchat messages, but they believed that the hackers had only stolen about 415 megabytes of photos and videos. After they learned about the breach, the Snapsaved founders deleted all of the content they had procured and shut down the website. The founders of Snapsaved did not reveal their identities to Isaac and explained that they had not spoken with authorities for fear of being prosecuted.

Although there were several confirmations that hackers breached data servers, Caitlyn Dewey noted in an October 13 post on The Washington Post’s Intersect blog that the stolen Snapchat images did not seem to be “making the usual rounds” online like the celebrity nude photos in September. Dewey speculated that part of the reason that the stolen photos apparently were not disseminated was due to logistics. Most of the stolen photos and video were of users doing benign activities. “[People wanting to view the content] must download massive files, and trawl through tens of thousand of cat pictures and other nonsense, in the hope of seeing a couple of 10-second nude videos,” Dewey wrote. “The obstacles won’t stop everyone, of course … But in general, it’s a lot of work. Too much work, apparently.”

Dewey also noted that the fact many of Snapchat users are under the age of 18 also might have played a big role in limiting the dissemination of images. Any nude photos of minors found in the stolen content would be considered child pornography, which could draw stiff criminal penalties for downloading the images and videos. Dewey pointed out that users on the 4chan and Reddit message boards urged others not to download the content because it might include child pornography. The users argued that if authorities viewed the dissemination of the stolen Snapchat content as child pornography trafficking, government officials would be likely to seek ways to place more stringent regulations on the Internet.

**Several Issues Brought to Light with Online Posting of Stolen Photos**

The online dissemination of stolen digital photos has raised questions about digital privacy and the role that anonymous online message boards can play in disseminating stolen digital images. In a September 22 story, The Washington Post’s Terrence McCoy explained that once images have been posted to online message boards like Reddit or 4chan, they are nearly impossible to completely remove from the Internet. “[The pictures] propagate and re-propagate faster than anyone can delete them — even when those images violate copyright laws,” McCoy wrote. He observed that as soon as moderators of Reddit deleted a message thread containing the stolen nude images, a different thread elsewhere on the web site would appear with the photos. Reddit’s administrators issued a September 7 statement on the web site contending that “[Removing the images] quickly devolved into a game of whack-a-mole. We’d execute a takedown, someone would adjust, reupload [sic], and then repeat.”

However, McCoy argued that the Reddit administrators were not taking a principled stand for privacy in deleting the celebrity photos but that concerns about the law played an important role. “Though Reddit did ultimately delete [the photos], it didn’t do [so] out of some moral code, but because there were rumors one of the celebrity photographs was taken while the subject was underage — a crime,” McCoy wrote. “The breach of privacy wasn’t a concern.”

McCoy also noted that Reddit released a separate statement on September 6 saying that the posting of the stolen images would not be likely to affect the web site’s policies. “We understand the harm that misusing our site does to the victims of this theft, and we deeply sympathize,” a Reddit administrator wrote in the statement. “Having said that, we are unlikely to make changes to our existing site.”

Other commentators have observed that the online distribution of the stolen digital photos also highlight the limits of legal remedies because of unique challenges that the Internet medium creates. Kevin C. Baltz, an attorney with Butler Snow, observed in a September 10 post on the firm’s Bizlimes Blog that victims have few remedies if hackers have stolen digital photos online. He noted that victims might be able to use the Copyright Act, 17 U.S.C. § 101 et seq., to demand that a website take down stolen images on the grounds of copyright infringement. Another option, Baltz wrote, was that victims could potentially bring an invasion of privacy suit against the hackers who stole and distributed the images.

However, Baltz predicted that suing perpetrators of online invasions of privacy would be difficult. “For the most part, a person’s ability to restrict the use of an illegally obtained photograph is limited. The subject of the photograph usually needs to know the identity of the hacker (thief) to enforce his or her rights,” Baltz wrote. “Often times, in the age of the Internet, such an identity is not easy to find. Accordingly, until more legislation is enacted to govern the content of the Internet, it may be advisable to avoid the camera or, at the very least, keep your clothes on when in front of it.”

Victims of stolen intimate photos also often face challenges with companies’ terms of service for using cloud-computing technologies when attempting to find legal remedies for the loss of private online data. In a September 2 post, Bloomberg View contributor Leonid Bershidsky explained that iCloud’s terms of service stated that users were responsible for “maintaining the confidentiality and security” of their account. The terms of service also stated that Apple was absolved of any responsibility so long as it “exercised reasonable skill and due care” in protecting a users account. “In plain English, as long as Apple can prove that it took care to prevent unauthorized access — and ... it will always be able to prove it — any hacks are the user’s fault after clicking that ‘Accept’ button,” Bershidsky wrote. He also noted that other providers of cloud-computing services, such as Google and Amazon, also had similar terms of services.

Bershidsky posited that the best solution for now was to avoid using cloud services to store personal information. “Given the share of responsibility Web giants are willing to take for our data — none, according to the service terms — it makes sense to keep personal stuff such as those nude pictures, bad poetry, love letters, etc., out of the cloud,” Bershidsky wrote. “Not being a Hollywood star or a world-class beauty provides a measure of protection, but only until someone develops an acute interest in you — stalkers, governments and other unwanted watchers obsess on the unluckiest of people every once in a while.”

CASEY CARmODY
SILHA BULLETIN EDITOR
n July 18, 2014, The Washington Post published an op-ed column by former State Department employee John Tye in which he contended that “Americans should be even more concerned” about United States government surveillance justified under Executive Order 12333 (EO 12333) than other more widely discussed authorities. The article sparked a new public debate about EO 12333, signed by President Reagan in 1981, which was initially intended to authorize foreign surveillance. The National Security Agency (NSA) stated in internal documents that EO 12333 “is the primary source of NSA’s foreign intelligence-gathering authority,” according to documents acquired by the American Civil Liberties Union (ACLU) and described in an Oct. 30, 2014 post to its blog. Tye asserted that EO 12333 empowers the government to conduct bulk surveillance of American’s domestic communications, so long as the collection occurs outside the United States. And, wrote Tye, “Unlike Section 215 [of the Patriot Act], the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons.” (For more on government surveillance under other legal justifications, see “Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone and Internet Communications” 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, and “NSA Surveillance Practices Prompt Reforms and Legal Challenges Throughout All Government Branches” in the Winter/Spring 2014 issue, and “Fallout from NSA Surveillance Continues One Year after Snowden Revelations” in the Summer 2014 issue.)

According to a Nov. 21, 2013 story by McClatchy’s Ali Watkins, EO 12333 has become a significant tool the government has used to authorize domestic surveillance because of at least two important developments: the technical advancements in communication technology and expansive interpretations of key provisions of the order. When signed in 1981, the types of “electronic” surveillance the order authorized largely consisted of telephone calls. Because a telephone call placed and received in the United States would need to be “collected” in the United States, the order’s dichotomy allowing collection only outside of United States borders largely shielded Americans from bulk collection of these communications. However, according to Tye, the technical realities of Internet communications mean that an e-mail, Internet call or other communication between two people within the United States will often pass through servers located outside the United States before reaching its domestic recipient. Thus, e-mails or other purely domestic online communications could be collected legally under the order so long as they are relayed or stored on servers outside the United States.

Tye argued that subsequent White House administrations’ interpretations of provisions of the order have also expanded the government’s information collection power. For example, under EO 12333, the government may not intentionally collect individual Americans’ communications. However, it may collect communications outside the United States in bulk, which, as discussed above, may contain both domestic and foreign communications by U.S. citizens. Under EO 12333, these “incidentally” collected communications may be retained and examined without any judicial oversight. The “minimization procedures,” which instruct agencies how to deal with improperly collected information, are approved only by executive branch officials, Tye explained.

Tye attacked the claim that the interception of Americans’ metadata could be considered “incidental.” He wrote that except for the executive-designed minimization procedures, the NSA is free to retain any information obtained via bulk collection. Once the information is collected, it can be retained for up to 5 years or more if an exception applies.

After the NSA has collected Americans’ data, it may examine it with far fewer restraints under EO 12333 than other authorities. For instance, under the government’s authority under the Foreign Intelligence Surveillance Act (FISA), an American’s information may be targeted for examination only if the government demonstrates a reasonable articulable suspicion for doing so in front of a FISA court judge. Under EO 12333, any American’s information the government has “incidentally” collected may be examined without any judicial oversight. Under FISA, the NSA may examine the metadata of individuals two “hops” from someone suspected of being a foreign agent. According to an Aug. 13, 2014 New York Times report, under EO 12333 there is no such limit, meaning any person’s information that is collected may be examined by the government through this chain of communication theory, no matter how tenuous the connection. The interpretation of 12333 to allow this targeting of Americans’ metadata is due to secret internal policy change made in 2010, according to documents leaked by NSA whistleblower Edward Snowden.

According to Tim Cushing in a Nov. 6, 2014 article for Techdirt.com, “This Executive Order is, and always has been, the go-to authority for the NSA.” Cushing explained that this is true because in addition to the more permissive collection and minimization standards under 12333 as compared to surveillance statutes like the Patriot Act and FISA, there is far less oversight required of surveillance activities justified under 12333. Minimization procedures need only be approved by the Attorney General. Senate Intelligence Committee Chair Diane Feinstein (D-Ca.) explained that her committee has not been able to “sufficiently” monitor the programs. Feinstein, who has frequently defended surveillance programs authorized by Congress, told McClatchy for a Nov. 21, 2013 article that “12333 programs are under the executive branch entirely.”

Despite the controversy and public debate over surveillance statutes, EO 12333 has received far less scrutiny. Even the President’s Review Group on Intelligence and Communication Technologies, a group designed to suggest reforms to oversight and transparency of surveillance activities, declined to explicitly reference EO 12333 in its proposals. The group’s report suggested reforms to foreign surveillance that, according to Tye’s op-ed, a member of the group later acknowledged was intended to suggest reform to EO 12333. According to a July 23, 2014 report by The Washington Post, the President’s Civil Liberties Oversight Board will be examining EO 12333 to propose reforms.

On Aug. 18, 2014, Civil Liberties Protection Officer for the Director of National Intelligence Alexander Joel published an article in Politico responding directly to many of Tye’s assertions. Although the NSA may perform bulk collection of information that includes Americans’ communications, Joel wrote, “NSA personnel may not use U.S. person ‘selection terms’ (such as names, phone numbers or email addresses) to retrieve communications from its collection under EO 12333 without a finding by the attorney general that the U.S. person is an agent of a foreign power (or in other similarly narrow circumstances)."
Order, continued from page 20

Joel also disputes Tye's claim that neither recent surveillance reforms by President Obama nor reform bills being debated in Congress would have any impact on the government's authority under EO 12333. Joel points out that Presidential Policy Directive 28, issued Jan. 27, 2014, required that collection activities "be as tailored as feasible." It also places limitations on the use of information collected in bulk, for instance requiring that the information will not "be used for the purpose of suppressing or burdening criticism or dissent."

The complex relationship between EO 12333 and other surveillance laws, combined with the lack of public knowledge about it, have made public debate complicated. The ACLU's Jameel Jaffer told The New York Times for a Aug. 13, 2014 article that debate over EO 12333 has been missing because "[i]t's a black box." In a March 25, 2014 article in the Atlantic, electronic security expert Bruce Schneier noted that EO 12333 facilitates U.S. intelligence officials' ability to give accurate but misleading answers about the government's surveillance authority. Schneier wrote that the public must "[b]e careful when someone from the intelligence community uses the caveat 'not under this program,' or 'not under this authority'; almost certainly it means that whatever it is they're denying is done under some other program or authority."

Although proposed Congressional reforms might clarify other surveillance laws, the reforms may leave the power to continue the same information collection activities intact via the powerful legal authority under EO 12333. Tye challenged readers to "[c]onsider the possibility that Section 215 collection does not represent the outer limits of collection on U.S. persons but rather is a mechanism to backfill that portion of U.S. person data that cannot be collected overseas under 12333."

— Judge Terrence L. O'Brien, U.S. Court of Appeals for the Tenth Circuit

Alex Vlides
Silha Research Assistant
Brokers' Choice, continued from page 2007, which included scenes where Clark said, “And I'm bringing these things up that disturb the hell out of them” and “I help my clients to protect their life savings from the nursing home and Medicaid seizure of their assets. See, that's scary, and it should be scary.” Dateline also supplemented the seminar footage with Hansen interviewing Minnesota Attorney General Lori Swanson, who criticized Clark's comments. In total, Dateline used clips that included a total of 112 words from Clark during the two-day seminar.

BCA and Tyrone Clark sued NBC's parent company, NBC Universal, in the United States District Court for the District of Colorado alleging several state-law claims, including defamation, trespass, fraud, and misrepresentation. BCA also alleged civil rights violations under 42 U.S.C. § 1983. BCA claimed a Fourth Amendment violation for an illegal search and seizure as well as Fourteenth Amendment violations of invasion of privacy and stigmatization. NBC Universal moved to dismiss the lawsuit for failure to state a claim and sought to stay discovery pending a district court’s ruling. BCA claimed that it needed Dateline’s unaired footage from the “Tricks of the Trade” story to substantiate its claims. However, a magistrate judge relied upon the Colorado Shield Law, Colo. Rev. Stat. §12-90-119(3), to determine that Dateline did not need to disclose its footage, which allowed discovery to be stayed. A district court judge granted NBC Universal’s motion to dismiss but gave leave to BCA to amend its complaint.

In an amended complaint, BCA claimed only defamation and violations of its civil rights under § 1983. BCA provided recordings it had created during a separate “Annuity University” seminar from March 2007 to demonstrate that Dateline’s segment had taken Clark’s statements out of context. BCA also asked the district court to compel discovery for the unaired footage of Dateline’s hidden-camera footage from the seminar. NBC Universal objected, claiming that Colorado’s shield law protected the unedited recordings, and filed a motion to dismiss. The magistrate judge again denied BCA’s motion for discovery based on a common law journalist’s privilege and the Colorado Shield law, noting that BCA failed to show that relevant information was unavailable from sources other than the Dateline footage. A district judge affirmed the magistrate’s order to dismiss BCA’s motion to compel discovery, and later dismissed all of BCA's claims with prejudice. Brokers’ Choice of America, Inc. v. NBC Universal, Inc., 2011 WL 97236 (D.Colo. 2011).

In its appeal to the U.S. Court of Appeals for the Tenth Circuit, BCA claimed that the district court erred in four ways: first, the district court did not accept BCA’s allegations as true for the purposes of considering the motion to dismiss; second, the district court did not make the appropriate determinations of fact; third, the district court should have found that BCA provided sufficient support for its § 1983 claims; fourth, the district court improperly applied the Colorado shield law. In a unanimous decision, a three-judge panel affirmed the district court’s dismissal of BCA’s claims of civil rights violations.

However, the panel reversed the dismissal of the defamation claims and remanded the case to the district court for further proceedings. In the panel’s opinion, Circuit Judge Terrence L. O’Brien first examined BCA’s defamation claims to determine whether the district court properly dismissed the lawsuit. BCA claimed Dateline’s selective footage of the seminar took Clark’s comments out of context to suggest that Clark was teaching insurance agents how to deceive senior citizens. O’Brien noted that NBC Universal acknowledged that the substance of its segment could be defamatory, but argued that all of Clark’s statements were substantially true. After examining each individual statement that Dateline aired from Clark’s seminar, the lower court had dismissed the defamation claim because it agreed with NBC Universal.

However, the Tenth Circuit panel found that “in a case where a plaintiff asserts a statement that could be defamatory, a defendant’s statement must be evaluated by considering the overall context in which it was made.” O’Brien wrote that a court should not have considered Clark’s statements in isolation to determine whether they were substantially true. Rather, the district court needed to examine how Dateline portrayed the “gist” of Clark’s statements and his seminars. The panel noted that Clark could not deny the accuracy of individual statements that Dateline attributed to him. “However, the program not only accused Clark of using scare tactics. The ‘gist’ or ‘sting’ was his calculated use of these tactics to sell inappropriate products to seniors,” wrote O’Brien. Clark had used the recording of his March seminar to argue that the selectively aired Dateline footage created an overall false impression of how he teaches insurance agents to approach discussions with senior citizens about annuity products. “Instead of promoting predatory tactics, BCA’s complaint alleged facts supporting its position that Annuity University provided a straightforward discussion of the pros and cons of annuity products and endorsed ethical (although scary) marketing,” wrote O’Brien. The Tenth Circuit panel reversed the district court’s dismissal of the defamation claim because BCA had provided enough of a factual basis to state a plausible complaint.

Next, O’Brien observed that the reversal of the district court’s decision would typically resolve the issue about whether discovery proceedings could commence. “However, this case is anything but normal,” O’Brien wrote. “Dateline claims it need not disclose its news material merely because BCA plausibly alleged a defamation claim. Rather it argues, under Colorado’s newsperson privilege [interpreted by state court precedent], ... BCA’s complaint must also sufficiently plead facts showing probable falsity before any disclosure is required.”

The panel noted that the Colorado shield law provided a qualified privilege that could be defeated if a party seeking information could prove that a news organization’s information was directly relevant, unavailable through alternative means, and the interest of the party seeking the information outweighed the First Amendment interests of the news organization and the public. O’Brien concluded that BCA had easily met the first two prongs of the test to overturn the privilege found in the Colorado statute. Neither party disputed that Dateline’s footage was directly relevant to the case. The panel also found that BCA’s recording of a March seminar was not an alternative to the information in Dateline’s October footage because BCA alleged that...
what Clark said at the March and October seminars was different. Information about the October seminar was available only through Dateline's footage.

As for the third prong of the state statute's qualified privilege test, the panel wrote that the Colorado Supreme Court had previously found that a showing of “probable falsity” should be considered in balancing the interests of plaintiffs and news organizations before revealing the identity of a confidential source or confidential information. NBC Universal argued that it could refuse to disclose Dateline's unedited footage until BCA proved the “probable falsity” of the segment's reports. However, the Tenth Circuit panel rejected NBC Universal's argument because the unaired footage of the seminar did not involve a confidential source or confidential information, which was the only context in which the “probable falsity” requirement applied. O'Brien wrote that the identities of who recorded Clark was not confidential nor did BCA seek information about the confidential information of the editorial process. As a result, NBC Universal could not rely on “probable falsity” arguments. "Without the probable falsity crutch, the equitable balance between 'important interests' and 'chilling effect' tip dramatically in favor of BCA," O'Brien wrote. "The object of discovery — the original footage — is the best and perhaps only evidence from which a fact-finder can determine whether Dateline's portrayal of the substance of what occurred at Annuity University cast Clark's teachings in such a way as to leave a false impression." The three-judge panel ruled that the Colorado shield law's qualified test had been overcome and disclosure of the unaired footage was warranted.

O'Brien then turned to BCA's violation of civil rights claims. Claims of civil rights violations under § 1983 apply only to the actions of the government, not private actors. However, if a private actor is participating in a joint endeavor with the government, the private actor could be held liable for a violation of civil rights. O'Brien wrote that in order to determine whether the actions of the private actor and the government were a joint endeavor, the court needs to examine "whether the government knew of and acquiesced in the private person's intrusive conduct" and "whether the party performing the search intended to assist law enforcement efforts or to further his own ends." The appellate court found that Alabama officials and Dateline had engaged in a joint effort to investigate Clark and BCA. "Knowing the producers would use hidden cameras to record the seminar, Alabama officials supplied the Dateline producers with false credentials that they could not otherwise obtain," O'Brien wrote. "Dateline agreed to share the information it obtained with the Alabama officials. Quid pro quo."

However, the key question was whether the arrangement between Dateline and Alabama authorities had resulted in a civil rights violation. The court found that Dateline's actions of posing as insurance agents and secretly recording the seminar did not violate any civil rights. Rather, O'Brien noted that Dateline was simply using typical investigative techniques of law enforcement officials. "Dateline misrepresented its employees as insurance agents, implicitly denying that they were agents of Alabama investigatory agencies," O'Brien wrote. "But, there were no coercive acts, only implicit lies about their actual identity and purpose. We see that as no different from an undercover police officer misrepresenting himself as a drug dealer."

O'Brien went on to dismiss BCA's argument that it had not given consent for recordings of the seminar, finding that Clark had made his statements in a public setting, which meant he should have had no Fourth Amendment expectations of privacy. O'Brien also noted that there was no instance of the government using coercive power to allow Dateline to record the seminar. "No government actors were present and the Dateline operatives neither represented themselves to be government officers nor demanded entry on behalf of the government," O'Brien wrote. "At worst, it is a classic case of government agents sending willing and available operatives to obtain information freely revealed to those operatives." The three-judge panel speculated that Dateline may have violated state tort law for invasion of privacy, but its actions did not amount to a Fourth Amendment civil rights violation. The district court was correct in its judgment to dismiss BCA's illegal search and seizure claim, the panel ruled.

The appellate court concluded by addressing BCA's claims for stigmatization under the Fourteenth Amendment violations for invasion of privacy and stigmatization. On the invasion of privacy claim, O'Brien wrote that the federal Constitution protects only against disclosure of highly personal matters. The court dismissed the alleged civil rights violation because the BCA did not claim that Dateline's segment disclosed any personal information. O'Brien also explained that BCA's claims of stigmatization would require allegations that government officials had assisted in the editing of Dateline's segment to harm the reputation of Clark and BCA. However, O'Brien observed that BCA provided facts that only alleged an Alabama law enforcement official, Joe Borg, appeared in an interview and that Borg's friend appeared during the Dateline's "sting" operation. The Tenth Circuit panel dismissed BCA's stigmatization claim on the grounds that the facts did not provide a sufficient basis to possibly prove a civil rights violation.

In a July 9, 2014 post on Hollywood, Esq., The Hollywood Reporter's law blog analyzing entertainment and law, senior editor Eriq Gardner noted that Brokers' Choice of America v. NBC Universal was unusual because the case raised a variety of issues related to media law topics, including journalist's privilege, defamation, and journalists working in conjunction with law enforcement officials for an investigation. "For a sly ploy where journalists (including Hansen, famous for "To Catch a Predator") doubled as police informants, NBC will have to face a defamation claim and maybe others like trespass (if the statute of limitations hasn’t passed), but it’s off the hook for trampling on the U.S. Constitution," wrote Gardner. "(For more on Hansen and "To Catch a Predator," see “To Catch a Predator” Criticized after Suspect’s Suicide" in the Winter 2007 issue of the Silha Bulletin.)"

On July 15, 2014, Carter Ledyard & Milburn LLP, the law firm representing BCA and Clark, issued a statement on its website applauding the appellate court's decision. "The 10th Circuit Court’s decision in [Brokers’ Choice of Am. v. NBC Universal] places our clients’ libel case back on the docket with clear guidance about how to proceed in accordance with its rulings," the firm wrote in the statement. "It rejects the common media defense tactics of filing a motion to dismiss designed to place evidentiary burdens of proof on libel plaintiffs at the pleading stage, coupling the motion with an application for a stay of all discovery which, if granted as it was here, stops the case while briefs are filed, hearings held, decisions considered, and months and even years pass."

However, The Denver Post reported on July 15 that NBC News spokeswoman Monica Lee told the newspaper in a statement that the Tenth Circuit's decision was not a significant setback. “Nothing in last week’s ruling stated that the Dateline segment was inaccurate,” Lee said in the statement. “We stand by our reporting.”

As the Bulletin went to press, further proceedings in the case at the United States District Court for the District of Colorado had not yet commenced.

CASEY CARMODY
SILHA BULLETIN EDITOR
Law Enforcement, Tech Companies Clash on Built-In Privacy Features

On Sept. 17, 2014, Apple announced that its newest mobile operating system would make it technically impossible to comply with law enforcement or intelligence agency warrants for password-protected user data. Google announced the following day that its new Android mobile operating system would similarly encrypt user information by default.

These intentionally-designed limitations responded to increasing consumer demand for truly private communication after several years of scandals and leaks related to U.S. government surveillance. Law enforcement and intelligence officials responded with biting criticism of the technology companies, arguing that the changes would make their jobs more difficult and make the country less safe. Nonetheless, these changes may signal the most substantive consumer-focused response to fears of government surveillance.

Under the “Government Information Requests” section of Apple’s new privacy policy, available at https://www.apple.com/privacy/government-information-requests/, password-protected “personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders” will be encryption-protected by default. Users will be able to set this password independently, and, according to the language of the policy, “Apple cannot bypass [the] passcode and therefore cannot access this data.” Because Apple says it will not build a technical backdoor into its new operating system allowing the company to bypass the encrypted password, “it’s not technically feasible for [Apple] to respond to government warrants for the extraction of this data.”

According to a September 18 story in The Washington Post, Google’s Android system’s default settings will encrypt all data. Google Spokeswoman Niki Christoff told the Post that “[f]or over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement.” Although Apple’s changes will be available to both new and old Apple devices that install the new iOS 8 operating system, Google’s changes making data encryption a default setting are only on new Android products. However, the Post noted that users of existing Androids can simply activate the encryption options that are available.

Law enforcement officials criticized the tech companies for changing their policies to emphasize data encryption. In an October 16 speech at the Brookings Institution, Federal Bureau of Investigation (FBI) Director James Comey argued that encryption changes would impede law enforcement investigations already “struggling to keep up” with criminals’ use of technology. This type of encryption, Comey said, is like “[a] safe that can’t be cracked” which “will have very serious consequences for law enforcement and national security agencies at all levels.” Comey emphasized the FBI’s fear of criminal investigations “going dark,” meaning that suspects might use communication or data storage methods that are inaccessible to law enforcement. Prominent city police chiefs also criticized the changes. Washington, D.C. Metropolitan Police Chief Cathy Lanier said criminals would make use of the encrypted phones. “We are going to lose a lot of investigative opportunities,” she told Bloomberg News in a Sept. 29, 2014 article.

Civil liberties advocates have applauded the changes as a positive, market-based response to protect user privacy. “Apple’s decision is simply setting the privacy standard for mobile devices in the same place as non-mobile ones,” wrote Electronic Frontier Foundation Staff Technologist Jeremy Gillula in a Oct. 10, 2014 blog post on the organization’s web site. “We applauded Apple and Google for standing up for their customers’ security even if law enforcement doesn’t like it.”

Others disputed the law enforcement officials’ claims that the default encryption settings mean that police are in a worse position to investigate crimes. Kevin Poulsen wrote in an Oct. 8, 2014 article for Wired, “On balance, smartphones have been a gold mine to police, and the mild correction imposed by serious [encryption] will still leave the cops leaps and bounds ahead of where they were [before smartphones].”

In an October 6 post on the blog Schneier On Security, electronic security expert Bruce Schneier argued that law enforcement’s criticisms of tech companies’ changes to data encryption settings on operating systems that focused solely on the possibility of blocking lawful warrants were misguided. He noted that encryption aims to prevent any outside incursion into a user’s information. “You can’t build a backdoor that only the good guys can walk through,” Schneier wrote. “Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You’re either vulnerable to eavesdropping by any of them, or you’re secure from eavesdropping from all of them.”

Many commentators have interpreted the companies’ changes simply as rational responses to demand for more private communication. Carl Howe, a mobile data analyst, told Bloomberg News for a Sept. 29, 2014 report, “They want to provide that feeling of privacy. Otherwise, people won’t use [the devices].” But critics have viewed this motivation as problematic. In an October 16 speech at the Manhattan Institute, New York Police Department Chief William Bratton said, “It is outrageous that in the interest of making money, [Apple and Google] are thwarting security and crime fighting.”

Experts agree that the new default settings will affect U.S. consumer, but other technology industry observers see the changes as particularly geared towards staying viable in the international marketplace. As the scope of the U.S. government’s data collection outside of the United States and the close relationship the government maintains with many communications company has become more widely known, fears of surveillance through American-made products has increased. If the American government imposes surveillance loopholes, wrote Wired’s Poulsen, “foreign technology companies would gain a competitive advantage over the US, since they’d have no obligation to weaken their [encryption].” Because technology consumers outside the U.S. lack many basic legal safeguards from U.S. government data collection, a technical safeguard provides an appealing solution.

Although the privacy changes have been largely framed as a response to National Security Agency surveillance programs, some believe that the changes are addressing a problem separate from the concerns that spawned them. George Washington University Law Professor and Fourth Amendment expert Orin Kerr told The Washington Post in a Sept. 25, 2014 article that “[t]he outrage is directed at warrantless mass surveillance, Apple, continued on page 25
29th Annual Silha Lecture Examines the Right to Access Government Information in the Wake of National Security and Privacy Concerns

First Amendment attorney David A. Schulz argued that “determining the proper level of government transparency is critical to how we proceed as a nation,” during the 29th annual Silha Lecture. Schulz’s lecture, “See No Evil: Why We Need a New Approach to Government Transparency,” took place on Oct. 16, 2014 at the University of Minnesota’s Cowles Auditorium with 200 people in attendance. Schulz, a partner at Levine Sullivan Koch & Schulz LLP and counsel to the Associated Press, The New York Times, and The Guardian, discussed how claims of national security and personal privacy have diminished the public’s ability to access government information and have led to more government secrecy.

Schulz began the lecture by addressing the classified National Security Agency (NSA) documents provided by Edward Snowden to one of his clients, The Guardian. In June 2013, The Guardian published information about classified documents that Snowden gave to journalist Glenn Greenwald. The disclosures and subsequent stories revealed a massive system of U.S. government surveillance of Americans and foreigners. According to Schulz, the Snowden disclosures highlighted two major trends driving the government to withhold information from the public: privacy and national security, especially in the aftermath of September 11.

“Snowden pulled back the veil on activities that the government had been doing that we knew very little about and which the government worked hard to keep secret,” said Schulz. Lack of government transparency is a real problem, Schulz explained, because Americans cannot engage in informed debate about important issues when they do not have access government information, limiting the democratic process.

Obtaining access to records is the main way the public can determine “what the government is up to,” Schulz said. According to Schulz, the two legal foundations for the public’s right to access government information are a statutory right found in the Freedom of Information Act and state open record laws, and a constitutional right found in the First Amendment. However, Schulz noted that government officials and judges have often cited privacy and national security concerns to limit the right of the public to access information.

Schulz provided an overview of the statutory right of access established by the Freedom of Information Act (FOIA), 5 U.S.C. § 552, signed into law in 1966. FOIA created three important principles, according to Schulz. First, the act created a presumption of openness that the public has a right to see federal agency records. Second, an agency can only refuse to release records that fall under nine exemptions outlined in the act, and the agency must prove why a specific exemption applied. Third, the act articulated the right to challenge an agency’s decision to withhold records in a court of law.

Schulz explained how the Constitutional right of access to information was first established by the Supreme Court in 1980. In Richmond Newspapers v. Virginia, 448 U.S. 555 (1980), the Court held that the public’s right to attend criminal trials was embedded in the First Amendment as implied by the structure of the Constitution. The Court reasoned that there must be some level of access to government information and proceedings in order for the other expressed rights of the First Amendment, such as the right of speech and the right of assembly, to be fully realized. The Court developed a two-part test in Press-Enterprise Co. v. Superior Court, 478 U.S. 555 (1986) to determine when the right of access applied or could be overcome. The test held that a right of

Apple, continued from page 24

and this is a very different context. It’s searching a device with a warrant.”

Law enforcement authorities will still be able to acquire the information on encrypted cell phones. Many smartphone users backup their data on a cloud storage service in a variety of ways. Apple’s iCloud service, for instance, is not encrypted and law enforcement officials could obtain the information in a user’s iCloud account from Apple with a warrant. In a Sept. 17, 2014 post to his blog Zdziarski.com, engineer Jonathan Zdziarski explained that if police acquire a password protected phone, there are tools that will reveal a significant amount of user information despite the phone being locked and password protected. Even on Apple’s new iOS 8 operating system, programs can extract photos, videos and third party application data without the password. Police may also be able to force users to enter their password. This tactic is the subject of legal controversy, because some courts have found that forcing suspects to reveal their own passwords violates the Fifth Amendment guarantee against compelled self-incrimination. American Civil Liberties Union Principal Technologist Christopher Soghoian told The Wall Street Journal on September 22 that federal and national security officials will have the resources to use other tools, but the encryption changes could disadvantage local law enforcement. “It’s not so much a problem for ‘Big Brother,’ but a problem for ‘Little Brother,’” Soghoian said.

— David A. Schulz, 29th Annual Silha Lecturer

Alex Vlides
Silha Research Assistant
Lecture, continued from page 25

access exists in situations when government proceedings and information have traditionally been available to the public and when public access plays a "significant positive role" in the functioning of government.

Schulz described how privacy and national security concerns have limited the public’s right of access found in FOIA and the U.S. Constitution. Courts have narrowed the scope of the access right under FOIA by broadly interpreting the several exemptions found in the law, Schulz explained. In particular, Schulz focused on the Supreme Court’s decisions in Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989) and National Archives and Records Administration v. Favish, 541 U.S. 157 (2004). In both cases, the Court broadly interpreted privacy exemptions under FOIA, which stated that government information can be withheld in circumstances when its disclosure would create an unwarranted invasion of personal privacy. The Court had to determine whether the public interest outweighed that risk. Schulz explained that under both cases, the Court narrowly construed the public interest in disclosure of the records while finding a broad privacy interest. In addition, Schulz explained that lower courts have read the majority opinions in Reporters Committee and Favish as shifting the burden of proof for access to information. Previously, the government needed to provide justification for why records should be withheld. Now, requesters of information need to explain why the information should be released, Schulz explained. (For more on the Favish decision, see “Citing Family Members’ Privacy, Supreme Court Allows Government to Withhold Foster Photos” in the Spring 2004 issue of the Silha Bulletin.)

Schulz shared recent examples of cases highlighting the problem of construing the privacy interest too broadly. For example, in Associated Press v. Department of Justice, 554 F. 3d 274 (2d Cir. 2009), the Associated Press submitted a FOIA request for names of Guantanamo Bay detainees who were alleging abuse from both other detainees and prison guards. The government refused to release the names, arguing that such a disclosure would harm the detainee’s privacy interest. The United States Court of Appeals for the Second Circuit agreed with the government. That court cited Favish in holding that in order for requests seeking information that might

highlight government misconduct to be successful, the requester must present some sort of evidence of wrongdoing as a pre-requisite to overcome privacy concerns found in FOIA exemptions. These decisions have “turned FOIA on its head” and have led to government secrecy, Schulz contended.

Courts have also often justified non-disclosure under the national security exemption in FOIA, which states that records can be withheld “that are specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy.” 5 U.S.C § 552(b)(1). Schulz explained that broadly interpreting national security interests in the aftermath of September 11 has created lasting restrictions on disclosure under FOIA. Schulz argued that courts often lack “institutional confidence” because they often defer to the executive branch’s arguments that national security would be harmed in order to withhold information. “Courts feel like they are unable to differentiate between legitimate and realistic concerns about national security and public safety and thus aren’t able to separate those from the speculative, the implausible, or the openly illogical excuses we too often get from agencies,” Schulz said.

Schulz provided examples when courts have been struggling with balancing the constitutional right of access and national security concerns. Schulz highlighted recent legal debates about whether the Constitutional right of the public to access criminal proceedings applies to the military tribunals taking place in Guantanamo Bay. Issues also arise when classified information is used in trial and whether a constitutional right of access to the courts allows the public to view the classified information. In particular, Schulz highlighted a recent example of a court finding a constitutional access right to classified information in Dhiab v. Obama, 1:05-cv-01457-GK (D.D.C. 2014), over the government’s objections. Abu Wa’el Dhiab, a Guantanamo Bay prisoner, was force fed while attempting a hunger strike in 2012. Dhiab claimed that the force-feeding violated international law as well as the United States Constitution as it constituted a form of cruel and unusual punishment. On October 3, 2014, D.C. District Court Judge Gladys Kessler ordered the release of 28 classified videotapes showing the force-feedings despite the government’s objections of national security. In analyzing whether the government’s arguments to restrict access to the tapes were compelling enough to overcome the established constitutional access right, Kessler concluded that “the fact that the Government has unilaterally deemed information classified is not sufficient to defeat the public’s right [of access].” Schulz praised Kessler’s approach in balancing the national security concerns and the public’s right to access information.

“I’m not suggesting that there are not legitimate national security concerns, but what I am saying is that the reflexive impulse that swept the nation after September 11 to withhold any information that could possibly be used by terrorists is today denying the public basic information it needs to function if our democracy is going to function,” said Schulz.

Schulz concluded the lecture with a pertinent paraphrase from Ben Franklin, “those who would sacrifice liberty in the interests of security will have neither, and I fear that is where we are today,” Schulz said.

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

— David A. Schulz, 29th Annual Silha Lecturer

“Courts feel like they are unable to differentiate between legitimate and realistic concerns about national security and public safety and thus aren’t able to separate those from the speculative, the implausible, or the openly illogical excuses we too often get from agencies.”

SARAH WILEY
SILHA RESEARCH ASSISTANT
Silha Center Co-Sponsors Forum on Ethics of “Pointergate” Broadcast

On Dec. 8, 2014, the Minnesota Pro Chapter of the Society of Professional Journalists (SPJ), in collaboration with the Twin Cities Chapters of the National Association of Black Journalist and the Asian American Journalists Association, the Minneapolis/St. Paul Business Journal, the Silha Center for the Study of Media Ethics and Law, and the Minnesota Journalism Center, hosted a forum on the ethics of a news story prepared by Twin Cities ABC-affiliate KSTP, which was dubbed “Pointergate” and received national criticism.

“Pointergate” began on Nov. 6, 2014, when KSTP aired the story during an evening broadcast of “5 Eyewitness News.” The broadcast reported a picture of Minneapolis Mayor Betsy Hodges and an African-American man, whose face was blurred, smiling and pointing at each other, a gesture which KSTP reported Jay Kolls described as “a known gang sign.” Kolls did not identify the man in the picture by name, but described him as a “twice-convicted felon for drug selling and possession and illegal possession of a firearm.” KSTP reported that law enforcement officials had found the photograph on the man’s Facebook page during investigative work. Kolls also interviewed on camera retired Minneapolis police officer Michael Quinn, who formerly managed the department’s Internal Affairs Unit. Quinn told KSTP that the photo was “disappointing because it puts police officers at risk.” Kolls reported that Hodges declined to be interviewed about the picture, but her office stated that the gesture was not a gang sign. Nevertheless, Quinn told KSTP, “[Hodges] can’t be that naive. She is legitimizing gangs who are killing our children in Minneapolis and I just can’t believe it. It hurts.” KSTP’s original broadcast is available online at http://kstp.com/news/stories/S3612199.shtml.

After the story aired, the station faced a public backlash on social media that included questions about whether the story was newsworthy, and whether KSTP’s reporting was intentionally taking the picture out of context, as well as accusations of racism. Many of the criticisms appeared on Twitter, with commentators using “#Pointergate” to organize their comments. In response to the criticism, KSTP ran a follow-up story on November 7 that again quoted Quinn, who said that the mayor’s gesture in the photo sent a troubling message. “[The hand signs] have real meaning on the street and gangs take them seriously and people have died for simply flashing a gang sign,” Quinn told KSTP. “This is serious and can lead to serious consequences.”

Subsequent reporting by other news organizations sought to provide greater context for KSTP’s reports. Other news organizations identified the man in the picture as Navell Gordon, who had been previously convicted of various drug and firearm related crimes but denied having any association with gangs. Additional reports noted that Gordon was working as an organizer with Neighborhoods Organizing for Change (NOC), a nonprofit organization focusing on social issues. The picture of Hodges and Gordon was taken during a NOC get-out-the-vote event. Reports also indicated that Minneapolis Police Chief Janéé Harteau had been present when the photograph had been taken, but was standing just out of frame. However, KSTP continued to stand by its reporting of the story in another November 13 story.

In a November 19 blog post on the organization’s web site, SPJ’s Minnesota Pro Chapter President Chris Newmarker called on KSTP to “disavow the story,” saying the it was “fundamentally flawed and based on a faulty premise that a silly gesture made by the mayor ... amounted to a gang sign,” and that describing Gordon merely as a convicted felon “creates the appearance that the reporter is a mouthpiece for members of the police force who have an axe to grind with the mayor’s office.” Although Newmarker acknowledged that KSTP and Kolls had made “invaluable contributions to the local journalism community through years of solid reporting and good journalism,” this particular story “was deeply flawed.” The SPJ statement is available online at http://www.mnspj.org/2014/11/19/spj-calls-on-kstp-to-disavow-pointergate-story.

On November 26, Hubbard Broadcasting Chairman and CEO Stanley S. Hubbard, owner of KSTP, responded to criticisms and defended Kolls’ story in a letter to Jonathan Kealing, SPJ’s Minnesota Pro Chapter’s President-elect and news editor for PRL.org. Hubbard contended that Kolls had been informed that police officials were concerned that the Mayor’s used of a gesture associated with the gang. “Stick Up Boys,” could create serious problems for police and the public. Hubbard emphasized that neither Hodges nor Gordon agreed to be interviewed when requested.

The December 8 forum, held at the University of Minnesota’s Cowles Auditorium, included panelists Kealing; Duchesne Drew, managing editor for operations at the Minneapolis Star Tribune; Anthony Newby, NOC’s executive director; and Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law. Hodges, Kolls and Hubbard were invited to join the forum as panelists, but none took part in the event.

During the panel discussion, Newby characterized KSTP’s original story as “non-existent” with “no substance” and exhibiting a “pre-determined view.” The follow up story, Newby said, was an example of a news organization “digging their heels in.”

Drew said that KSTP had called the mayor’s office to ask whether the mayor had been photographed making a gang sign but was told that she had not. At that point, Drew said, there was no longer a story of any substance, yet the station decided to run it anyway. Once it became apparent that running the story had been a mistake, Drew argued that it would have been appropriate for KSTP to apologize. “We [journalists] make mistakes all the time,” Drew said. “But the point is to follow through on making it right. That tendency should be in the DNA of all news organizations.”

Asked whether news organizations should have policies in place to respond to public criticism, Kirtley replied that not only would such policies be useful, but that news organizations ought to proactively engage with the public and invite their participation in the news reporting and gathering process and express its concerns. She suggested that news organizations should listen to the public’s concerns carefully. Enacting such policies increases a news organization’s credibility, she said. Kirtley noted that although people often want a single, simple narrative, the approach can oversimplify complex issues and compartmentalize people. “News organizations need to take the time and resources to tell complicated stories and tell them well,” she said.

A video of the panel discussion is available online at http://theuptake.org/live-video-post/journalists-discuss-pointergate/.

ELAINE HARGROVE
SILHA CENTER STAFF
Silha Research Assistantships

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

The number of available Research Assistantships varies from year to year. Appointments are competitive. A strong academic record and excellent legal research and writing skills are required. Journalism experience is strongly preferred. Applications for Summer 2015 and for the 2015-16 academic year will be due in March 2015.

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