THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | FALL 2013

Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms

Months after the June 2013 leaks by former U.S. National Security Agency (NSA) contractor Edward Snowden revealed NSA surveillance practices to the world, government responses to the leaks have spurred domestic and international efforts at reforming data security and have led to contentious international relations. Alan Rusbridger, editor of the *Guardian*, told the British Parliament on Dec. 3, 2013 that less than one percent of Snowden's leaked documents have been published by the newspaper. Fresh reporting on the leaks has brought new information to light on the NSA's domestic and international spying techniques. The reports have sparked disquiet from the boardrooms of multinational corporations to the halls of foreign governments to streets full of protestors around the world. The NSA was dealt its first major legal blow when a federal judge ruled in December 2013 that the agency's telephony metadata collection program was unconstitutional. (For more information on Snowden's leaked information about the NSA, see "Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone and Internet Communication" in the Summer 2013 issue of the Silha *Bulletin*.)

Leaks Reveal NSA Targeted Top Encryption Techniques

On Sept. 5, 2013, reporters for ProPublica and *The New York Times* reported that the NSA was "winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age." Encryption techniques are methods of digital encoding that are used to protect sensitive information transmitted over the Internet. When a message is encrypted, it is formatted into an indecipherable code that, in theory, can only be decoded by the intended recipient. The NSA has made strong efforts to crack the most commonly used encryptions in the United States. According to the ProPublica article, these include encryptions used in sending emails and securing transactions in online commerce. Also targeted are mobile Internet encryption tools such as Secure Socket Layers (SSL) and Virtual Private Networks (VPN), as well as the encryption tools used to protect fourth generation (4G) smartphones.

According to documents leaked by Snowden, the NSA invested billions of dollars over the last two decades developing the highly classified program called "BULLRUN." The program worked to gather encrypted information in three ways: by investing in massive supercomputers and the world's most advanced cryptoanalytics to decode encrypted materials; by identifying and hacking into targeted computers to obtain messages before they were encrypted; and by using the NSA's influence as the "world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world." This also includes efforts to access protected traffic on some of the busiest sites on the Internet, including, according to the documents, "'new access opportunities' into Google's systems."

According to the leaked documents, security officials justified the program as an indispensable security need. "In the future, superpowers will be made or broken based on the strength of their cryptanalytic programs," a 2007 document said. "It is the price of admission for the U.S. to maintain unrestricted access to and use of cyberspace." On Sept. 6, 2013, the day after the story was published, the office of the Director of National Intelligence (DNI) released a statement saying, "Anything that yesterday's disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using . . . to keep America safe."

The leaks have revealed that the NSA specifically targeted and infiltrated data streams within large American media companies. According to documents leaked by Snowden and reported on in an Oct. 30, 2013 article in the *Washington Post*, the NSA tapped connections linking Yahoo and Google data centers, copying and recording massive amounts of data. A NSA report from January 2013 stated that "181,280,466 new records" had been collected in the previous 30 days, "including 'metadata,' which would indicate who sent or received e-mails and when, as well as content such as text, audio and video." The report revealed that the NSA uses a tool called MUSCULAR, a joint venture with its British intelligence counterpart GCHQ, to intercept the data transmissions at undisclosed points and copy the data. The *Washington Post* noted that although the NSA is known for its spying capabilities, "it has not been known to use them routinely against U.S. companies." Google chief legal officer David Drummond said in an Oct. 30, 2013 statement that the company was "outraged," and that Google had "long been concerned about the possibility of this kind of snooping." Drummond concluded that the hacking "underscores the need for urgent reform."

On Nov. 18, 2013, Yahoo denied that it had ever given the government access to its databases and announced that, in response to the reports, it was improving data security, according to a report by PCWorld.com. The online tech magazine reported that Yahoo

NSA, *continued on page 3*

Inside This Issue

Fall 2013: Volume 19, No. 1

Silha Center Staff

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

Brett Johnson
Silha *Bulletin* Editor

Cassie Batchelder
Silha Research Assistant

Alex Vlisides
Silha Research Assistant

Elaine Hargrove
Silha Center Staff

NSA, *continued from page 1*
plans to encrypt all information sent between data centers by the end of the first financial quarter of 2014. In addition, Yahoo announced increased security measure for users, including an option to encrypt all information sent to and from Yahoo. The Nov. 18, 2013 blog post by Yahoo CEO Marissa Mayer announcing the changes did not specifically address whether the encryption methods would be sufficient to protect users against the NSA's encryption hacking techniques.

Newly Revealed NSA Program Tracks Location of Hundreds of Millions of Cell Phones Worldwide

The NSA's CO-TRAVELER program continuously tracks the location on hundreds of millions of mobile communication devices worldwide, according to a Dec. 4, 2013 report by the *Washington Post*. The *Post*'s Barton Gellman and Ashkan Soltani reported that the NSA collects more than five billion records per day, tracking cell phone locations and mapping their relationships, according to documents leaked by Snowden. A senior NSA official, speaking with the *Post* on a condition of anonymity, said that the vast data is collected by "tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones." The location data is stored in vast databases and analyzed for patterns of movement. According to the leaks, the program does not target Americans' location data. However, it does "incidentally" collect some domestic location data and likely collects location data "from the tens of millions of Americans who travel abroad with their cellphones every year."

COVER STORY

According to the *Washington Post* article, the NSA general counsel's office denied that such location tracking was occurring in the United States. However, in an Oct. 2, 2013 hearing before the U.S. Senate Judiciary Committee, NSA director Keith Alexander stated that domestic cell phone location tracking had been pilot tested beginning in 2010, but was discontinued after the NSA concluded that it did not have practical value. In the hearing, Alexander stated that such domestic location tracking "may be something that is a future requirement for the country, but it is not right now."

Civil liberties groups have condemned the program. The ACLU called for greater transparency in a Dec. 4, 2013 statement, writing, "It is staggering that a location-tracking program on this scale could be implemented without any public debate." The Electronic Frontier Foundation (EFF) argued that the program violated both U.S. and international law. A Dec. 5, 2013 blog post by EFF staff members April Glaser and Kurt Opsahl argued that the program violated the Fourth Amendment "right against unreasonable search and seizure," and "the program disregards international human rights law, which is currently in the process of being reaffirmed in a draft resolution by the UN General Assembly."

According to a Dec. 10, 2013 report by the *Washington Post*, the NSA has also been "secretly piggybacking on the tools that enable Internet advertisers to track consumers, using 'cookies' and location data to pinpoint targets for government hacking and to bolster surveillance," according to the leaked documents. The program reportedly allows the NSA to use a web cookie to single out a target's computer, "in order to send out software that can hack that person's computer." These cookies, which are small tracking files placed automatically on Internet users' computers, can also be used to track the location of mobile devices. For instance, many apps for Apple and Google operating systems track device locations without notice to users. The practice of using cookies would allow for more specific location tracking of individuals than the broader tracking involved in the CO-TRAVELER program. The *Post* also reported that the cookies were collected under FISA, which would mean that "the companies know [of the collection] and are legally compelled to assist." Google, which the NSA documents specifically identify as a platform for the tracking, had not commented on the report as the *Bulletin* went to press.

Chris Hoofnagle, a lecturer in residence at UC Berkeley School of Law, told the *Post* that the reports mean that advertiser tracking practices often portrayed as innocuous or even good for consumers must now be considered in a new light. "On a macro level, 'we need to track everyone everywhere for advertising' translates into 'the government being able to track everyone everywhere,'" Hoofnagle said in the Dec. 10, 2013 *Washington Post* report. Nathan Ingraham of the online tech magazine *The Verge* wrote in a Dec. 10, 2013 article that the report could threaten the model of online advertising. "Google relies on its ad revenue, and it certainly doesn't want users to actively start blocking its advertising cookies because of surveillance fears."

On Dec. 9, 2013, ProPublica, the *Guardian*, and *The New York Times* jointly reported that leaked documents demonstrated NSA efforts to perform mass surveillance on the online gaming network Xbox Live. According to this report, the program was intended to "obtain target identifiers (such as profile photos), geolocation, and collection of communications." The documents state that "Al-Qaida terrorist target selectors . . . have been found associated with Xbox Live, Second Life, World of Warcraft, and other GVEs [games and virtual environments]." The report indicated that the NSA also suspected online gaming platforms could be used for secret communication or funding transfers between terrorists, but had little evidence to support these suspicions.

Congress Proposes Surveillance Reform

The controversy and outrage over the Snowden leaks has led to a number of competing congressional proposals for surveillance reform. On Sept. 25, 2013, a bipartisan group of Senators, including Ron Wyden (D-Ore.), Mark Udall (D-Colo.), Rand Paul (R-Ky.), and Richard Blumenthal (D-Conn.), proposed S. 1551, the Intelligence Oversight and Surveillance Reform Act (IOSR). The omnibus bill proposes to amend several laws, including § 215 of the USA PATRIOT Act and several sections of FISA, including § 501 (relating to collection of business records) and § 702 (relating to collection of phone and email data). According to Sen. Wyden, speaking at a Sept. 25, 2013 press conference announcing the bill, the law would attempt to compile the most effective reforms from several bills proposed since the leaks, making it "the most comprehensive bipartisan intelligence reform proposal since [Snowden's] disclosures of last June."

The most prominently reported part of the IOSR seeks to end the warrantless collection of telephone metadata for virtually every call made in the United States. The government had previously relied on an interpretation of § 215 that deemed all such metadata "relevant" to ongoing investigations, thus justifying its use. In order for the government to acquire such data, the bill would require a "statement of facts showing that there are reasonable grounds to believe that the records" sought by the request would be relevant to an investigation. According to a Sept. 25, 2013 press release by Sen. Blumenthal's office, the bill is designed to "prohibit[] the bulk collection of Americans' records in any form, while still authorizing the government to obtain records of individuals suspected of involvement in terrorism or espionage."

The bill also seeks to amend § 701 of the FISA Amendments Act, which the NSA has argued enables its PRISM program. The proposed amendments would close the so-called "backdoor searches loophole," which allows the government to retain and make use of information pertaining only to Americans that has been collected through surveillance aimed at those outside the United States. Opponents of this data collection have called it a loophole because such purely domestic communications and information would not have been legally obtainable if targeted directly. The bill would not allow use of such information, unless the government could demonstrate that it could have legally collected the data in the first place.

NSA, *continued on page 4*

NSA, *continued from page 3*

IOSR also seeks to increase the transparency and oversight of intelligence gathering by intelligence agencies under FISA. The bill would establish an independent counsel, who would challenge government arguments in front of FISA court judges in significant cases. It also would install a process by which secret FISA court opinions would be released to the public, in an attempt to provide greater transparency to the court that hears arguments on many of the government's surveillance programs. (For more information on proposed reforms to FISA courts, see "U.S. Supreme Court Rejects Challenge to Federal Surveillance Law" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

The bill would also allow for greater disclosure by private companies about the degree to which they have cooperated with covert government surveillance efforts. On Oct. 31, 2013, a group of companies, including tech giants Google and Apple, and privacy advocates sent a letter to key lawmakers requesting legal changes to allow companies to be more transparent with the public regarding such cooperation. Independent of the issue of the NSA hacking the data transmissions of some of these companies without their permission, the companies sought to combat negative publicity in the wake of reports that the tech industry was voluntarily cooperating with NSA surveillance programs. The letter asked for changes that would allow companies to reveal the "number and nature of requests" for user data from the government. The companies argued that "transparency in this regard will also help to counter erroneous reports that we permit intelligence agencies 'direct access' to our companies' servers or that we are participants in a bulk Internet records collection program." On Dec. 17, 2013, executives from some of these firms, including Apple CEO Tim Cook and Yahoo CEO Marissa Mayer, met with Obama and Vice-President Joe Biden to discuss the changes proposed in their letter. The executives contended that the spying programs are damaging to their reputations and harmful to the economy, according to the *Washington Post*.

The IOSR has largely been supported by online privacy advocates, including the ACLU and EFF, which called the bill a "fantastic start" toward federal surveillance reform in an Oct. 21, 2013 blog post. However, the IOSR is now competing with a newer bill that proposes many similar reforms, but has a larger base of bipartisan sponsors and has been introduced in both houses of Congress. On Oct. 29, 2013, Rep. Jim Sensenbrenner (R-Wis.) and Sen. Patrick Leahy (D-Vt.) proposed H.R. 3361/S. 1599, the USA FREEDOM Act. The bipartisan bill, sponsored by Sensenbrenner, one of the authors of the PATRIOT Act, has 16 Senate and more than 102 House co-sponsors, according to a Nov. 30, 2013 report by *The Hill*'s Brendan Sasso.

Comparing the IOSR to the Sensenbrenner bill, Jennifer Granick of Stanford University's Center for Internet and Society wrote in an Oct. 29, 2013 post on the Center's blog that "there are many similarities, and few differences between the proposals." Like the IOSR, the Sensenbrenner bill proposes to end bulk collection of metadata under § 215 and eliminate the "backdoor searches loophole" by requiring a court order before such information incidentally collected about Americans could be used. It also seeks to increase the transparency of FISA courts by requiring that all decisions from 2003 to the present that make significant interpretations of law be released to the public. It would create a FISC Special Advocate to provide a more adversarial presence in such cases, although, according to a comparison of the bills by Stanford's Center for Internet and Society from Nov. 1, 2013, the IOSR would give these advocates more tools to challenge the government. For instance, the IOSR would allow the advocates to appeal decisions, and it would allow outside parties to submit *amici curiae* briefs to the FISC.

However, the Sensenbrenner bill, unlike the IOSR, proposes reform of national security letters, which are secret requests for information by intelligence agencies, that recipients cannot tell anyone about. The bill would restrict the scope of these letters to the records of terrorists and foreign spies, or the activities or people communicating with terrorists or spies. The bill adopts the FISA definition of terrorism, defined as violence intended to coerce a population or influence governmental decisions. It would also allow companies who have received the letters to provide public estimates of the number of letters they have received and complied with. The government would also be required to release public reports estimating the number of people subject to electronic surveillance, which would include national security letters.

The bill generally has been endorsed by privacy advocates, and has largely eclipsed the IOSR for their support. The ACLU endorsed the bill in an Oct. 29, 2013 article on its website and wrote that it "incorporates the language and principles of past reform" efforts such as the IOSR. The EFF has also endorsed the bill, and in a Nov. 14, 2013 blog post the organization emphasized the bill's combination of valuable reform and bipartisan support, calling it the "best shot at fixing some of the worst problems with NSA surveillance." The bill has also been supported by such interest groups as the Center for Democracy & Technology and the Arab American Institute. However, in her Oct. 29 blog post, Stanford University's Granick criticized both the Sensenbrenner and Wyden bills for not doing enough to protect Americans from "indiscriminate surveillance." According to Granick, "neither bill addresses the vast surveillance NSA conducts outside of FISA," and neither "stop[s] the NSA's BULLRUN program['s] efforts to undermine the implementation of strong encryption on the public internet."

Some security advocates have argued that the bill misunderstands the nature of terrorism investigations because it assumes that intelligence agencies will have specific suspects. "You are reducing the amount of data available and therefore making it much more difficult to make the connections that we need to make," Patrick Kelley, general counsel for the FBI, told Techworld.com for a Nov. 4, 2013 article.

On Oct. 31, 2013, Sen. Dianne Feinstein (D-Calif.) introduced S.1631, the FISA Improvements Act of 2013, a competing surveillance reform bill with a more limited scope than the Sensenbrenner or Wyden proposals. The bill purports to make some of the same changes proposed by the other two bills, such as reforming bulk metadata collection under § 215 and increasing transparency regarding NSA surveillance. However, Feinstein's bill would continue to allow metadata collection, but under specified practices, such as a five-year retention period for communication data, after which the NSA would be required to destroy it. The bill would also offer little reform to FISA courts or national security letters.

According to a Nov. 15, 2013 article in the *Guardian*, the Feinstein bill also contains provisions that allow domestic law enforcement agencies to query NSA databases. Michelle Richardson, the surveillance lobbyist for the ACLU, told the *Guardian* in an interview that the bill could "expand current practices by allowing law enforcement to directly access U.S. person information that was nominally collected for foreign intelligence purposes."

Critics of Feinstein's bill have argued that it reinforces current surveillance procedures. A Nov. 5, 2013 *Los Angeles Times* staff editorial opposed the bill, writing, "[T]he protections are minimal, and in return for the minor changes, Congress would give its explicit approval for the wholesale acquisition of metadata by the government." The Cato Institute's Julian Sanchez called the bill's reforms "cosmetic changes" in an Oct. 31, 2013 post on the Institute's blog, writing that "the bill for the first time *explicitly authorizes*, and therefore entrenches in statute, the bulk collection of communications records." Privacy advocates have strongly opposed the bill, with EFF staff member Trevor Tim writing in an Oct. 31, 2013 blog post that "the bill codifies some of the NSA's worst practices, would be a huge setback for everyone's privacy, and it would

permanently entrench the NSA's collection of every phone record held by U.S. telecoms."

The executive branch has also proposed changes in the wake of the Snowden leaks. On Dec. 5, 2013, the White House released a new U.S. Open Government National Action Plan (NAP), which seeks to "increase citizen participation, collaboration, and transparency in government." The plan is the administration's second open government plan, following a 2011 plan that created initiatives such as the "We the People" online petition process, through which over 10 million people have petitioned the White House, according to the 2013 NAP. The new NAP proposes to improve Freedom of Information Act (FOIA) compliance through government-wide training and improve the classification system by making classification decisions more consistent and accountable. It also seeks to increase transparency for FISA activities by implementing annual reports on how often certain surveillance tools were used and creating a declassification process for FISA court decisions. These provisions are similar to aspects of the congressional reform bills.

Steven Aftergood, in a Dec. 6, 2013 Secrecy News article, questioned the efficacy of the efforts regarding classification, writing that "[t]he Administration has not embraced an explicit theory of how overclassification occurs, or even how overclassification is to be defined, and therefore it is not yet well-equipped to address the problem." The Sunlight Foundation, a non-profit government transparency advocate that has been critical of the administration's FOIA policy, wrote in a Dec. 6, 2013 blog post that the "proposed FOIA advisory board and committee could be transformative." However, John Wonderlich, director of the Sunlight Foundation, said the NAP "isn't necessarily progress, it's just a different conversation," according to a Dec. 6, 2013 article in the *Washington Post*.

On Dec. 13, 2013, the *Washington Post* reported that the Obama administration will maintain the structure of NSA leadership. Currently, one official oversees both the NSA and the military cyberwarfare command. Some top security officials had suggested that splitting the responsibilities between two positions would increase oversight and accountability. The *Post* article stated that the announcement signaled that the Obama administration "favors maintaining an agency program that collects data on virtually every phone call that Americans make."

On Dec. 18, 2013, the five-member Review Group on Intelligence and Communications Technologies released a report recommending reforms to the NSA metadata collection program, according to the *Washington Post*. The *Post* reported that among the Review Group's more than 40 recommendation was that phone companies or other third parties, rather than the NSA, should store the metadata that the NSA collects. The Review Group also suggested that the NSA be barred from building so-called "backdoors" into the systems of tech companies, and that the agency be prohibited from undermining standards of global encryption technology. The proposals are non-binding, and the White House "is free to accept, reject or modify the panel's ideas," according to the *Post*.

Supreme Court Rejects Challenge to FISA Court Decision Approving NSA Surveillance; Federal Judge Rules Metadata Collection Program Unconstitutional

On Nov. 18, 2013, the U.S. Supreme Court declined to consider a challenge by the Electronic Privacy Information Center (EPIC) to the NSA metadata surveillance program. On July 8, 2013, EPIC filed a petition for a writ of *mandamus* with the court, asking it to find that the FISA court exceeded its authority in ordering telecommunications giant Verizon to grant the NSA access to their customers' metadata. In its petition, EPIC argued that "[t]o compel production of 'tangible things,' the FISA requires the items sought be 'relevant' to an authorized investigation." Because Verizon was ordered to turn over tangible records, and because "it is simply not possible that every phone record in the possession of a telecommunications firm could be relevant to an authorized investigation," EPIC argued that the FISA court had exceeded its statutory authority. The Supreme Court made no comment on its decision not to hear the case.

In a Nov. 18, 2013 post for SCOTUSblog, Lyle Denniston called the legal challenge an "unusual request" to the court because EPIC asked for a writ of *mandamus* directing a FISA court judge to vacate the April 2013 order approving portions of the NSA surveillance. EPIC argued that the challenge was appropriately filed at the Supreme Court level because no other court had jurisdiction, but according to Denniston, the high court very rarely grants such *mandamus* petitions.

The ACLU filed a similar challenge in the Federal District Court for the Southern District of New York on June 11, 2013. In *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y. June 11, 2013), the organization is arguing that the NSA's metadata program exceeds the authorization provided by the PATRIOT Act and violates the First and Fourth Amendments. The ACLU's motion for a preliminary injunction on the program and the government's motion to dismiss were pending as the *Bulletin* went to press.

In an article for the September 2013 issue of *Internet & Computer Lawyer*, University of Houston Law Center adjunct professor David Bender addressed some of the legal questions at issue in these cases. Bender's reading of FISA would reject EPIC's argument, finding that FISA courts do have the power to decide an order like the one EPIC is challenging. Bender also disagreed with the argument that NSA metadata collection is unlawful because it exceeds the power granted by the "Business Records" provision of FISA, which authorizes empowers intelligence agencies to seize records relevant to an investigation. Section 1861 of FISA requires specific minimization procedures that limit how the government can use the business records data. The legal question presented is whether the metadata collection violates these minimization procedures. EPIC argued that the metadata that is collected must be relevant to an investigation. However, Bender argued that the minimization procedures apply only to "retention and dissemination" of data. The NSA's massive metadata collection program does not seem to "violate the letter of the statute" because these procedures do not apply to "collection in the first place, and in general not to use thereafter," Bender wrote.

On Dec. 16, 2013, the NSA was handed its first major legal defeat since the Snowden leaks emerged. In *Klayman v. Obama*, Federal District Court Judge Richard Leon found that the telephony metadata collection violated the Fourth Amendment protection from unreasonable search and seizures. No. 13-0851 (D.D.C. Dec. 16, 2013), available at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48. The government argued that Fourth Amendment precedent established that citizens do not have a reasonable expectation of privacy in the numbers dialed from one's phone. However, Judge Leon found that "present-day circumstances — the evolutions in the Government's surveillance capabilities, citizens phone habits, and the relationship between the NSA and telecom companies" had changed so significantly from the past that these precedents did not apply. "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying it and analyzing it without judicial approval," Judge Leon wrote. In addition to emphasizing the scope of the collection, Leon questioned the intelligence value of the metadata collection program. "I have significant doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism." Judge Leon cited several other federal cases, including *ACLU v. Clapper* and *In re Electronic Privacy Information Center*, as alleging

NSA, *continued on page 6*

NSA, *continued from page 5*
similar claims. Because of the important national security interests implicated in the case, Judge Leon stayed the decision pending appeal.

International Outrage Continues Over Snowden Leaks

On Oct. 24, 2013, European Parliament President Martin Schulz said that the Transatlantic Trade and Investment Partnership negotiations should be suspended until further investigation of, and resolution of, allegations of NSA spying on dozens of world leaders, including the mobile phone of German Chancellor Angela Merkel. Bloomberg News reported on Oct. 30, 2013 that Schulz said, "We can not expect to conduct these negotiations if the National Security Agency is listening in on EU institutions, including the European Commission office in Washington and the European Parliament. This is unacceptable."

Der Spiegel reported on Oct. 23, 2013 that German Chancellor Angela Merkel's personal cell phone number appeared on a list of targeted phones leaked by Snowden, and may have been monitored for the last 10 years. According to an Oct. 27, 2013 story in *Der Spiegel*, Merkel responded to the report at a European Union summit in Brussels by saying, "Spying between friends, that's just not done," and that "trust has to be rebuilt." Some German legislators have criticized Merkel for not taking a harder line in response to the spying accusations. According to a Nov. 18, 2013 article in the *Guardian*, German MP Gregor Gysi accused Merkel's government of being "lulled to sleep" by insufficient assurances from the NSA.

An Oct. 24, 2013 article in the *Guardian* sparked further controversy by reporting that leaked NSA memos revealed that the NSA tapped the phones lines of 35 world leaders, although the memo did not provide the names of these leaders. An Oct. 21, 2013 article in *Le Monde* detailing surveillance in France led former Prime Minister Dominique de Villepin to call the reports a "major blow" to U.S. foreign interests because it shows that "America doesn't trust its allies."

According to a Sept. 24, 2013 article in the *Washington Post*, Brazilian President Dilma Rousseff strongly condemned American spying, "telling a gathering of world leaders at the U.N. General Assembly that American eavesdropping constitutes 'a breach of international law and an affront' to Brazil's sovereignty." Brazil has continued to be among the most vocal critics of the NSA. However, *The Verge* reported on Nov. 5, 2013 that Brazil, itself, had spied on foreign diplomats, including those from the United States, Russia, and Iran. The *Guardian* reported on Dec. 17, 2013 that Snowden sent an open letter to the Brazilian government offering more information on U.S. spying practices against Brazil in exchange for asylum. The Brazilian government had not formally responded to the offer as the *Bulletin* went to press.

On Nov. 1, 2013, the Brazilian and German U.N. delegations circulated a draft joint resolution to the U.N. General Assembly that sought to limit international surveillance, framing the issue as a violation of human rights. The resolution called on member states to "to take measures to put an end to violations of these rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law." On Nov. 26, 2013, the U.N.'s social, humanitarian and cultural committee unanimously passed the resolution without a vote. The U.S. mission to the U.N. endorsed the resolution in a Nov. 26, 2013 statement, saying, "[W]e applaud this resolution's recognition that full respect for the right to freedom of expression." However, the statement noted that "conduct that violates privacy rights does not violate the right to freedom of expression in every case." The non-binding resolution is expected to move to the General Assembly for a vote, and it is likely to pass, according to a Nov. 26, 2013 report by ABC News.

According to an Oct. 28, 2013 article by *New York Times* reporters Mark Landler and David E. Sanger, Obama administration officials have said that the administration would make "unspecified changes in surveillance policy and plan further changes, particularly in the monitoring of government leaders." In an Oct. 28, 2013 press release, Senate Intelligence Committee chair Dianne Feinstein stated that the White House informed her that "collection on our allies will not continue." However, the White House said this was not accurate. According to the Oct. 28, 2013 *New York Times* report, "the [Obama] administration will reserve the right to continue collecting intelligence in friendly countries that pertains to criminal activity, potential terrorist threats and the proliferation of unconventional weapons."

Guardian *Editor Rusbridger Called to Appear Before UK Parliament*

On Dec. 3, 2013 Alan Rusbridger, editor-in-chief of the *Guardian*, was called before the UK House of Commons' home affairs committee to answer questions in connection with the newspaper's reporting on the Snowden leaks. Committee members were particularly concerned about materials leaked to the *Guardian* by Snowden, which the newspaper had transmitted to other news organizations. Committee member Michael Ellis (Conservative - Norhampton North) said in the hearing, "It isn't only about what you've published, it's about what you've communicated. That is what amounts, or can amount, to a criminal offense."

At the hearing, Rusbridger described what he characterized as efforts by the UK government to intimidate the *Guardian*. According to a Dec. 3, 2013 *Washington Post* report on the hearings, he said, "They include prior restraint, they include a senior Whitehall official coming to see me to say: 'There has been enough debate now.' They include asking for the destruction of our disks. They include MPs calling for the police to prosecute the editor. So there are things that are inconceivable in the U.S."

Rusbridger stated that the *Guardian* had communicated extensively with the UK and U.S. governments about its reporting, and said, "We will continue to consult them, but we are not going to be put off by intimidation, but nor are we going to behave recklessly."

Former *Washington Post* reporter Carl Bernstein published an open letter to Rusbridger in the *Guardian* on Dec. 3, 2013, calling the parliament's inquiry "an attempt by the highest UK authorities to shift the issue from government policies and excessive government secrecy in the United States and Great Britain to the conduct of the press." Committee Chair Keith Vaz (Labour – Leicester East) has been widely criticized for asking Rusbridger, "Do you love this country?" In a Dec. 3, 2013 editorial for *The Telegraph*, Dan Hodges called Vaz's questioning "the very definition of McCarthyism." Many media sources have emphasized the contentious nature of the appearance, including a Dec. 3, 2013 *Washington Post* article describing it as an "occasionally combative public grilling."

In a Dec. 6, 2013 editorial for *The Huffington Post*, Robert Mahoney, President of the Committee to Protect Journalists, argued that the UK government's treatment of the *Guardian*, epitomized by the home affairs committee's hostility toward Rusbridger, set a dangerous precedent. "The intimidation of journalists and news organizations covering the fall-out from the Snowden files is troubling for many reasons, not least because of the signal it sends to authoritarian and repressive regimes around the world. If the editor of a national newspaper in a country with a functioning democracy and 300-year-old tradition of a free press can be threatened and bullied, what more does an autocrat need to do except invoke national security and cite the British example?"

EU Parliament Committee Votes for Overarching Privacy Reform

On Oct. 21, 2013, the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted 51-1, with three abstentions, to adopt two pieces of data protection legislation meant

to update the 1995 Data Protection Directive. The first is the General Data Protection Regulation (GDPR), a set of 91 amendments that are intended to modernize how personal data is regulated in the European Union. A regulation is stronger than a directive under EU law. The GDPR will regulate data processing procedure by private companies and define what rights individuals have over their personal data. The second is a directive governing law enforcement procedures regarding personal data.

LIBE approved the 91 amendments out of more than 3,000 that were proposed to the original draft of the regulations submitted in January 2012 by the European Commission, according to an Oct. 28, 2013 report from Bloomberg News, which noted that the regulations are a stark contrast to the more pro-business nature of the original regulations. According to an Oct. 21, 2013 press release by LIBE, the amendments are designed to put consumers in control of their personal data. Where data processing requires consent, such consent must be "freely given, specific, informed and explicit indication of his/her wishes, either by a statement or by a clear affirmative action." Many believe that such strong data privacy protections are a response to the privacy concerns raised by the Snowden leaks, according to the Bloomberg News report.

Many of these provisions could have important implications for the private sector. Companies failing to comply with the regulations can be subject to fines of up to either €100 million or 5 percent of their annual worldwide turnover, whichever is greater. The original draft proposed maximum fines of 2 percent of global turnover. Additionally, the European Union would have jurisdiction over all claims regarding the personal data of EU citizens regardless of where the data was processed. According to a Nov. 4, 2013 report from Lexology.com, it is not clear how the European Union will be able to enforce such actions against companies with little or no EU presence.

The amendments also require that all companies processing personal data relating "to more than 5,000 data subjects during any consecutive 12-month period" must appoint a Data Protection Officer (DPO)." The DPOs are subject to several employment requirements, including independence from other middle management and a minimum employment term of four years to ensure that independence.

The regulations also would require companies to notify and gain approval from EU data protection officials before complying with a government's request for an EU citizen's personal data. Jan Phillipp Albrecht, rapporteur of the GDPR, told journalists at an Oct. 22, 2013 press conference that "there is a problem of noncompliance, especially of big IT companies coming from outside the European market. We needed to answer that." However, Karin Retzer, a partner at Morrison & Foerster LLP, in Brussels, told Bloomberg News on Oct. 22, 2013 that complying with this procedure in time to satisfy government requests would be "basically impossible."

Article 80 of the GDPR is of particular note for media organizations and journalists. The article requires member states to adopt exceptions or regulations necessary to comport data protection rights with the freedom of expression, which is recognized as a fundamental right. The amendments have removed specific references to "journalistic purposes," which some say broadens the potential protections for expression, yet may also reduce journalists' ability to defend against data privacy claims. Free press advocates have argued that the original mention of "journalistic purposes" in the 1995 directive provided media with an argument that their activities deserved greater protection against such claims, and that the deletion of these provisions could provide privacy advocates strong evidence that the European Parliament specifically rejected heightened protections for journalism.

In a joint statement released Dec. 2, 2013, a coalition of European media interest organizations criticized the "data protection reform plans for failing to underpin press freedom and protect journalistic sources," according to a Dec. 3, 2013 press release by the European Federation of Journalists. The statement specifically objected to the Article 80 amendments, stating, "A clear reference to 'journalistic purposes' needs to be upheld as it is the only way to maintain proper protection of journalism." European Publishers Council Executive Director Angela Mills Wade emphasized the need to balance newsgathering with other important values, saying, "It is essential that legitimate newsgathering and investigative activities are given the greatest respect when balancing the right to privacy and other fundamental rights," according to the press release.

Article 17 of the GDPR outlines the "right to erasure." The right to erasure is a narrower form of the right to be forgotten, a hotly debated proposed amendment that would enable Internet users to request the deletion of all personal data. According to an Oct. 21, 2013 report by Reuters, LIBE officials believed that opting for the right to erasure was "necessary as consultations with technology companies had made clear that it would be impossible to entirely remove someone's traces from the Internet." In contrast, the right to erasure provides a right for individuals to request that specific content be erased. Individuals have the right to request erasure of personal data by those controlling the data, "and to obtain from third parties the erasure of any links to, or copy or replication of that data," according to the new amendments. This right to erasure may be invoked where the data is no longer being used for its originally intended purpose, where consent has been revoked, or where the party has not complied with Article 6(1) of the GDPR, which defines lawful processing of data. Subject to exceptions from Article 80 (freedom of expression), Article 81 (public health), and Article 83 (research), controllers and third parties are required to erase such personal data without delay on request of the data subject. Another exception, which some see as business friendly, exempts controllers whose data storage system does not allow for erasure and was created before the regulations took effect from right to erasure responsibilities. (For additional information about developments in data protection law in the United States, see "California Legislators Address Data Protection and New Technology of Several Fronts" on page 16 of this issue of the Silha *Bulletin*.)

The amendments will be negotiated between Albrecht and the EU council, with the stated goal of having an agreement in place for the European Parliament to vote on before the May 2014 round of elections.

The amendments have received much criticism in the United States, particularly from the business community. American Internet companies such as Google, Yahoo and Facebook have opposed the amendments. John Higgins, the director general of DigitalEurope, an interest group that represents tech companies such as Apple, Microsoft and I.B.M. within the European Union, called the GDPR a "half-baked law" that "risks throwing away a vital and much needed opportunity to stimulate economic growth," according to an Oct. 21, 2013 *New York Times* report. However, American privacy advocates have supported the changes. EPIC, in an Oct. 21, 2013 blog post, called the European Union's amendments "the best prospect for the protection of Internet users around the globe."

Alex Vlisides
Silha Research Assistant

Senate Considers Federal Reporter's Privilege Bill

On May 16, 2013, Senators Chuck Schumer (D-N.Y.) and Lindsay Graham (R-S.C.) introduced S. 987, the Free Flow of Information Act of 2013 (FFIA). The bill is meant to create a statutory federal journalist's privilege by "codify[ing] into law and expand[ing] upon the recently-updated Department of Justice media guidelines," according to Sen. Schumer's website. Journalists and media entities have long sought a statutory guarantee of certain legal privileges protecting their sources and records, privileges that to varying degrees have been protected as a matter of common law and executive branch discretion. The bill was proposed just days after news broke in May 2013 that the Obama administration had subpoenaed the Associated Press's (AP) phone records in April and May 2012 without providing notice until May 2013. Schumer specifically referred to the AP subpoena the day before officially introducing the bill, commenting, "At minimum, our bill would have ensured a fairer, more deliberate process in this case," according to a May 15, 2013 article in *The New York Times*. (For more information about the controversy surrounding the Obama administration's subpoenaing of journalists, see "Justice Department Secretly Subpoenas Associate Press Phone Records" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

FEDERAL SHIELD LAW

On Nov. 6, 2013, the Senate Judiciary Committee approved an amended version of the bill, allowing the bill to be placed on the Senate's calendar for debate. The bill has many similarities with the DOJ guidelines, thereby fulfilling the goal of codifying the guidelines and giving them the force of law. Decisions on who and what is protected from compelled disclosure would no longer be made by DOJ officials — who may have a vested interest in a successful investigation — but rather by disinterested federal judges.

In recognition of the public interest in newsgathering, the current DOJ guidelines, which were first adopted in 1970, dictate that "[a]ll reasonable attempts should be made to obtain information from alternative sources before considering issuing a subpoena" to a member of the media. The DOJ guidelines also dictate how investigators should go about obtaining journalists' records from third parties such as phone companies or Internet service providers. If it is determined that the information is essential, the guidelines call for officials to enter negotiations with the media member to acquire the information, so long as this would not present a "substantial threat to the integrity of the investigation." In criminal cases, this means the information should be essential to "establishing guilt or innocence," and in a civil case it should be essential to winning a "case of substantial importance." When the DOJ subpoenas a third party for a media member's information, the guidelines state that the media member should be notified except where doing so would pose a "clear and substantial threat to the integrity of the investigation." In such cases, notification should be delayed no longer than 90 days. Subpoenas to third parties are addressed only in criminal cases (presumably excluding use in civil cases) and must be narrow in scope, in both subject matter and time period. Finally, the guidelines state that no direct or third party subpoenas shall be issued "without the express authorization of the Attorney General." Failure to receive prior approval can result in disciplinary action, but the guidelines are "not intended to create or recognize any legally enforceable right in any person."

> "The Free Flow of Information Act sets forth reasonable standards to guide federal judges in assessing requests to compel journalists and their service providers to reveal information that could harm confidential sources and the newsgathering process."
>
> **— Newspaper Association of America**

On July 12, 2013, the DOJ released a report detailing proposed changes to the media guidelines. The most significant change imposed by the report is the strengthening of the notice requirements. The report states that the "presumption of advance notice will be overcome only if the Attorney General affirmatively determines . . . that for compelling reasons, advance notice and negotiations would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm." The report would also update protections for electronic information held by third parties, clarifying that the guidelines apply to "'communications records' or 'business records' of members of the news media that are stored or maintained by third parties." As the *Bulletin* went to press, these proposed changes had not been formally adopted into the DOJ guidelines. (For more on the revisions to the DOJ guidelines, see "Department of Justice Revises Guidelines for Investigating Journalists" in the Summer 2013 issue of the Silha *Bulletin*.)

The provisions of the FFIA practically mirror the DOJ guidelines. Under the FFIA, in both criminal and civil cases, investigators seeking to compel disclosure must have "exhausted all reasonable alternative sources." For criminal cases, there must be "reasonable grounds to believe that a crime has occurred," the information sought must be "essential" to the investigation, and the subpoena must be consistent with the DOJ guidelines. However, unlike the guidelines — under which each request must balance the law enforcement interest with the public interest in newsgathering — the FFIA would allow the compelled disclosure except where the subject "established by clear and convincing evidence that disclosure of the protected information would be contrary to the public interest." In civil cases, the compelled disclosure must be "essential to resolution of the matter." The bill provides for a higher presumption of the public interest in civil cases, requiring that the party seeking disclosure must establish that "the interest in compelling disclosure clearly outweighs the public interest" in newsgathering.

Like the DOJ guidelines, the FFIA also addresses compelled disclosure of journalists' information from third

party service providers. The government would be required to notify the journalist of a subpoena for third party records unless providing notice is a threat to the investigation or national security, and notice must not be delayed for more than 90 days. However, unlike the guidelines, the proposed law would require proof of such a threat by "clear and convincing evidence" as determined by a federal judge.

The bill contains a number of exceptions. It provides no protection where the information is reasonably related to the prevention of death, bodily harm or threats to infrastructure under the USA PATRIOT Act. The bill also has a national security exception. If a court finds by "a preponderance of the evidence" that the information could "assist" in "prevent[ing] or mitigat[ing]" a national security threat, the law's protections would not apply. The national security exception instructs courts to give "appropriate deference" when assessing national security claims by government officials. The exception applies to leaks of confidential information, allowing for compelled disclosure where national security concerns stemming from a leak are at stake.

Another exception is that the proposed law does not apply to "acquisition or dissemination of information pursuant to the Foreign Intelligence Surveillance Act of 1978." According to *The First Amendment Handbook*, a media guide to press law produced by the Reporters Committee for Freedom of the Press (RCFP), "in order to obtain a FISA warrant . . . investigators need show only that national security is a 'significant purpose.' And because proceedings of the FISA court are secret, journalists will have no warning that their sources are being disclosed." Under the proposed law, these procedures would remain in place, because the law does not apply to investigations pursuant to FISA.

The FFIA explicitly applies only to materials that have been conveyed or acquired by the reporter upon a promise of confidentiality, providing no protection to a non-confidential work product. The DOJ guidelines make no mention of a journalist's assurance of confidentiality to a source, and have been interpreted to give some protection to non-confidential materials. Although the proposed law does not yet displace the DOJ guidelines, it appears that fewer materials would be covered by the law than the guidelines because the FFIA applies only to confidential materials.

One provision that has received much debate is to whom the bill's protections apply, with some arguing that the proposed law would be a way for the government to define who is a journalist. "Covered persons" for protection in the bill includes those who, broadly defined, collect information with the intent of disseminating news to the public. It also includes those who work with or are affiliated with such persons. The bill does not explicitly define "journalist" outside the purposes of coverage of the law. David Greene, a Senior Staff Attorney with the Electronic Frontier Foundation (EFF), embraced what he termed the bill's "functional definition" of a journalist in a Sept. 20, 2013 blog post, arguing that this approach is more likely to protect "non-traditional journalists such as self-publishing bloggers and citizen journalists."

> "Most journalism organizations acknowledge [the bill is] not perfect. Far from perfect, really. But having some protection is better than none at all."
>
> **— Society of Professional Journalists**

Many media advocates support the bill as a step toward stronger protections for newsgathering. The *Washington Post* endorsed the bill in a Sept. 22, 2013 editorial, calling the bill's protections "necessary" to protect journalists. The Newspaper Association of America (NAA) endorsed the bill in a Sept. 10, 2013 press release, writing that the "Free Flow of Information Act sets forth reasonable standards to guide federal judges in assessing requests to compel journalists and their service providers to reveal information that could harm confidential sources and the newsgathering process." The RCFP commented in a Sept. 12, 2013 press release that the bill "goes a long way toward ensuring that reporters will be protected from subpoenas for their confidential information and sources."

Society of Professional Journalists (SPJ) President David Cuillier wrote an Oct. 1, 2013 post on his "Freedom of the Prez" blog in support of the bill, claiming that most media advocates and intellectuals, including four out of the five prominent scholars he contacted, support the bill. The SPJ wrote in its "Shield Law 101" explainer on its website, "Most journalism organizations acknowledge [the bill is] not perfect. Far from perfect, really. But having some protection is better than none at all." Reporter's privilege scholar RonNell Anderson-Jones, a professor at Brigham Young University Law School, described the bill less optimistically, saying, according to Cuillier's Oct. 1 blog post, "It's better than a kick in the teeth."

Some, however, have argued that the protections offered by the bill are so marginal that no statutory protections would be better than the ones offered in the bill. In an undated article for the SPJ website, former SPJ President Gordon "Mac" McKerral argued that the bill's protections are negated by the long list of exceptions, which he argues includes "all things classified, all things terrorist related and all things that threaten national security." Silha Center Director and Silha Professor of Media Ethics and Law Jane Kirtley had similar concerns and opposed the bill based on the opportunity costs of expending political capital to pass a subpar bill. According to Cuillier's Oct. 1 blog post, Kirtley argued that a flawed law would hinder journalists' protections because press advocates would be "unlikely to get an opportunity to amend a problematic law any time in the foreseeable future."

Alex Vlisides
Silha Research Assistant

Reporters Struggle to Claim Privilege to Avoid Testifying About Confidential Sources

Several reporters who received information from confidential sources have faced potential jail time and fines for refusing to testify about their sources in recent months. In October 2013, the United States Court of Appeals for the Fourth Circuit ordered James Risen, a *New York Times* reporter, to testify about his source who allegedly leaked information about Iran's nuclear program that Risen included in a book. Risen refuses to testify and plans to petition the United States Supreme Court to hear his case. Reporting about the July 2012 mass shooting in Aurora, Colo., New York-based Fox News reporter Jana Winter received a notebook that the accused shooter allegedly sent to his psychiatrist. The Colorado district court approved a defense request for a subpoena to compel Winter to reveal her source, which she has refused to do. New York's highest court ruled in December 2013 that New York's reporter's shield law protects Winter from being compelled to testify about her source in Colorado. Joe Hosey, a reporter in Illinois, received leaked police reports about a murder and was ordered to identify his source. He is awaiting the results of his appeal. These recent cases highlight the challenges reporters who rely on confidential sources face and raise longstanding questions about the existence of a reporter's privilege.

REPORTER'S PRIVILEGE

Appellate Court Orders* New York Times *Reporter James Risen to Testify About Leak Source; Risen Plans to Appeal to United States Supreme Court

On Oct. 13, 2013, the United States Court of Appeals for the Fourth Circuit denied *New York Times* reporter James Risen's petition for the full appeals court to hear his argument that he should not be compelled to testify about his source in a leak investigation. The Department of Justice contends that former CIA official Jeffrey Sterling is Risen's source. Charges filed against Sterling allege that Sterling leaked information to Risen about a botched CIA attempt to sabotage Iran's nuclear program, which Risen included in his 2006 book *State of War*.

On July 30, 2011, United States District Court Judge Leonie M. Brinkema, based in Alexandria, Va., issued an order severely restricting what prosecutors could ask Risen during his testimony, preventing the government from forcing Risen to identify his source's identity. *United States v. Sterling*, 818 F.Supp.2d 945 (E.D. Va. 2011). "I think it's an important victory for the First Amendment and for freedom of the press," Risen told the *Times* for a July 30, 2011 story. "The protection of sources will allow for the American press to continue to find and report the truth." (For more information on Judge Brinkema's ruling, see "Judges Rebuke Government on Leak Prosecutions" in the Summer 2011 issue of the Silha *Bulletin*.)

> "I am not discouraged at all, because I have actually been encouraged by the broad level of support that I have received. I think a lot of people now recognize the significance of this case. I will go to jail if necessary to keep up the fight."
>
> **— James Risen**
> **Reporter,**
> ***The New York Times***

However, the Obama administration appealed Judge Brinkema's ruling, and two members of a three-judge panel for the United States Court of Appeals for the Fourth Circuit overturned the lower court's ruling on July 19, 2013. *United States v. Sterling*, 724 F.3d 482 (4th Cir. 2013). "There is no First Amendment testimonial privilege, absolute or qualified, that protects a reporter from being compelled to testify by the prosecution or the defense in criminal proceedings about criminal conduct that the reporter personally witnessed or participated in, absent a showing of bad faith, harassment, or other such non-legitimate motive, even though the reporter promised confidentiality to his source," Chief Judge William B. Traxler, Jr. wrote for the majority. Judge Roger Gregory dissented. "Our country's Founders established the First Amendment's guarantee of a free press as a recognition that a government unaccountable to public discourse renders that essential element of democracy — the vote — meaningless," Judge Gregory wrote. "The majority reads narrowly the law governing the protection of a reporter from revealing his sources, a decision that is, in my view, contrary to the will and wisdom of our Founders."

Risen then filed a petition requesting that the full Fourth Circuit Court of Appeals reconsider the subpoena *en banc*. The appellate court denied his appeal on Oct. 15, 2013 in a 13-1 vote. *United States v. Sterling*, 732 F.3d 292 (4th Cir. 2013). The judges who denied rehearing did not explain their reasoning. Judge Gregory was again the lone dissenter, writing that the issue raised by the case is one of "exceptional importance." For "public opinion to serve as a meaningful check on governmental power, the press must be free to report to the people the government's use (or misuse) of that power," he wrote.

Risen has said that he will take his appeal to the United States Supreme Court. On Oct. 22, 2013, his attorney filed a motion with the appellate court requesting that it stay the subpoena until the Supreme Court decides whether to grant *certiorari* in the case. The Fourth Circuit granted the motion for a stay on Nov. 6, 2013. *United States v. Sterling*, No.11-5028, 1:10-cr-00485-LMB-1 (Nov. 6, 2013). Risen told the *Times* for an Oct. 16, 2013 report that he has decided to take his case to the Supreme Court. "I am not discouraged at all, because I have actually been encouraged by the broad level of support that I have received," Risen said. "I think a lot of people now recognize the significance of this case. I will go to jail if necessary to keep up the fight." At the time the *Bulletin* went to press, Risen's attorney, Joel Kurtzenberg, partner at Cahill Gordon & Reindel, had not yet filed a petition for a writ of *certiorari* with the Supreme Court.

Several media organizations have spoken out in Risen's favor. In an Aug. 21, 2013 letter to Attorney General Eric Holder, the Reporters Committee for Freedom of the Press (RCFP), joined by 45 media organizations, asked the Justice Department to withdraw the subpoena

issued to Risen. The letter called the Fourth Circuit's decision a "complete rejection of the interests of a free press and [a] narrow reading of the [reporter's] privilege factors." The letter explained that the Justice Department has many other ways to identify the leaker and should not demand Risen's testimony.

Some have argued that the Supreme Court should agree to hear Risen's case. The court last considered the reporter's privilege in *Branzburg v. Hayes*, 408 U.S. 665 (1972). The plurality opinion in the case declined to create a testimonial privilege for reporters, although Justice Lewis Powell's concurring opinion, some argue, could be interpreted as indicating that a reporter's privilege exists, even if it was not warranted in *Branzburg*. The case has left confusion about whether any privilege exists. "It seems like we've had a split personality and different approaches at different times," Ted Boutrous, First Amendment lawyer and partner at Gibson, Dunn & Crutcher LLP, told the *Washington Post* for a July 20, 2013 story. "That's why I think the Supreme Court should step in."

New York's Highest Court Rules Fox News Reporter Need Not Testify in Aurora, Colo. Shooting Case

The New York Court of Appeals, the state's highest court, ruled on Dec. 10, 2013 that Jana Winter, a Fox News reporter, does not need testify to disclose a confidential source in Colorado. Winter was reporting on the July 20, 2012 mass shooting at a movie theater in Aurora, Colo. when she obtained a notebook that James Holmes, the accused shooter, allegedly sent to his psychiatrist. The notebook, which contained details of Holmes' plan, was sealed evidence, and the judge had issued a gag order preventing its release. On Jan. 17, 2013, Holmes' attorney, Douglas K. Wilson, sought a subpoena against Winter because he believed the leaker was a law enforcement official and the notebook might interfere with Holmes' right to a fair trial.

Fourteen law enforcement officials swore in the District Court for Arapahoe County, Colo. that they did not leak the notebook. Arapahoe County District Court Judge William Sylvester approved the subpoena request on Jan. 18, 2013, and asked the New York Supreme Court for New York County in Manhattan to issue a subpoena to force Winter, a New York resident, to testify in Colorado. The court relied on the Uniform Act to Secure the Attendance of Witnesses from Without the State in Criminal Cases (a law adopted in all 50 states) to argue Winter should be compelled go to Colorado to testify.

New York County Criminal Court Judge Larry Stephen signed the subpoena on March 14, 2013. The Supreme Court Appellate Division, First Department in New York affirmed Judge Stephen's decision to enforce the subpoena in a 3-2 decision on Aug. 20, 2013. *Holmes v. Winter*, 970 N.Y.S.2d 766 (N.Y. App. Div. 1st Dept. 2013). The appellate court concluded that the subpoena only compelled Winter to appear, and she could still try to assert a privilege not to reveal her source when she testifies.

> "A journalist's ability to go beyond official press releases and uncover the facts that authorities, corporations, or even just private individuals might prefer be kept hidden — the very definition of an investigative reporter — depends almost entirely on the journalist's ability to cultivate and maintain relationships with sources."
>
> **— Christopher T. Handman**
> **Attorney,**
> **Hogan Lovells U.S.**

One of the dissenting judges, Judge David Saxe, wrote that New York has a policy "in favor of protecting the identity of investigative reporters' confidential sources." He said that New York's shield law, N.Y. Civ. Rights Law § 79-h, grants journalists stronger protection than the Colorado Press Shield Law, C.R.S. § 13-90-199. New York's shield law is "absolute," according to Judge Saxe. Colorado's law, on the other hand, weighs the journalist's First Amendment concerns against the interest of the party seeking information.

New York's highest court considered whether to uphold the subpoena on Nov. 12, 2013. The court ruled in a 4-3 decision on Dec. 10, 2013 that Winter cannot be ordered to testify in Colorado and nullified the subpoena. *Holmes v. Winter*, No. 245 (N.Y. Ct. App. Dec. 10, 2013), available online at http://www.nycourts.gov/ctapps/Decisions/2013/Dec13/245opn13-Decision.pdf. The decision marks the end of the case; Winter will not have to testify in Colorado. "New York journalists should not have to consult the law in the jurisdiction where a source is located or where a story 'breaks' (assuming either is ascertainable) in order to determine whether they can issue a binding promise of confidentiality," Justice Victoria Graffeo wrote in the majority opinion. The majority concluded that there is "no principle more fundamental or well-established than the right of a reporter to refuse to divulge a confidential source."

The three dissenting justices argued that Colorado's shield law, not New York's, should apply because Winter's newsgathering occurred in Colorado. "The majority is holding, in substance, that a New York reporter takes the protection of New York's Shield Law with her when she travels — presumably, anywhere in the world," wrote Justice Robert Smith. "This seems to me an excessive expansion of New York's jurisdiction, one that is unlikely to be honored by other states or countries or to attain the predictability that the majority says is its goal." One of Winter's lawyers, Dori Ann Hanswirth of the Washington, D.C.-based firm Hogan Lovells U.S., told the Albany *Times Union* for a Nov. 11, 2013 story that Winter would have gone to jail before revealing her sources' identities.

"Today's ruling is a major win for all journalists," said Fox News Chairman and CEO Roger Ailes for a Dec. 10, 2013 Fox News story. "The protection of Jana Winter's confidential sources was necessary for the survival of journalism and democracy as a whole. We are very grateful that the highest court in New York State agreed with our position."

"A journalist's ability to go beyond official press releases and uncover the facts that authorities, corporations, or even just private individuals might prefer be kept hidden — the very definition of an investigative reporter — depends almost entirely on the journalist's ability to cultivate and maintain relationships with sources," one of Winter's attorneys, Christopher T. Handman of Hogan Lovells U.S., stated in a brief to the New York court. "If a New York reporter can be stripped of her protections under New York's public policy simply because the reporter crossed state lines, New York's robust public policy in favor of

Privilege *continued on page 12*

Privilege *continued from page 11*

confidential sourcing will become a dead letter for all but the most parochial stories."

"This is an important victory for journalists everywhere, and it protects the ability for the public to get the information it needs to self-govern," said Dave Cuillier, Society of Professional Journalists (SPJ) president, in a Dec. 10, 2013 statement. Hanswirth, Winter's attorney, told *USA Today* for a Dec. 10, 2013 story, "We are absolutely thrilled and delighted that New York state's highest court has once again reaffirmed how important the protection of confidential sources is to the proper functioning of our society."

Illinois Patch.com Reporter Held In Contempt For Refusing to Reveal Source of Leak of Police Reports in Murder Case

Joe Hosey, an editor for Joliet, Ill.'s Patch.com site, has refused to comply with a judge's order that he must disclose a confidential source. Patch.com is an online news organization with branches across the country that specializes in covering local issues. Early in 2013, Hosey obtained police reports about the murders of two men, Terrance Rankins and Eric Glover. The reports disclosed grisly details about the murders and the four individuals charged with strangling the men. Hosey wrote a series of articles for Patch.com published between February and March 2013 about the murders based on the reports. After Hosey published his articles on Patch.com, Will County Judge Gerald Kinney issued a gag order in the case against the defendants because defendant Bethany McKee's attorney, Chuck Bretz, argued the articles could taint the jury pool.

Bretz filed a motion to compel Hosey to disclose who leaked the confidential reports. Judge Kinney ordered Hosey to hand over the reports from his confidential source on Aug. 31, 2013. If the source could not be identified from the documents, the judge wrote, Hosey would have to give the court an affidavit identifying the source. Judge Kinney concluded that the Illinois reporter's privilege statute, 735 ILCSA 5/8-901 *et seq.*, did not apply because the state had exhausted all other sources of information to find the source of the leak. The court held hearings on the motion and received affidavits from more than 500 individuals at law firms, police agencies, the Will County State's Attorney's Office and Will County Public Defender's Office representing that they did not leak the reports.

Finding the source of the leak is in the public interest because the information contained in the leaked reports might impact the trial, Judge Kinney wrote. He noted it might also prove that the leaker violated the secrecy of a grand jury or otherwise broke the law by leaking the reports. If the leaker is an attorney, he or she could be held in contempt of court. If the individual is one of the 500 who signed an affidavit denying being the source, he or she could face perjury charges, the judge wrote.

> "The leaked records here were police reports about one of the most grisly crimes in recent history. No news organization or journalist should face punitive fines and jail for revealing information so obviously in the public interest."
>
> **— Chuck Tobin**
> **Attorney,**
> **Holland & Knight**

On Sept. 20, 2013, Judge Kinney held Hosey in contempt of court for refusing to hand over the leaked documents or reveal his source. The judge fined Hosey $1,000 and another $300 per day until he reveals his source, but stayed the fines while Hosey appeals the order. Hosey's attorney, Kenneth Schmetterer, asked the judge to enter the contempt order so he could appeal it because Hosey did not intend to reveal his source. As the *Bulletin* went to press, Hosey was awaiting the ruling on his appeal.

SPJ's Cuillier wrote in a Sept. 4, 2013 post on his blog "Freedom of the Prez" that "[s]ociety depends on leakers." He added, "We rely on people providing us information that we care about, even if the government doesn't want it out. Even if the information is inconvenient. Some of the best reporting — incredible journalism that makes a difference — is based on such leaks."

The Radio Television Digital News Association (RTDNA) agreed with Cuillier in a Sept. 26, 2013 post on its website. RTDNA said there is no evidence that the court could not identify the leaker through other means. "Judge Kinney's ruling is clearly an overreach and one that is designed to seriously chill journalists in Illinois," said Mike Cavender, RTDNA Executive Director. "It's in direct conflict with the state's shield law."

Chuck Tobin, a First Amendment attorney with Holland & Knight in Washington, D.C., told *USA Today* for an Oct. 14, 2013 story, "The identity of the person who leaked the police reports to the Patch won't help the court decide whether the defendants are guilty or innocent of these terrible murders. So there doesn't seem to be any interest in this case that would outweigh the public's interest, under the Illinois shield law, in helping reporters honor their promises to sources." He continued, "The leaked records here were police reports about one of the most grisly crimes in recent history. No news organization or journalist should face punitive fines and jail for revealing information so obviously in the public interest." In his order compelling Hosey to reveal his source, Judge Kinney wrote that there is a significant interest in preventing leaks concerning criminal cases. "In this era of digital media where information is available to the public immediately, it is more important than ever that this Court balance the rights of the parties appropriately," Kinney wrote. "This Court is aware of its duty and obligation to protect the First Amendment Rights of reporters, but cannot envision where those rights are superior to the fair trial rights of individuals charged by the State with the most serious criminal offenses."

– Cassie Batchelder
Silha Research Assistant

Courts Expand Protection for Online Speech, Define When Some Online Speech Is Private

Courts have granted protection to unique types of online speech under the First Amendment in recent months. United States appellate courts have held that actions by users on Facebook and rankings based on online users' opinions are entitled to First Amendment protection. Meanwhile, a federal district court held that comments posted on someone's Facebook wall are protected to a limited extent under the Stored Communications Act. The decisions demonstrate courts' willingness to recognize speech rights in novel online environments and also raise questions about how far courts will go to protect Internet speakers' rights.

ONLINE SPEECH

Fourth Circuit Court of Appeals Rules that a Facebook "Like" Constitutes Protected Expression

The United States Court of Appeals for the Fourth Circuit addressed speech on Facebook in September 2013. It held that the action of "liking" a post on Facebook is speech that warrants First Amendment protection. *Bland v. Roberts*, 2013 WL 5228033 (4th Cir. 2013).

The "like" function allows a Facebook user to click a button to express a "thumbs-up" symbol beside a post made by another user. The name of the user expressing the "like" and a link to that user's Facebook page then appears below the original post. This button got Daniel Ray Carter, Jr., an employee in the Hampton, Va. sheriff's office, in trouble. Six plaintiffs alleged they were fired from the sheriff's office for supporting the candidate for sheriff running against the incumbent sheriff, their boss B.J. Roberts. Carter expressed his support by clicking the "like" button for the Facebook page of the opposing candidate. All six former employees filed suit against Roberts. Carter argued Roberts fired him in retaliation for expressing his support for the opposing candidate, violating his First Amendment right to free speech. Roberts argued that clicking the "like" button is not speech protected by the First Amendment.

The United States District Court for the Eastern District of Virginia first ruled on the case in April 2012. *Bland v. Roberts*, 857 F.Supp.2d 599 (E.D. Va. 2012). United States District Court Judge Raymond A. Jackson held that "liking" the candidate's page was not constitutionally protected speech. Judge Jackson wrote that the action was not a "substantive statement" that constituted a specific enough message to warrant First Amendment protection. He suggested that extending protection to the mere action of pressing the "like" button would require the court to "attempt to infer the actual content" of what Carter meant when he liked the Facebook page. The plaintiffs then appealed the decision to the Fourth Circuit Court of Appeals.

> "We commend the Fourth Circuit for recognizing that interactions in social media deserve the same protection as talking from a soapbox on the street corner."
>
> **— Rebecca Glenberg**
> **Legal Director,**
> **ACLU of Virginia**

Writing for the appellate court, Chief Judge William B. Traxler reversed the district court judgment as to the First Amendment claim. "On the most basic level, clicking on the 'like' button literally causes to be published the statement that the User 'likes' something, which is itself a substantive statement," Judge Traxler wrote. "In the context of a political campaign's Facebook page, the meaning that the user approves of the candidacy whose page is being liked is unmistakable." He noted that although the writing of a statement requires several keystrokes, the fact that clicking a "like" requires merely one keystroke "is of no constitutional significance."

The court concluded that "liking a political candidate's campaign page communicates the user's approval of the candidate and supports the campaign by associating the user with it." Judge Traxler compared the act of "liking" a Facebook page to placing a political sign in one's yard. The United State Supreme Court granted First Amendment protection to political signs in yards in *City of Ladue v. Gilleo*, 512 U.S. 43 (1994). The appeals court concluded that just as posting a sign in one's yard shows support for a campaign, "liking" a campaign page demonstrates open support for a candidate.

By a 2-1 majority, however, the court ultimately held that the sheriff had qualified immunity from the plaintiffs' suit. The law prior to the incident, two of the three judges agreed, did not clearly establish the right to a "like" as protected speech. This allowed the sheriff to escape liability for the terminations. Judge Ellen Lipton Hollander concurred in part and dissented in part because she disagreed that Roberts should be protected from liability by qualified immunity. She wrote that, at the time the plaintiffs were discharged, "the law was clearly established" that they "could not be fired on the basis of political affiliation."

Several organizations voiced their support for the Fourth Circuit's ruling, at least on the discussion of a "like's" place in First Amendment jurisprudence. Having filed an *amicus* brief in support of Carter, Facebook itself commended the decision. "We are pleased the court recognized that a Facebook 'like' is protected by the First Amendment," Pankaj Venugopal, Facebook's associate general counsel, said in a statement.

The American Civil Liberties Union also expressed satisfaction with the result. "We commend the Fourth Circuit for recognizing that interactions in social media deserve the same protection as talking from a soapbox on the street corner," said ACLU of Virginia Legal Director Rebecca Glenberg. "From wearing buttons on their clothing to placing signs in their yards, Americans have a long and constitutionally protected tradition of publicly voicing their political preferences." The ACLU of Virginia wrote an *amicus* brief in support of the plaintiffs.

The decision in *Bland v. Roberts* is "an excellent example of substance triumphing over form, and a model for other courts called upon to evaluate freedom of expression online," Jeff Hermes, director of the Digital Media Law Project (DMLP), wrote in a Sept. 19, 2013 post on the DMLP blog. Hermes, however, criticized the court for letting the sheriff

Online speech, *continued on page 14*

Online speech, *continued from page 13*

"off the hook" by finding that the speech right was not previously established.

The Fourth Circuit's decision shows the court "understands the potential for Facebook — even the meager 'like' function — to communicate important ideas in small but powerful ways," said Dahlia Lithwick, senior legal editor at *Slate*. In a Sept. 20, 2013 column in the online magazine, Lithwick applauded the court for its understanding of the power of technology to spread one's opinions broadly and effectively.

Some have questioned how far courts will go in protecting online speech. The "like" in *Bland* was specific to political speech, noted Steve Silverman, attorney at Kluger, Kaplan, Silverman, Katzen & Levine, P.L. in Miami, Fl., in an Oct. 16, 2013 post on the firm's blog. Political speech traditionally receives the most First Amendment protection, and Silverman speculated that it will be interesting to see how courts apply this decision to other online contexts. Brian Fung, technology reporter for the *Washington Post*, questioned in a Sept. 18, 2013 post for the newspaper's technology policy blog "The Switch" how the ruling in *Bland* will apply to other opportunities to share or post information online. "What happens when I only ironically like something but don't literally support what's being liked? . . . Is the fact that I linked to Slate just now an endorsement of Slate?" Fung concluded, "While [*Bland*] is an unquestionable victory for the First Amendment, it actually raises more questions than it answers."

Online Lists Created from Users' Rankings are Protected Opinions, Rules Sixth Circuit Court of Appeals

The United States Court of Appeals for the Sixth Circuit unanimously held in August 2013 that an online list that ranked businesses based on certain qualities as rated by online users receives First Amendment protection as opinion. *Seaton v. TripAdvisor LLC*, 728 F.3d 592 (6th Cir. 2013).

TripAdvisor LLC, a website that provides travel information to its users, published a list on its website called "Dirtiest Hotels, as reported by travelers on TripAdvisor." The Grand Resort Hotel and Convention Center in Pigeon Forge, Tenn. topped the undesirable list. Its owner, Kenneth Seaton, sued TripAdvisor for defamation, false light invasion of privacy, injurious falsehood, and tortious interference with business relations. TripAdvisor moved to dismiss the claims, and the District Court for the Eastern District of Tennessee granted the motion on the grounds that the list was protected opinion. *Seaton v. TripAdvisor, LLC*, No. 3:11-cv-549, 2012 WL 363794 (E.D. Tenn. Aug. 22, 2012). Seaton appealed the district court's decision.

The Sixth Circuit unanimously affirmed the district court's opinion. To prove defamation, a plaintiff must show that the statement could reasonably be interpreted as stating facts about the subject. The United States Supreme Court in *Milkovich v. Lorain Journal Co.*, 497 U.S. 1 (1990), held that statements of opinion cannot serve as a basis for a claim of defamation unless the opinions themselves are based on false statements of fact (e.g. falsely calling someone a liar). Writing for the court, Circuit Judge Karen Nelson Moore said that the list "employ[ed] loose, hyperbolic language and its general tenor undermine[d] any assertion by Seaton that the list communicates[d] anything more than the opinions of TripAdvisor's users."

The court said that the word "dirtiest" was a hyperbole that could not be considered a statement of fact because it is a "superlative of an adjective that conveys an inherently subjective concept." Further, the court noted that the list was specifically identified as reflecting the rankings of hotels by the site's users.

Seaton had argued that the list was misleading, saying that the word "dirtiest" suggested objectivity, when the list was actually based on users' subjective rankings of hotels. He said the numerical rankings lended objectivity to the list. The court disagreed with Seaton, holding that TripAdvisor's method of assembling the list was clearly inherently subjective and the use of numbers does not make the rankings objective statements of facts. Thus, the list was protected opinion.

Seaton also argued that because TripAdvisor held itself out as a trusted authority on travel advice, the list should be taken as fact. The court disagreed, noting that the site claims credibility because so many users share their opinions on it. The court also acknowledged the ubiquity of such lists online. Because lists ranking various qualities have become commonplace, the court concluded that the broader context of the Internet should suggest to readers that the lists are based on opinion, not fact.

The DMLP submitted an *amicus* brief in the case to support TripAdvisor at the appellate level. In an Aug. 29, 2013 post on the DMLP blog, director Jeff Hermes explained that if the court had found that the methodology behind such lists did not constitute protected opinion, the constitutional status of "crowdsourced data" used to reach conclusions in academic research and data journalism might come under fire. "Allowing debates over methodology to devolve into defamation claims could substantially chill the advancement of research on important but sensitive issues," Hermes wrote.

Eric Goldman, professor at Santa Clara University School of Law, approved of the result, but argued the Sixth Circuit's opinion might have left the law about lists "muddled and unpredictable." In an Aug. 30, 2013 post on his "Technology & Marketing Law Blog," Goldman argued that the decision does not provide a way for future courts to determine the difference between lists based on opinions and those that do make factual assertions.

Goldman also expressed concern at the court's deference to TripAdvisor's methodology. "Taking the court's conclusion to its logical extreme, TripAdvisor could have used a defective or even corrupt methodology and still not be liable for defamation because the 'dirtiest' label could never be defamatory," Goldman wrote. If a list-maker had a "malicious" motive behind its subjective rankings, Goldman argued, the subject of the list might have a claim for defamation. He concluded that the court's "weak judicial analysis" suggests that courts do not "want to see lawsuits over compilations of user ratings and comments."

Other courts have heard defamation cases based on online reviews by users as websites that allow customers to rate businesses and service providers, like Yelp.com and AngiesList.com, have proliferated in recent years. (For examples of defamation cases based on online comments, see "Recent Cases Put Online Defamation in the Spotlight" in the Winter/Spring 2013 issue of the Silha *Bulletin*.) Like the Sixth Circuit's decision in *Seaton*, other courts have dismissed claims of defamation when users' comments contain obvious hyperbole or are clearly statements of opinion, not fact. These cases, in conjunction with *Seaton*, show that protection for online opinions is robust.

Federal District Court Applies the Stored Communications Act to Facebook Wall Posts

In August 2013, the United States District Court for the District of New Jersey held that the Stored Communications Act, 18 U.S.C. § 2701

et seq., protects posts made on an individual's Facebook wall. *Ehling v. Monmouth-Ocean Hospital Service Corp.*, No. 2:11-cv-3305 (WMJ) (D.N.J. Aug. 20, 2013). A Facebook user's wall is the part of the individual user's page on which the user and those to whom the user grants access can post content, including status updates, links, and photographs.

The plaintiff, Deborah Ehling, was a nurse and paramedic. She was the president of her union. Her employer, Monmouth-Ocean Hospital Service Corporation, once suspended Ehling with pay for posting a statement on her Facebook wall that paramedics should have let a patient, a perpetrator of a June 2009 shooting at the United States Holocaust Memorial Museum, die. One of Ehling's co-workers, who was friends with her on Facebook, gave the post to the hospital unsolicited. The hospital decided that her post showed a "deliberate disregard for patient safety." Over her years of employment, Ehling accrued a significant disciplinary record for attendance problems, which eventually led hospital authorities to fire her. Ehling filed suit against the hospital for violating the Stored Communications Act by accessing her Facebook wall following the museum shooting incident. Other claims included violation of the Family Medical Leave Act, violations of the New Jersey Law Against Discrimination, violation of the Conscientious Employee Protection Act, and invasion of privacy.

Judge William J. Martini concluded that Facebook wall posts are a type of Internet communication protected by the Stored Communications Act. The Act, which falls under Title II of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522, protects electronic communications that are configured to remain private, Judge Martini wrote. The Act covers electronic communications transmitted via an electronic communication service that are maintained in electronic storage and that are not public. A person who, unauthorized, accesses electronic communications or exceeds permitted access in violation of this law is liable for damages. Judge Martini decided that Facebook wall posts are electronic communications because they are made over the Internet and that Facebook is an electronic communication service within the meaning of the law. Further, Facebook archives posts on its servers "for backup purposes."

> "The touchstone of the Electronic Communications Privacy Act is that it protects private information. . . . When users make their Facebook wall posts inaccessible to the general public, the wall posts are 'configured to be private.'"
>
> **— William J. Martini**
> **Judge,**
> **U.S. District Court for the District of New Jersey**

The real issue for the court hinged on whether the posts are public or private within the meaning of the law. "The touchstone of the Electronic Communications Privacy Act is that it protects private information," Judge Martini wrote. He then discussed the various options that Facebook offers for the privacy of users' walls, emphasizing that "[a]ccess can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user." He held that "when users make their Facebook wall posts inaccessible to the general public, the wall posts are 'configured to be private'" under the Act. Critically, Ehling had configured her privacy settings to ensure that only those with whom she was friends on Facebook could see the posts on her wall. Ehling did not receive relief, however, because Judge Martini concluded that the hospital did not exceed access to her Facebook wall under the Stored Communications Act. The hospital received the wall post from one of Ehling's authorized Facebook friends, a co-worker, who printed it and brought it to the hospital. Judge Martini wrote that Ehling's co-worker and Facebook friend, "voluntarily provided [the posts to the hospital] . . . without any coercion or pressure." Judge Martini dismissed Ehling's Stored Communications Act claim, saying she "provided no evidence to support her theory that access to the Facebook page was unauthorized." This reasoning also resulted in the dismissal of her invasion of privacy claims. All of Ehling's remaining claims were dismissed for other reasons.

The case follows in a recent line of cases, including *Bland v. Roberts*, above, that suggest employers should use caution when it comes to employees' social media accounts, wrote Lindsay Burke, attorney at Covington & Burling LLP, in a Sept. 4, 2013 post for the firm's "Inside Privacy" blog. Allen Smith, attorney and the manager of workplace law content for the Society for Human Resource Management (SHRM), noted in a Sept. 6, 2013 post on SHRM's Legal Issues page that the court's reasoning suggests that an employer would violate the Stored Communications Act if it forced an employee to disclose the Facebook wall posts of another employee. (For more on recent legislation and cases involving employee privacy online, see "Social Media Policies Threaten Employee Privacy" in the Fall 2012 issue of the Silha *Bulletin*.)

– Cassie Batchelder
Silha Research Assistant

California Legislators Address Data Protection and New Technology on Several Fronts

CALIFORNIA LEGISLATION

With a burst of legislation, the California legislature tackled several topics related to privacy in the fall of 2013. New and amended laws addressed young peoples' control over their online presence, subpoenas of journalists' records that are held by third parties, the phenomenon of revenge porn, greater disclosure of online tracking of consumers, increased notification to consumers for data breaches, and photography of children by paparazzi. These new laws demonstrate a continuation in the online realm of California's historical focus on matters of its citizens' privacy. Several of the laws also highlight tensions between privacy protections and the First Amendment.

California "Online Eraser" Law Attempts to Give Children More Control Over Their Online Presence, But May Face Constitutional Challenges

California lawmakers, concerned about minors' online activities and potential long-term ramifications, gave them an "online eraser" to take back content they posted online when Gov. Jerry Brown signed California SB 568 into law on Sept. 23, 2013. It is codified at Cal. Bus. & Prof. Code § 22581 (West 2013).

The law targets operators of websites, online services, online applications, and mobile applications "directed to children." These operators must permit children under the age of 18 who are registered users of their services "to remove, or to request and obtain removal of content or information posted" on the operator's site, service, or application. This content could include, for example, compromising photographs. The statute requires that operators provide both notice to minors that they can remove content and instructions to explain how the user can remove content. An operator does not need to completely delete the content from its servers to comply with the law. Instead, an operator simply can make the content invisible to other users and keep the content intact on its servers.

The statute includes several exceptions. The "online eraser" does not apply to content posted by a third party. If a third party reposts the original post by the child seeking removal, the post by the third party need not be erased. Also, operators cannot remove the content if state or federal law requires that the operator maintain it. Finally, if the "operator anonymizes the content or information" — i.e. removes any information identifying a minor with the content — it need not provide the erasure option.

> "This [bill] will restrict minors' access to constitutionally protected material, limit their opportunities for speech, and discourage development of content designed for younger audiences."
>
> **— Emma J. Llansó**
> **Policy Counsel,**
> **Center for Democracy & Technology**

Operators have just over a year to figure out how to allow for the removal of posts. The law does not go into effect until Jan. 1, 2015.

California's law expands on federal law, which already provides a provision governing the use of children's information online. The Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, or COPPA, requires operators who have knowledge that they are collecting information from children under the age of 13 to provide notice of what information they are collecting, explain how the operator uses it, and give children's parents the chance to stop the collection of information. The law also adds to COPPA's standards by prohibiting advertising of various products, including guns, tobacco, alcohol, tattoos, drug paraphernalia, and tanning beds to children under the age of 18.

The bill's sponsor was Senate President Pro Tem Darrell Steinberg (D-Sacramento). "This is a good business practice that should filter through the industry," Rhys Williams, Steinberg's press secretary, told *The Huffington Post* for a Sept. 24, 2013 story. "These companies are keen to avoid bad press just as parents are keen to avoid bad attention toward their children." The new law does not allow parents to request removal of their children's content.

However, some have criticized the law as failing to achieve its goal of giving children more control over their online presence than they already have. Facebook, Twitter, and other social media sites already provide users with a way to delete their own posts from others' view without deleting them from the operator's servers, according to a Sept. 24, 2013 post by Gregory Ferenstein, a journalist for the technology news blog TechCrunch. Ferenstein also noted that, online, "embarrassing photos spread virally, and Internet archives automatically create copies of nearly every piece of information on the web," making complete deletion nearly impossible. This reality, he suggests, makes California's law unrealistic and ineffective.

Eric Goldman, professor at Santa Clara University School of Law, sees several flaws with the law. He noted in a Sept. 24, 2013 blog post for *Forbes* that the law might run afoul of the Commerce Clause. U.S. Const. art. I, § 8, cl. 3. The clause means that only the United States Congress can regulate commerce between states. The state where an Internet user is located is often unclear. Because the law "doesn't clarify its jurisdictional nexus" and websites do not always know where their users are located, the law leaves a "question open for future fights and a potential Constitutional challenge." In other words, because websites might have to apply California's standards to users across the country, the sites could argue the law is an unconstitutional burden on interstate commerce.

Goldman and Ferenstein both expressed concern that California's online eraser is similar to the European Union's proposed "right to be forgotten," which would give EU citizens the right to unilaterally request that information about themselves online be deleted, or the "right to erasure." (For more on the "right to

be forgotten," see "Amid Skepticism, Uncertainty, Culture Clash, EU Eyes Online 'Right to be Forgotten'" in the Fall 2011 issue of the Silha *Bulletin*, the "Director's Note" in the Summer 2011 issue, and "Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms" on the first page of this issue.) Goldman said the California law has the potential to literally "rewrit[e] history" and "hinder[] society's ability to understand where we came from and why things are the way they are."

First Amendment concerns also animate criticism of the online eraser. Emma J. Llansó, policy counsel for the Center for Democracy & Technology, a civil liberties organization that focuses on the application of the First Amendment online, testified before the California State Assembly's Committee on Arts, Entertainment, Sports, Tourism, and Internet Media on June 25, 2013, opposing the bill. She expressed concern over the bill's focus on platforms that are "directed to minors," which she said is too vague. "When faced with obligations to treat minors' content differently or to restrict certain marketing or advertising material to minors, many operators unsure of their status under this bill will opt to bar minors from their sites and services altogether," Llansó testified. "This will restrict minors' access to constitutionally protected material, limit their opportunities for speech, and discourage development of content designed for younger audiences."

California Legislature Criminalizes Some Forms of "Revenge Porn" with a Law that Raises Constitutional Questions

In recent years, a number of websites purveying so-called "revenge porn" have emerged. The term revenge porn refers to pornographic images and videos that ex-lovers post of their ex-girlfriend or boyfriend on the Internet without permission. The pictures are often accompanied by the individual's contact information in order to encourage harassment of the victim. Revenge porn first made headlines in 2011 when Hunter Moore, an early purveyor of revenge porn who owned the website isanyoneup.com, said he did not mind benefitting from public revenge in a November 2011 interview with CNN's Anderson Cooper. The phenomenon has attracted significant national attention as victims have emerged around the country, some of whom have sued their exes for copyright infringement and invasion of privacy, according to a Sept. 23, 2013 story in *The New York Times*. Until enactment of the California statute, New Jersey was the only state with a law that could be used to criminalize revenge porn. The state's 2003 law makes it a felony to post secretly recorded videos or photographs online, but the law was not passed with revenge porn in mind. N.J. Stat. Ann. § 2C:14-9.

California became the first state to pass a law specifically targeting revenge porn with SB 255, codified as Cal. Penal Code § 647(j)(4). It was signed into law on Oct. 1, 2013. The law makes it a misdemeanor to photograph or film another person in a state of undress and distribute the image "with the intent to cause serious emotional distress" if the person depicted in the images "suffers serious emotional distress." The law is specific to situations when the two people "agree or understand that the image shall remain private." Violation of the law is punishable by up to six months in jail and a $1,000 fine.

> "You need to be extraordinarily careful in criminalizing privacy law because of the risk you're going to deter legitimate speech."
>
> **— Jeff Hermes**
> **Director,**
> **Digital Media Law Project**

The law has faced criticism from both free speech proponents and advocates of victims of revenge porn. The Cyber Civil Rights Initiative (CCRI), an organization that advocates for protection of and legal recourse for revenge porn victims, maintains that the law fails to adequately address the types of photographs that constitute the majority of revenge porn cases: photos the victim takes of him- or herself and sends to the partner who later posts it. These images, known as "selfies," make up 80 percent of revenge porn images, according to a CCRI survey, released Sept. 10, 2013.

Others argue that the law does no more to protect victims than existing anti-stalking or anti-harassment laws. "As usual, one of the key questions is how existing law has failed and what behavior is being newly criminalized," said Eric Goldman, professor of law at Santa Clara University, for an Aug. 27, 2013 story in *The New York Times*.

The law also raises First Amendment concerns. "You need to be extraordinarily careful in criminalizing privacy law because of the risk you're going to deter legitimate speech," Digital Media Law Project director Jeff Hermes told NBC News for a Sept. 3, 2013 story. "With the California bill, I don't see an exemption here for material that's legitimately newsworthy." Privacy law, such as the tort of publication of private facts, generally allows an exception for speech that relates to newsworthy topics that involve matters of public concern. Hermes provided the example of a salacious or compromising photographs of a political candidate with a "clean" image. "The distribution of these photos could indicate (to voters) that candidate might be lying about their past," Hermes said.

State Sen. Leland Yee (D-San Francisco and San Mateo County) voted against the law. "First Amendment protections are fundamental to our free society," he said in a statement to NBC News. "While I appreciate the intent of this legislation, I feel it was too broadly drawn and could potentially be used inappropriately to censor free speech."

Anti-Paparazzi Law Prevents Photography of the Children of Public Figures

Following the testimony of several celebrities, California restricted the activities of paparazzi photographers and videographers with a law Gov. Brown signed on Sept. 24, 2013. SB 606, codified at Cal. Penal Code § 11414, increases the penalty for harassment — defined as activity that "seriously alarms, annoys, torments or terrorizes" — of a child. It includes photographing or recording a child without the consent of a parent or legal guardian, and it also prohibits "following the child's activities or lying in wait" for the child. Although the law does not refer to celebrities, it prohibits harassment if the violator is motivated by the child's parent or guardian's "employment." The existing harassment law already subjected offenders to up to six months in jail and a $1,000 fine. The penalty under SB

CA Legislation, *continued on page 18*

CA Legislation, *continued from page 17*

606 is increased to up to one year in jail and a $10,000 maximum fine. The law also creates a private cause of action, allowing parents to sue violators on behalf of their children.

Actress and mother of three Jennifer Garner testified in support of the bill before the California Assembly Judiciary Committee in August 2013. "I chose a public life and understand that this means sacrifices in terms of privacy for our jobs," Garner said. "In my case this means that I am sometimes photographed. However, my three children are private citizens, and more than that — at one, 4 and 7 years old — they're just little kids."

Legislators said that the law does not violate the First Amendment because it states that "the act of transmitting, publishing, or broadcasting a recording of the image or voice of a child does not constitute commission of the offense." Therefore, they say it targets conduct, not speech.

However, some media organizations disagree. "We believe the increased penalties and liabilities related to such actions improperly abridges [*sic*] First Amendment protected activity occurring in traditional public forums and other places where a person normally has no reasonable expectation of privacy," Mickey Osterreicher, general counsel for the National Press Photographers Association, wrote in an August 2013 letter opposing the law. "We are also extremely concerned that the bill as it pertains to photography and recording is overly broad and vague and infringes upon otherwise protected forms of speech and expression." He explained that the law specifically targets photographers because they take pictures, which is constitutionally-protected activity. It does not, in his mind, regulate only conduct.

Others have emphasized the importance of protecting even speech that seems repugnant. "Even though paparazzi may occupy the lowest rung of First Amendment activity, they still enjoy the Amendment's full protection," wrote Julie Hilden, an attorney focused on writing about First Amendment issues for outlets including Justia, a website about legal issues, for an Oct. 22, 2013 column in Justia's "Verdict" blog. "And they must, if we are to protect First Amendment activity, because in some contexts, there may be a fine line between paparazzi and more legitimate journalists."

Do-Not-Track Law Increases Disclosures to Consumers

The California legislature unanimously amended the California Online Privacy Protection Act (CalOPPA) of 2003, Cal. Bus. & Prof. Code §§ 22575-22579, to address new "do-not-track" technology. Websites use code known as "cookies" to collect information about their visitors. Many web browsers allow users to enable "do-not-track" technology that stops websites from collecting this information about users.

"Even though paparazzi may occupy the lowest rung of First Amendment activity, they still enjoy the Amendment's full protection. And they must, if we are to protect First Amendment activity, because in some contexts, there may be a fine line between paparazzi and more legitimate journalists."

— Julie Hilden Columnist, Justia

CalOPPA already required websites to have a privacy policy in which the operator explains what information it collects. AB 370, signed into law on Sept. 27, 2013, requires operators of commercial websites or online services that collect personally identifiable information about California residents through the Internet to disclose in their privacy policies whether the site "honors or complies" with do-not-track technology that "indicates a request to disable online tracking of the individual consumer who uses or visits its commercial Web site or online service." The operator must disclose the categories of personal information it collects and with whom it shares that information in the privacy policy.

"[T]his bill would increase consumer awareness of the practice of online tracking by websites and online services, such as mobile apps," California Assembly member Al Muratsuchi (D-Torrance) wrote in a June 18, 2013 analysis of the bill for the Assembly. "A.B. 370 will allow consumers to learn from a website's privacy policy whether or not that website honors a Do Not Track signal. This will allow the consumer to make an informed decision about their use of the website or service."

However, some criticize the law for its potential to hurt business interests. "While highly beneficial for research and ad-serving purposes, the use of tracking technologies to document users' behavior online, or via mobile apps, has garnered the attention of regulators concerned with its implication on consumer privacy," wrote Dominique R. Shelton and Paul G. Martino, attorneys with Los Angeles firm Alston & Bird LLP, for a Sept. 19, 2013 post on the firm's website. Shelton and Martino note that many studies show that advertising based on tracking consumers has proven highly beneficial for websites. (For more information about do-not-track technology and legislation, see "Legislators Seek Increased Consumer Privacy Protections; FCC and FTC Investigations of Online Companies Continue" in the Winter/Spring 2012 issue of the Silha *Bulletin*.)

Companies Must Provide Increased Notification to Consumers Under Amended Data Breach Law

California addressed consumers' increasing reliance on Internet services and accounts by heightening notification requirements for companies when breaches of data occur. SB 46, codified at Cal. Civ. Code § 1798, amended a law that already required companies to notify consumers when data breaches expose consumers' Social Security, driver's license, or credit card numbers, as well as medical and health insurance information.

The amended law, which Gov. Brown signed into law on Sept. 27, 2013, expands the definition of such sensitive personal information. It requires companies to notify consumers if their username or email address is compromised in conjunction with the password or the answer to a security question that would permit access to their accounts.

The company maintaining the breached data can provide notice through an "electronic or other form that directs the person whose personal

information has been breached promptly to change his or her password and security question or answer." The company can also advise users to take steps to protect their accounts and all others that may have been affected. If the breach involves information associated with an email account that the company has provided, the notice cannot be sent to that email account. Instead, it must be sent in written form via an alternative electronic notice, or the company must give notice to the user when they are connected to the company's site through an Internet protocol (IP) address that the company knows the individual regularly uses to access his or her account.

Other states are likely to follow California, wrote Jon Frankel, counsel with ZwillGen PLLC, a Washington, D.C.-based law firm focused on Internet law, in an Oct. 17, 2013 post on the firm's blog. Frankel wrote that the 45 states, plus the District of Columbia and Puerto Rico, that have data breach laws — which were inspired by California's first-of-its-kind 2003 law — differ significantly in their required notifications. California's data breach law is the most stringent, however, and it often makes sense for companies to choose to comply with the most restrictive state's law in all of its practices for ease of administration. He did note, however, that compliance with the most restrictive law "can be frustrating or even impossible to execute when a company experiences a data security breach."

California Shield Law for Journalists Increases Warning Time in Advance of Subpoenas on Records Held By Third Parties

In the spring of 2012, the U.S. Department of Justice secretly subpoenaed the telephone records of Associated Press reporters. In May 2013, the DOJ also executed a search warrant to obtain the emails of James Rosen, a Fox News reporter who the DOJ argued was a co-conspirator in a criminal leak case about a CIA source with knowledge of North Korea's nuclear program. (For more on the seizure of the AP's phone records, see "Justice Department Secretly Subpoenas Associated Press Phone Records" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

These incidents sparked an outcry about the Obama administration's treatment of journalists. In response, the DOJ amended its guidelines with respect to investigations involving journalists in the summer of 2013. The new guidelines offer expanded protection for journalists. One section in particular, "Reversing the Existing Presumption Regarding Advance Notice," amended the DOJ's policy on subpoenas issued to seize journalists' communication records held by third parties, like phone companies. In the past, the DOJ negotiated with the media before issuing a subpoena for records about reporters' newsgathering activities connected with an investigation, provided the negotiations did not threaten "the integrity of the investigation." The new guidelines ensure prior notification, unless the Attorney General determines that doing so would pose a "clear and substantial threat" to the investigation in question. The guidelines also allow the Attorney General to delay notification in "rare" cases, among numerous other provisions. (For additional information about the DOJ's new guidelines, see "Department of Justice Revises Guidelines for Investigating Journalists" in the Summer 2013 issue of the Silha *Bulletin*, and "Senate Considers Federal Reporter's Privilege Bill" on page 8 of this issue.)

The California legislature chose to mirror the DOJ's enhanced protection of journalists with respect to subpoenas of their third-party records with a bill Gov. Brown signed into law on Oct. 3, 2013. California's existing shield law already required law enforcement or other entities to give journalists five days' notice when seeking a subpoena for records in the journalists' possession. The new law, SB 558, codified at Cal. Evid. Code § 1070 (West 2013), requires that journalists or news organizations also receive five days' notice if law enforcement or anyone else issues a subpoena for their records that are held by a third party. The notice must explain how the records would materially further the case and why other sources of information were insufficient in that effort. The five days' notice provides journalists and media organizations with the opportunity to go to court to challenge the subpoena before it is executed.

> "The government has shown on some occasions a disregard for Freedom of the Press. California will protect the First Amendment."
>
> **— Ted Lieu**
> **California State Senator, (D-Torrance)**

The author of the bill, State Sen. Ted Lieu (D - Torrance), said in an Oct. 3, 2013 statement that the old shield law did not adequately address the rise of mobile communications and cloud computing, which many journalists now use for newsgathering. Individuals using cloud computing can store information on off-site servers that are connected to the Internet, which presents special issues when law enforcement seeks to subpoena those records. "The government has shown on some occasions a disregard for Freedom of the Press," Lieu said in the statement. "California will protect the First Amendment."

Media outlets in California spoke in favor of the law. "SB 558 will ensure that reporters will be able to continue to deliver to readers solid investigative stories about government activities without fear that officials can tiptoe around the Reporters' Shield law to access their sources and notes from the Cloud or cell phone providers," said Jim Ewert, general counsel for the California Newspaper Publishers Association, for an Oct. 3, 2013 statement. The Association sponsored the bill.

– Cassie Batchelder
Silha Research Assistant

Fifth Circuit Denies Enforcement of Canadian Defamation Judgment in Mississippi Court, Citing SPEECH Act

On Sept. 5, 2013, a unanimous panel of the United States Court of Appeals for the Fifth Circuit upheld a district court ruling granting summary judgment to a Mississippi blogger who argued that a Canadian defamation judgment could not be enforced against him because it violated the 2010 Securing the Protection of our Enduring and Established Constitutional Heritage ("SPEECH") Act, 28 U.S.C. § 4102. The case is the first time that the SPEECH Act has been cited at the appellate level. *Trout Point Lodge v. Handshoe*, 729 F.3d 481 (5th Cir. 2013).

SPEECH ACT

Douglas Handshoe ran the blog "Slabbed.org," which he defined as "Alternative New Media for the Gulf South." Among the topics that Handshoe wrote about were the scandals surrounding Aaron Broussard, who was Parish President of Jefferson Parish (La.). Broussard pleaded guilty to charges of bribery and theft in September 2012, an outcome that Handshoe credited to his reporting. In January 2010, Handshoe alleged that Broussard, who owned property in Nova Scotia, had an ownership interest in a hotel near his property called Trout Point Lodge. The hotel was owned by plaintiffs Vaughn Perret and Charles Leary, who were a same-sex couple originally from New Orleans. The New Orleans *Times-Picayune*, whose parent company Advance Publications owned Handshoe's blog, also reported on the connection between Broussard and Trout Point Lodge, alleging that Broussard let various contractors stay at the lodge as a kickback for doing business with Jefferson Parish. Perret and Leary informed the *Times-Picayune* that the story contained purported "factual errors in [its] reporting," which led the newspaper to retract the story.

Advance Publications severed ties with Slabbed.org, prompting Handshoe to move his blog to the free Wordpress platform. There, he continued to write about the plaintiffs and their alleged connection with Broussard. For example, in one post Handshoe wrote that "the Lodge's financial records would certainly contain evidence to . . . support the pay-to-Trout Point to play in Jefferson Parish allegations that are at the heart of this story." The district court acknowledged that Handshoe's posts could "be characterized as derogatory, mean spirited, sexist, and homophobic." Handshoe posted that Perret and Leary "had Champagne taste on a beer budget," "work as a unit to grift their way through life," and were "first-class bitches, common thugs, or plain ol' morons." He commonly referred to Perret and Leary in his posts as "the girls."

Perret and Leary brought a defamation action against Handshoe in the Supreme Court of Nova Scotia on Sept. 1, 2011. They argued that Handshoe's blog posts "were directly defamatory . . . by both true and false innuendo in that they would tend to lower the opinion or estimation of the plaintiffs in the eyes of others who read the defamatory publications as a series." In particular, Perret and Leary claimed Handshoe defamed them by alleging that they were involved with the Broussard corruption scandal and that their business was failing. Further, the plaintiffs claimed that Handshoe's "unabashed anti-gay, anti-homosexual rhetoric and rants . . . amplif[ied] and support[ed] . . . all the other defamatory imputations."

> "This decision demonstrates that foreign libel tourism will not be tolerated in our country, and with the advent of bloggers and other non-traditional types of media, the decision extends free speech freedoms to them, as well as main stream journalist [*sic*]."
>
> **— Bobby Truitt**
> **Truitt Law Firm**

In December 2011, the Nova Scotia court entered a default judgment against Handshoe after he did not appear in court to contest the action. Under Canadian law, claims are to be treated as proven if the defendant does not appear in court to contest them. The Nova Scotia court proceeded immediately to a damages hearing, at which it awarded $75,000 in general damages to Trout Point Lodge, and $100,000 in general damages to both Perret and Leary. It also awarded $25,000 in punitive damages, and $2,000 in costs. The court also issued an injunction against Handshoe, "restraining him from disseminating, posting on the Internet or publishing, in any manner whatsoever, directly or indirectly, any statements about the plaintiffs," and requiring him "to immediately remove any such materials from publication" on his blog.

In March 2012, Perret and Leary sought to enroll the judgment in the Circuit Court of Hancock County (Miss.), prompting Handshoe to remove the case to the federal District Court for the Southern District of Mississippi, where he moved for summary judgment by arguing the plaintiffs had not met their burden under the SPEECH Act to enforce the judgment. The SPEECH Act prevents foreign plaintiffs from enforcing defamation judgments in U.S. courts unless they can prove one of two things. First, plaintiffs could show that "the defamation law applied in the foreign court's adjudication provided at least as much protection for freedom of speech and press in that case as would be provided by the first amendment to the Constitution of the United States." Second, plaintiffs could show that "even if the defamation law applied in the foreign court's adjudication did not provide as much protection for freedom of speech and press as the first amendment to the Constitution of the United States . . ., the party opposing recognition or enforcement of that foreign judgment would have been found liable for defamation by a domestic court applying the first amendment to the Constitution of the United States and the constitution and law of the State in which the domestic court is located."

In December 2012, the district court granted Handshoe summary judgment, holding that Perret and Leary could not meet their burden under the SPEECH Act. Chief U.S. District Judge Louis Guirola, Jr. held that Canadian law does not provide as much protection against a defamation claim as U.S. law because Canadian law does not require that plaintiffs prove falsity. Guirola wrote that the district court could "[]not determine, based on the record before it, the truth or falsity of Handshoe's claims that the Plaintiffs are connected to Aaron Broussard's criminal activities." He wrote that the court would not "enforce a judgment in an action that, if brought in this Court, would depend upon the plaintiffs' proof that the statements at issue are false," which Guirola held the plaintiffs had not done. *Trout Point Lodge v.*

Handshoe, 2013 U.S. Dist. LEXIS 25138; 2013 WL 685978 (S.D. Miss. Feb. 25, 2013).

Perret and Leary appealed the ruling to the United States Court of Appeals for the Fifth Circuit. In their appellate brief, they argued that the district court ruling "hinged entirely upon the erroneous finding that [they] failed to prove . . . falsity." Perret and Leary argued that they did prove Handshoe's statements were false in their original claim to the Nova Scotia court, but because that court entered a default judgment on their behalf due to Handshoe's absence, they did not have to prove the falsity of the statements in court.

The Fifth Circuit upheld the district court's ruling. Writing for a unanimous panel, Judge Jennifer Walker Elrod agreed with the district court's logic that foreign plaintiffs could only successfully collect damages stemming from a foreign defamation judgment in the United States if they could meet one of the two standards under the SPEECH Act. As to the first standard, Elrod held that Canadian law did not provide Handshoe as much protection as he would have found under the First Amendment. "The most critical legal difference here is that a Canadian plaintiff — unlike a plaintiff subject to First Amendment and Mississippi state law — need not prove falsity as an element of its *prima facie* defamation claim," she wrote.

The plaintiffs' remaining option to prevail under the SPEECH Act was to show that the Mississippi state court, given the facts of the case, would have found Handshoe liable for defamation. Elrod again agreed with the district court that Perret and Leary had not proved that Handshoe's statements were false, and thus concluded that the plaintiffs did not meet the requirements of the second option for prevailing under the SPEECH Act. Elrod rejected the plaintiffs' argument that they did, in fact, prove falsity in the initial claim to the Nova Scotia court. She held that the plaintiffs "offer[ed] no facts to rebut or undermine most of Handshoe's statements." She pointed to the plaintiffs' own admission that Handshoe's statements were "defamatory by both true and false innuendo" as being "unclear regarding whether all, or just some, of Handshoe's statements [were] false." Elrod further held that some of Handshoe's blog posts were "statements of unverifiable opinion" protected by the First Amendment and were therefore not actionable in Mississippi.

Elrod also rejected the argument that the Nova Scotia court's own factual findings, which it made in the course of awarding damages, sufficiently proved the falsity of Handshoe's statements. These findings were void, she held, because they came after that court's default judgment against Handshoe; in other words, the process was backwards according to U.S. law, as a Mississippi court would have required proof of falsity before damages could be awarded. Elrod also found the Nova Scotia court's findings unconvincing, pointing out that the court "noted generically that some statements were 'erroneous,' but remained silent as to the truth of others."

U.S. legal scholars have hailed the Fifth Circuit's decision as a victory for press freedom. In a Sept. 13, 2013 post on his "Technology & Marketing Law Blog," Eric Goldman, professor at Santa Clara University School of Law, argued that the ruling would lead more international plaintiffs to file defamation actions against U.S. defendants in U.S. courts because the SPEECH Act essentially forces the plaintiffs to litigate the case twice. Goldman argued that obtaining foreign defamation judgments against U.S. defendants would now become "economically irrational" because they would offer plaintiffs only a means to clear their name under their own law and not the financial damages that would justify spending time and money on litigation.

> "If a person is defamed in Canada, and that's where the publication was read, one would have thought that the lawsuit is properly brought in Canada. If the defamer is situated in the United States, and, using the Internet, defames a Canadian, [the SPEECH Act] ends up leaving somebody [in Canada] without meaningful recourse. I think that's a concern."
>
> **— David Coles**
> **Barrister,**
> **Boyne Clarke**

Handshoe's lawyer, Bobby Truitt of the New Orleans-based Truitt Law Firm, told Goldman for his blog post that the Fifth Circuit's decision "demonstrates that foreign libel tourism will not be tolerated in our country, and with the advent of bloggers and other non-traditional types of media, the decision extends free speech freedoms to them, as well as main stream journalist [*sic*]."

The Trout Point Lodge litigation represents the first time the SPEECH Act was dispositive in preventing a foreign defamation judgment in the United States. In 2011, the Missouri Court of Appeals (E.D. 1st Div.) cited the SPEECH Act, as well as similar state statutes, to determine that a Canadian defamation judgment was not enforceable in Missouri state court. However, that court instead relied on the Full Faith and Credit Clause of the U.S. Constitution (Art. IV § 1), holding that the Canadian judgment was not entitled to full faith and credit in a Missouri court because it was not certified and authenticated. *Pontigon v. Lord*, 340 S.W.3d 315 (Mo. Ct. App. Apr. 19, 2011). Also in 2011, a Canadian corporation conceded before trial that the SPEECH Act precluded it from collecting damages from a Canadian defamation judgment against a Florida-based company. *Investorshub.com, Inc. v. Mina Mar Group*, 2011 U.S. Dist. LEXIS 87566, (N.D. Fla. June 20, 2011). (For more coverage on the passage of the SPEECH Act, see "Federal 'Libel Tourism' Law to Nullify Anti-Speech Rulings" in the Summer 2010 issue of the Silha *Bulletin*.)

David Coles of the Halifax, N.S.-based firm Boyne Clarke, who was involved in litigating the *Trout Point Lodge* case in Nova Scotia, told the Silha *Bulletin* in a Dec. 11, 2013 phone interview that he believed the Fifth Circuit's "categorization of Nova Scotia law was a bit off the mark." Coles argued that the SPEECH Act presented "real difficulties" to Canadian libel plaintiffs. "If a person is defamed in Canada, and that's where the publication was read, one would have thought that the lawsuit is properly brought in Canada. If the defamer is situated in the United States, and, using the Internet, defames a Canadian, [the SPEECH Act] ends up leaving somebody [in Canada] without meaningful recourse. I think that's a concern."

Brian MacLeod Rogers, a barrister and solicitor based in Toronto, told the Silha *Bulletin* in a Dec. 11, 2013 email that despite the Fifth Circuit's holding, the SPEECH Act "will not help [U.S.] defendants who have assets or income in Canada, as many U.S. businesses do." Therefore, Rogers said, "U.S. publishers would be wise to pay attention to Canadian law when publishing about those who could bring suit north of the border."

Brett Johnson
Silha *Bulletin* Editor

Copyright Decisions Emphasize the Broad Protections of the Fair Use Doctrine in Infringement Cases

Courts examining the fair use doctrine, a defense to copyright infringement, have expanded how much of the copyrighted works of others can be used in several high-profile cases in the second half of 2013. A federal district court in New York concluded that Google Books, a program that makes digital copies of copyrighted books, is a fair use of these works. The United States Supreme Court denied a petition for *certiorari* in a closely-watched case involving incorporation of a different artist's work into another a piece of art. The decision that stands from the United States Court of Appeals for the Second Circuit clarifies that artists have relatively expansive abilities to legally copy the work of others. Both decisions highlight that courts see fair use as a broad defense to claims of copyright infringement.

COPYRIGHT

Google Books Ruling Holds that Posting Books Online Constitutes a Fair Use of Works Protected by Copyright

Google's practice of scanning books and posting them online for its Google Books service is a fair use of authors' copyrighted works, a court concluded after eight years of litigation surrounding the service. Judge Oymin Chin of the United States District Court for the Southern District of New York granted Google's motion for summary judgment on Nov. 14, 2013. *Authors Guild, Inc. v. Google Inc.*, 2013 WL 6017130 (S.D.N.Y. Nov. 14, 2013).

Google reached agreements with several libraries in 2004 to create digital copies of books in the libraries' collections. Google Books delivers digital copies of books to participating libraries, has created an electronic database of books, and allows regular Google users to search books online, allowing users access to "snippets" of books, as the court explained. The Authors Guild filed a class action lawsuit against Google in 2005, claiming that Google's digitization of books violated authors' copyrights in their works. Judge Chin's November decision ruled on both parties' cross-motions for summary judgment as to whether Google's use of the authors' works constitutes fair use under the Copyright Act, 17 U.S.C. § 107.

Section 107 provides breathing room for certain uses of copyrighted works considered to be "fair." Courts must weigh four factors when deciding whether a defendant's use of a plaintiff's work is fair: "1) the purpose and character of the use; 2) the nature of the copyrighted work; 3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and 4) the effect of the use upon the potential market for or value of the copyrighted work."

Addressing the first factor, Judge Chin wrote that the character of Google's use of the books — digitizing them — "transforms expressive text into a comprehensive word index that helps readers, scholars, researchers, and others find books." He noted the use is transformative because Google Books does not "supersede or supplant books," but "adds value to the original, and allows for the creation of new information, new aesthetics, new insights and understandings." This weighed in Google's favor.

Considering the nature of the copyrighted work, Judge Chin said that this second factor also weighs in Google's favor because 93 percent of the digitized works are nonfiction, which is less creative than fiction and therefore warrants lesser copyright protection.

The third factor weighed against Google, Judge Chin wrote, because in many cases the "amount and substantiality of the portion used" included entire books. Although he noted that entire copies of works can sometimes constitute fair use, "Google limits the amount of text it displays in response to a search," so he found that this factor weighed slightly in the authors' favor.

As to the effect of the use on the potential market for the books, Judge Chin said Google's use was clearly fair. "Google does not sell the scans it has made of books for Google Books; it does not sell the snippets that it displays; and it does not run ads on the About the Book pages that contain snippets; it does not engage in the direct commercialization of copyrighted works," he explained. "Google does, of course, benefit commercially in the sense that users are drawn to the Google websites by the ability to search Google Books," he wrote. However, he concluded that Google Books "also serves several important educational purposes," which he said strongly weighed in Google's favor for the fourth factor.

Judge Chin suggested that the project benefits even the authors who filed suit because it "help[s] readers and researchers identify books" and provides an "About the Book" page that gives readers links to purchase the entire book. "Google Books will generate new audiences and create new sources of income," he wrote.

Judge Chin outlined the project's societal benefits. Citing language from the U.S. Constitution, he wrote that "[Google Books] advances the progress of the arts and sciences, while maintaining respectful consideration for the rights of authors and other creative individuals, and without adversely impacting the rights of copyright holders." He cited its usefulness as a research tool for identifying and purchasing books, for conducting full-text searches of books, for preserving books that are old or out-of-print, and for facilitating access to books for populations that have struggled with access in the past. "Indeed, all society benefits," he concluded.

The Authors Guild has said it will appeal the decision. Authors Guild executive director Paul Aiken told *Publishers Weekly* for a Nov. 14, 2013 story that "[t]his case presents a fundamental challenge to copyright that merits review by a higher court." Aiken said, "Google made unauthorized digital editions of nearly all of the world's valuable copyright-protected literature and profits from displaying those works. In our view, such mass digitization and exploitation far exceeds the bounds of the fair use defense." The National Writers Union also expressed disappointment in a Nov. 16, 2013 post on its website. "We continue to believe that Google's practices violate writers' copyrights," the organization stated. "These practices interfere with our ability to control and receive fair compensation for secondary uses of works included in the books that Google is scanning and using for its own purposes and profit."

Google issued a statement on Nov. 14, 2013, saying, "Google Books is in compliance with copyright law and acts like a card catalog for the digital age — giving users the ability to find books to buy or borrow." Others have also come out in favor of the decision. "[The American Library Association] applauds the decision to dismiss the long running Google Books case," Barbara Stripling, president of the ALA, told *Publishers Weekly* on Nov. 14, 2013. "This ruling furthers the purpose of copyright by recognizing that Google's Book search is a transformative fair use that advances research and learning." Kenneth Crews, the director of Columbia University Libraries, agreed. "[E]ven extensive digitization can be within fair use where the social benefits are strong and the harm to rightsholders is constrained," he wrote in a Nov. 14, 2013 post on the library's website. "There will be more to come as we transition into a new era of copyright, technology, and even reading."

Some commentators have observed that the decision seemed inevitable based on how technology has developed since the

lawsuit was originally filed. Timothy B. Lee, a journalist who covers technology policy for the *Washington Post*, wrote in a Nov. 14, 2013 post on the *Post*'s "The Switch" blog, "Many innovative media technologies involve aggregating or indexing copyrighted content." Lee argued that "[if the decision stands], it would expand fair use rights, benefiting many other technology companies." Jonathan Band, a copyright lawyer for the Library Copyright Alliance, which filed an *amicus* brief in support of Google, told *The New York Times* for a Nov. 15, 2013 story, "There's an understanding that the way this technology works, there's going to be copying." He argued "that there's a sensibility in the courts that as long as the whole work is not displayed, and as long as the rights-holder isn't harmed, then this copying that goes on behind the curtain just doesn't matter."

Supreme Court Refuses to Hear Fair Use Case, Allowing a Broad Definition of Fair Use to Stand

On Nov. 12, 2013, the United States Supreme Court denied a petition for *certiorari* filed by an artist raising the question of when it is legal for an artist to incorporate the work of another artist's copyrighted work into a new work. *Cariou v. Prince*, 13-261. The denial lets stand the United States Court of Appeals for the Second Circuit's prior decision, which gave artists significant leeway to claim a fair use defense when their work copies the work of another artist. *Cariou v. Prince*, 714 F.3d 694 (2d. Cir. 2013).

In 2011, Judge Deborah A. Batts of the United States District Court for the Southern District of New York granted summary judgment in favor of the plaintiff. *Cariou v. Prince*, 784 F.Supp.2d 337 (S.D.N.Y. 2011). Patrick Cariou is a photographer who took portraits of Rastafarians in Jamaica. He published a book containing his photographs called *Yes, Rasta*. Richard Prince is a known "appropriation artist." Appropriation art, according to the the New York City-based Museum of Modern Art's website, is a genre of art typified by an artist's "intentional borrowing, copying, and alteration of preexisting images and objects." Prince took 35 photographs from Cariou's book and made them into a collage series called "Canal Zone." He affixed the photographs to wooden boards and enlarged, cropped, painted over them, and otherwise modified the images in varying ways. Some were not modified and simply attached to the collage.

Judge Batts concluded that Prince's collage violated Cariou's copyright in his photographs and failed the fair use test codified in 17 U.S.C. § 107. Relying on the statutory factors and the U.S. Supreme Court's decision in *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994), Batts held that Prince's art did not do enough to transform Cariou's images into a new work. In *Campbell*, the Supreme Court affirmed a finding of fair use in a song by the band 2 Live Crew that parodied Roy Orbison's original song, "Oh, Pretty Woman." The Supreme Court found that 2 Live Crew's parody, which used the music and lyrics of Orbison's song, transformed the original into a new work. Judge Batts concluded that Prince's art merely used Cariou's photographs, and to qualify for the fair use defense the new work must "comment on Cariou, on Cariou's Photos, or on aspects of popular culture closely associated with Cariou or the Photos."

> "Even extensive digitization can be within fair use where the social benefits are strong and the harm to rightsholders is constrained. There will be more to come as we transition into a new era of copyright, technology, and even reading."
>
> **— Kenneth Crews**
> **Director,**
> **Columbia University Libraries**

On April 13, 2013, a divided panel of the Second Circuit Court of Appeals reversed the district court's decision. Writing for the court, Judge Barrington D. Parker held that "the law does not require that a secondary use comment on the original artist or work, or popular culture," as the district court incorrectly concluded. Parker said that some types of fair use, like parody or satire, "invariably comment on an original work and/or on popular culture," citing 2 Live Crew's parody of "Oh, Pretty Woman" as an example. However, "the law imposes no requirement that a work comment on the original or its author in order to be considered transformative," Parker wrote. Instead, "to qualify as a fair use, a new work generally must alter the original with 'new expression, meaning, or message.'"

For 25 of the works in question, Judge Parker compared Cariou's "serene and deliberately composed portraits and landscape photographs [that] depict the natural beauty of Rastafarians and their surrounding environs" to Prince's "crude and jarring works [that] . . . are hectic and provocative." The court also noted the significant difference in the media the artists used: Cariou's book contrasted with Prince's collages. The court limited its holding, noting that its "conclusion should not be taken to suggest . . . that any cosmetic changes to the photographs would necessarily constitute fair use. A secondary work may modify the original without being transformative." The court said that "a derivative work that merely presents the same material but in a new form, such as a book of synopses of televisions shows" would not constitute a transformative fair use. The court sent back five of Prince's works to the district court for findings on whether Prince's alterations were sufficient to constitute fair use.

Judge John Clifford Wallace of the United States Court of Appeals for the Ninth Circuit, sitting by designation, dissented in part from the majority. He concluded that the court should have remanded all of Prince's works to the district court for further factual findings about whether the art was transformative. He noted that judges are not art experts, and factual findings in the district court would be a more principled way to make decisions about whether a use is transformative.

The Supreme Court's refusal to review — which, in keeping with tradition, did not include an explanation of the decision — has drawn both applause and criticism from copyright experts and members of the art community.

Echoing Cariou's arguments to the court, Gary Rosen, a copyright attorney who writes the blog "Express Written Dissent," contended that the Second Circuit's standard is too uncertain for artists and attorneys. He wrote in a Nov. 17, 2013 post that in "assessing the 'purpose and character' of Prince's use the court had taken an exceptionally broad and subjective approach to the question of whether the accused works were 'transformative uses.'" He also suggested there might be "a judicial double standard favoring artists that judges and their acquaintances either 'get,' or think they ought to 'get,'" and art that judges may not understand or appreciate.

Attorney Virginia Rutledge filed an *amicus* brief on behalf of the Warhol Foundation for the case. Of the Second Circuit's decision, she said in an *Art in America* magazine article on Oct. 24, 2013, "This decision absolutely clarifies that the law does not require that a new work of art comment on any of its source material to qualify as fair use." Rutledge said that the decision adequately protects artists' free expression interests under the First Amendment.

– Cassie Batchelder
Silha Research Assistant

China Intensifies Crackdown on Microblogging

On Sept. 9, 2013, the Chinese Supreme People's Court and Supreme People's Procuratorate announced a new interpretation of the country's law against spreading rumors via social media. The law penalizes users of microblogs, such as Sina Corporation's popular service Weibo, with up to three years in jail for posting "serious rumors" that are viewed by more than 5,000 Internet users or that are reposted more than 500 times. The two state judicial bodies defined "serious rumors" as information that "causes mental anguish to the subjects of rumors," or that "causes protests, ethnic or religious unrest, or has a 'bad international effect,'" according to a Sept. 9, 2013 report by Reuters. State officials called the new interpretation a move toward "the purification of the online environment," according to a Sept. 19, 2013 report by the *Wall Street Journal*.

INTERNATIONAL NEWS

Analysts say the law is designed specifically to weaken the influence of so-called "Big V's" — members of Weibo whose accounts are "verified," meaning they have attained hundreds of thousands, or even millions, of followers. According to a Sept. 2, 2013 report by *Tea Leaf Nation*, an online magazine covering China, Big V's "have become a de facto trusted source of information for the younger, more tech-savvy generations that have grown increasingly tired of the same old rhetoric on state media." Meanwhile, according to *Tea Leaf Nation*, the government has argued on state media that the Big V's are "egotistical celebrities" acting in their own self interest because they "are paid by public relations firms to retweet certain posts."

Under the new law, authorities have arrested several famous Big V's and forced them to confess to their crimes on Chinese Central Television (CCTV). For example, Chinese-American businessman Charles Xue, who has more than 12 million followers on Weibo, was arrested in late August 2013 on charges of soliciting a prostitute. On Sept. 15, 2013, Xue was put before the country on CCTV, where he admitted to being a "womanizer" and said that his 12 million followers "had fueled his ego and made him feel 'like an emperor,'" according to Freedom House's Sept. 19, 2013 issue of its *China Media Bulletin*. *Tea Leaf Nation* reported on Sept. 2, 2013 that the editor of the state-run newspaper *Global Times* posted on his Weibo account that he could not "rule out the possibility" that Xue's public confession was a warning to other Big V's. *Tea Leaf Nation* reported that the editor later deleted the post. On July 12, 2013, Xue posted on Weibo that Chinese people "have all become 'people who tolerate,'" in response to issues such as high prices, low wages, and toxic food, according to a Sept. 19, 2013 story in the *Wall Street Journal*.

The crackdown appears to have chilled the speech of some prominent microbloggers. The *Wall Street Journal* reported on Sept. 19, 2013 that Pan Shiyi, a real estate mogul with more than 16 million followers on Weibo who is famous for his posts criticizing China's air pollution, said in an interview on CCTV that Big V's "should have even higher requirements of themselves" and show "more discipline" in their posts. Zhao Jing, a member of the Beijing-based group Internet Freedom in China, told *Bloomberg News* for a Sept. 10, 2013 report that under to the new law, "this Internet crackdown campaign will no longer be a tiger without teeth."

> "This Internet crackdown campaign will no longer be a tiger without teeth."
>
> **— Zhao Jing**
> **Founding Member,**
> **Internet Freedom in China**

Chinese authorities have also enforced the new law against less prominent Weibo users. In one instance, a teenager named Yang Hui was arrested on Sept. 17, 2013 in the rural northwest province of Gansu for posting comments critical of local police over how they handled the death of a bar manager, according to a Sept. 22, 2013 article by the *South China Morning Post*. Police reported the bar manager died after he jumped from a building, but Yang posted that he heard the man was beaten to death. He accused the police of not investigating the death properly, and he called for locals to protest, according to the *South China Morning Post*. Yang's lawyer, You Feizhou, told the newspaper that the boy's posts had not been read more than 5,000 times or shared more than 500 times, as the new law required. National Public Radio reported that Yang was released on Sept. 23, 2013.

The crackdown on Weibo users coincided with the arrests of two high-profile journalists on defamation charges. On Sept. 30, 2013, Liu Hu, a journalist for the Guangzhou-based newspaper *New Express*, was officially charged with defamation after being arrested on Aug. 24, 2013, according to an Oct. 11, 2013 report by Reporters Without Borders (RSF). RSF reported that Liu posted on his Weibo account on July 29, 2013 accusations of corruption against a state official who failed to investigate the privatization of two state-owned companies "that resulted in considerable losses for the state." On Oct. 10, 2013, the *South China Morning Post* noted the "stark contrast" between Liu's arrest and the outcome of a December 2012 report by internationally-respected journalist Luo Changping. Luo had accused the deputy head of the National Development and Reform Commission of corruption, which led to the official's expulsion from the Party in August 2013. Luo was not arrested for the story.

Another *New Express* journalist, Chen Yongzhou, was arrested in mid-October 2013 and charged with "damaging commercial reputation" for reports he wrote in May 2013 alleging that the partly state-owned construction equipment company Zoomlion had exaggerated its earnings. After Chen's arrest, *New Express* published the headline "Please Release Him" on Oct. 22, 2013, and on the following day it published the headline "Again: Please Release Him," a move that BBC correspondents called "rare and bold" in an Oct. 24, 2013 report. On Oct. 27, 2013, Chen confessed on CCTV to "writing false stories for money," according to a report by the BBC. "I've caused damages to Zoomlion and also the whole news media industry and its ability to earn the public's trust," Chen said. Following Chen's public confession, *New Express* issued an apology for "failing to verify his stories," according to an Oct. 28, 2013 report by the *Sydney Morning Herald*. However, Jeremy Goldkorn, director of the website Danwei.com, which is devoted to researching Chinese media, told the *Morning Herald* that the *New Express*'s apology was written in a "tiny corner" of its front page, and thus "it d[id]n't look like a very sincere apology."

The new "rumormongering" law and the crackdown on journalists may be a strategy by President Xi Jinping to consolidate power ahead of the Communist Party's Third Plenum from Nov. 9-12, 2013, according to an interview with Reuters Beijing correspondent Benjamin Lim on CNN's Oct. 16, 2013 "On China" program. A Third Plenum is the third time new a new set of leaders holds a plenary session of the Communist Party's Central Committee, a meeting at which party leaders discuss policy issues. Historically, these sessions are seen as a test of the president's leadership because

they have been the meetings at which party leaders have tended to enact major reforms, according to a Nov. 1, 2013 report from *International Business Times*.

On Nov. 15, 2013, the Chinese state news agency Xinhua released a transcript of a speech given by Xi during the Third Plenum in which he addressed the matter of managing Internet communications. "[T]he question of how to strengthen online legal building and public opinion channeling to ensure order in online communications and national security has already become a conspicuous problem standing before us," Xi said, according to the transcript. Regarding exactly how the Party would address that problem, Xi said, "[We must] perfect systems and mechanisms for adhering to correct guidance of public opinion. We must fully build interactive mechanisms for the work of basic management, content management, industry management and the crackdown on and prevention of criminal conduct online. [We must] perfect mechanisms for handling online sudden-breaking incidents, creating an online public opinion work pattern that integrates positive public opinion channeling and management according to rule of law."

The crackdown on social media and journalists is also seen as a way for the party to set the norms of exposing corruption. One of Xi's principal policy goals since he took office in November 2012 has been stamping out corruption within the party. His so-called "Tigers and Flies" campaign is designed to root out corrupt prominent party officials (Tigers) and small-time provincial officials (Flies). Renowned Sinologist Willy Lam told CNN's "On China" program on Oct. 16, 2013 that party officials are worried that allowing Weibo users to denounce corrupt officials — even the "Flies" — will lead those users to criticize the entire party.

The "rumormongering" law represents a new strategy in China's notorious campaign of Internet censorship. Prior to the new law, the typical practice for censors was to monitor keywords used on Weibo. For example, following the social-media driven uprisings in Egypt and Libya in February 2011, rumors began swirling on Chinese microblogs about the potential for a similar "Jasmine Revolution" in China. Censors subsequently deleted any microblog posts with the word "Jasmine" in them. The new law shifts the focus of the government's censorship efforts to the messengers themselves. (For more coverage on the early 2011 crackdown, see "International Journalists Face Censorship in Confronting Governments" in the Winter/Spring 2012 issue of the Silha *Bulletin*.)

The new law also represents a calculated move on the part of the government to control speech on social media while also not angering social media users. In late March 2012, authorities disabled the commenting feature on Weibo for three days following rumors of a coup. That move led many Weibo users to vent their anger against authorities, according to an April 3, 2012 report by the *Wall Street Journal*. By targeting the major users of Weibo and not completely forbidding access to the site, the government is keeping citizens from growing restive while also recognizing the value of Weibo for its e-commerce function, according to a Sept. 19, 2013 report by the *Wall Street Journal*.

In conjunction with the crackdown on the spread of rumors, the government also detained about 110 ethnic Uighurs in the far western province of Xinjiang in August 2013 for allegedly spreading "jihadist" rumors, according to an Oct. 29, 2013 report by Freedom House's *China Media Bulletin*. Uighurs, who are predominantly Muslim, are frequent targets of crackdowns by Chinese authorities, who view their religious activities and web postings as "incitement to separatism and religious militancy," according to Freedom House.

Analysts are uncertain of what the future holds for the role of Weibo in Chinese society. Reuters Beijing correspondent Benjamin Lim said on CNN's Oct. 16, 2013 "On China" program that Xi may soften the party's stance against Weibo users if he builds his reputation as a strong leader following the Third Plenum. However, the *Wall Street Journal* reported on Sept. 19, 2013 that Weibo users may migrate to mobile platforms, such as Tencent Holding's WeChat app, because so far the government has not monitored mobile platforms as strictly as broadband platforms.

Reuters reported on Dec. 12, 2013 that the current number of active WeChat users, estimated at around 272 million, has more than doubled since September 2012. According to the report, WeChat limits discussion groups to 40 people. Therefore, although WeChat users can still be monitored, the service "does give users a way to avoid running afoul of the government's new rules, that hold users accountable for 'online rumors' read by 5,000 people or reposted 500 times." Min Jiang, associate professor of communication at the University of North Carolina at Charlotte, told Reuters for the Dec. 12, 2013 story, "Weibo is like a public square, and [WeChat] is like your sitting room." However, Jiang said, "If anything happens and it becomes explosive, everybody knows that [WeChat] will be the next target."

ProPublica Publishes Censored Weibo Images

On Nov. 14, 2013, U.S. non-profit investigative news source ProPublica published 527 images that Weibo users attempted to publish between July 24 and Aug. 4, 2013, but were taken down by Weibo's in-house censors. ProPublica collected the images by writing code to monitor 100 Weibo accounts and recognize posted images that were later deleted, according to a Nov. 14, 2013 ProPublica story describing its methodology. The 100 Weibo users were selected because they were journalists or lawyers, but ProPublica said the users did not know that their accounts were being monitored. Of the 527 images, 156 were categorized as "political speech" because they "explicity criticized the Chinese government, questioned official accounts of historical events or called out social injustices."

The second-largest group of images, with 124, involved long passages of text produced by the platform known as "Long Weibo," which converts text to image files to "render[] inoperable the automatic filters that might monitor the use of forbidden words in a text post," according to ProPublica. These images include "politically charged essays, signed petitions calling for the release of activists, and transcripts of interviews [of] high-profile officials making controversial remarks about Chinese society." Other categories of images — all of which were political in nature — included images of posts that had been deleted by censors, images of error screens that appear following the censoring of a post (which are seen as an anti-censorship symbol), and images of protests.

ProPublica wrote in a separate Nov. 14, 2013 story about the project that its goal was to "allow[] readers to see and understand the images that censors considered too sensitive for Chinese eyes" and to show that "while the speech on Weibo is equal parts sophisticated and base, considerate and raucous, it is by no means free." The organization stressed that because the users and their posts were not chosen at random, people "should not generalize our findings to larger populations."

Brett Johnson
Silha *Bulletin* Editor

Minnesota Supreme Court Approves Use of Cameras in Civil Cases, Considers Expansion to Criminal Cases

On Dec. 3, 2013, the Minnesota Supreme Court issued an order amending Rule 4 of the Minnesota General Rules of Practice, permanently allowing video cameras in certain Minnesota courtroom proceedings. The order codified a pilot program launched by the Supreme Court in March 2011 authorizing Minnesota state court judges to allow video and audio recordings of certain types of civil proceedings, at their discretion. Before that 2011 order, those wishing to record audio or video in a courtroom needed the express approval of the judge and all parties to the case.

CAMERAS IN THE COURTROOM

The Minnesota Supreme Court codified the pilot program based on a report by the Advisory Committee on the General Rules of Practice, assigned to monitor the program in its March 2011 order. Based on the report from the advisory committee, the high court found that the pilot program had created no reported "problems, complaints, delays or known prejudice to the parties during the project." (For more on the evolution of the Minnesota pilot program, see "Minnesota Senate Expands Floor Access; State Supreme Court Approves Cameras" in the Winter/Spring 2011 issue of the Silha *Bulletin*, "Federal and State Courts Consider Proposals to Permit Cameras in Trial Proceedings" in the Fall 2010 issue, and "Minnesota High Court Approves Cameras-in-Court Pilot Program" in the Winter 2009 issue.)

The Supreme Court noted that the program had attracted fewer media requests than anticipated, but that the rules were effective when used. The high court found that most other states had already embraced cameras in courtrooms, concluding that "there is no reason to retreat from the controlled use of cameras and recordings in certain civil court proceedings, and there is every reason to, as we have previously stated, allow such coverage." However, it nonetheless maintained current restrictions on certain types of coverage. These exceptions include proceedings involving child custody, divorce, juvenile defendants, child protection, paternity, and civil commitment proceedings, as well as coverage of jurors and coverage of witnesses who object to the recording of their testimony.

> "There is no reason to retreat from the controlled use of cameras and recordings in certain civil court proceedings, and there is every reason to, as we have previously stated, allow such coverage."
>
> **— Minnesota Supreme Court**

A group of news media practitioners, represented by Minneapolis attorney Mark Anfinson, had petitioned the advisory committee to recommend making the pilot program permanent and expanding the program into some categories of criminal proceedings. At the committee's Sept. 20, 2013 meeting, Anfinson framed media coverage of criminal cases as a way of increasing public trust in courts, arguing to the committee that video from in courtrooms allows "society to be able to see how well the justice system works."

The Minnesota Supreme Court did not expand the program to criminal cases. It did, however, direct the Advisory Committee on the Rules of Criminal Procedure to evaluate how such a program could be implemented in criminal cases, "in particular those in which concerns regarding witnesses and jurors are minimized or largely absent, such as arraignments, pretrial hearing, and sentencing proceedings." The committee's report is due no later than Dec. 1, 2014.

Although the high court concluded based on the advisory committee's Oct. 1, 2013 report that "no one recommends discontinuing the audio and video coverage permitted under the pilot project," this was not the case at the Sept. 20, 2013 meeting of the advisory committee debating the program. A vocal minority at the meeting, including Hennepin County District Court Judge Mel Dickstein, opposed extending the pilot program. Dickstein argued that cameras had been used in too few cases for the committee to conclude that the program should continue. "There's not enough here for us to say 'it worked,'" Dickstein said at the Sept. 20, 2013 meeting.

According to information about cameras in the courtroom available on the Reporters Committee for Freedom of the Press's website, all 50 states have rules permitting some sort of extended media coverage in courtrooms, but "Minnesota courts have been among the most restrictive for visual and audio coverage." Anfinson said the news media petitioners were pleased with the order, saying, "This is progress, no doubt about that," according to a Dec. 3, 2013 report by *Pioneer Press* reporter Emily Gurnon.

Alex Vlisides
Silha Research Assistant

Ethical Issues in Fall 2013 Include Questionable "60 Minutes" Source, Restrictive White House Photography Practices

During the fall of 2013, major issues in media ethics included a "60 Minutes" correspondent failing to properly vet a key source in a story about the September 2012 terrorist attack in Benghazi, and news organizations criticizing the Obama administration for not allowing professional photojournalists to cover the president at public events. A former *Newsweek* reporter faces a libel suit after attempting to atone for a past ethical lapse of revealing the identity of a confidential source, and many in the news media debated whether they should use the term "Redskins" when writing about the Washington, D.C. National Football League team.

ETHICS

"60 Minutes" Errs in Benghazi Report, Fails to Address Questionable Reporting

On Nov. 8, 2013, "60 Minutes" correspondent Lara Logan apologized in an interview on the program "CBS This Morning" for the TV news magazine's use of a questionable source during its Oct. 27, 2013 report on the Sept. 11, 2012 attack on the U.S. consulate in Benghazi, Libya. "The most important thing to every person at '60 Minutes' is the truth, and today, the truth is that we made a mistake," Logan said.

In the Oct. 27, 2013 report, Logan interviewed a British man named "Morgan Jones," an employee with the British security company Blue Mountain, which the U.S. State Department had contracted to provide security for the consulate. Jones claimed to have rushed to the aid of Americans in the compound during the September 2012 attack, knocked out militants with the butt of a rifle, and later sneaked into a Benghazi hospital to see the body of U.S. Ambassador to Libya J. Christopher Stevens, who was killed in the attack. Jones' book *The Embassy House*, in which Jones recounted a similar story of his involvement at the consulate during the attack, was released in the week following the "60 Minutes" interview.

On Oct. 31, 2013, Karen DeYoung reported in the *Washington Post* that Jones' real name was Dylan Davies, and that on Sept. 14, 2012, he had filed an incident report with his employer that conflicted with the story he recounted to "60 Minutes." According to DeYoung's report, Davies wrote that he "spent most of that night at his Benghazi beach-side villa," and that he was not able to "get anywhere near [the consulate] as roadblocks had been set up." Davies also stated in the incident report that he saw Stevens' body in a photo that a colleague had taken with his phone.

The co-author of *The Embassy House*, Damien Lewis, told DeYoung that Davies may have deliberately filed a false incident report so as not to upset his superiors at Blue Mountain, who had told him to stay away from the compound. On Nov. 2, 2013, Eli Lake and Josh Rogin of *The Daily Beast* posted a copy of the incident report on their website, and reported that they interviewed Davies, who denied writing the incident report. "I am just a little man against some big people here," Davies told Lake and Rogin. "They can do things, make up things, anything they want. I wouldn't stand a chance." Davies told *The Huffington Post*'s Michael Calderone for a Nov. 4, 2013 article that he lied to his superiors about his whereabouts on the night of the attack, but that the account he gave to "60 Minutes" was true. In the article, Calderone called "60 Minutes" into question over whether the show's staff properly vetted Davies and his story prior to the interview.

On Oct. 31, 2013, "60 Minutes" spokesman Kevin Tedesco told DeYoung, "We stand firmly by the story we broadcast last Sunday [Oct. 27, 2013]." Logan also told *New York Times* reporter Bill Carter on Nov. 5, 2013 that she stood by her reporting. However, she admitted to Carter that she should have disclosed that *The Embassy House* was being published by Simon and Schuster, a subsidiary of CBS. Logan also told Carter that she blamed the "political atmosphere surrounding the [Benghazi] incident" for the critical response to the interview. On Nov. 6, 2013, chairman of CBS News Jeffrey Fager told *The Huffington Post*'s Calderone in an email, "We are proud of the reporting that went into the story and have confidence that our sources, including those who appeared on '60 Minutes,' told accurate versions of what happened that night."

On Nov. 7, 2013, Bill Carter and Michael Schmidt reported for *The New York Times* that Davies had told the FBI that he did not arrive on the scene of the attack until the following morning. Following Carter and Schmidt's story, CBS News stated on its website, "We are currently looking into this serious matter to determine if he [Davies] misled us, and if so, we will make a correction." On Nov. 8, 2013, CBS News removed the "60 Minutes" interview with Davies from its website. Fager told *The New York Times* on Nov. 8, 2013, "There are people in the world who try to deceive others. We believe we have a really good system to guard against that. This guy got through that." *The New York Times* reported on Nov. 10, 2013 that Fager said CBS News would not conduct an internal investigation into the production of the "60 Minutes" interview. After CBS News admitted its error, Simon and Schuster ceased publication of Davies' book, according to a Nov. 8, 2013 report by the BBC.

However, according to a Nov. 26, 2013 report by NPR News, CBS News' executive director of standards and practices, Al Ortiz, did conduct an internal investigation that led CBS News to ask Logan and her producer to take a leave of absence from "60 Minutes." NPR News reported that it had obtained a summary of Ortiz's investigation, which concluded that Logan had missed "red flag[s]" about Davies' credibility, and that "60 Minutes" staff not only had failed to corroborate Davies' story with other sources, but they had missed previous reports in *The New York Times* and the *Washington Post* that contradicted Davies' story. The exact length of Logan's leave had not been disclosed as the *Bulletin* went to press.

Prior to Logan's forced leave of absence, many in the news media criticized CBS News' handling of the mistake. The Poynter Institute's Craig Silverman, who runs the correction and fact-checking blog "Regret the Error," told *The New York Times* for its Nov. 10, 2013 report that Logan's apology "struck a very passive tone and pushed the responsibility onto the source," and "said nothing about how the show failed to properly vet the story of an admitted liar." David Brock, founder of the liberal media watchdog organization Media Matters, called CBS News' response "wholly inadequate and entirely self-serving" in a Nov. 10, 2013 post on the Media Matters blog. Brock called for CBS News to "come clean by appointing an independent commission to determine exactly how and why it fell prey so easily to an obvious hoax." Michael Calderone of *The Huffington Post* criticized CBS News in a Nov. 11, 2013 article for not addressing such questions as whether anyone would be fired for the erroneous report and how CBS News would hold itself accountable in future reporting.

Alicia Shepard, former ombudsperson for NPR, called the "60 Minutes" interview

Ethics, *continued on page 28*

Ethics, *continued from page 27*
a "12-minute infomercial for *The Embassy House*" in a Nov. 11, 2013 column for *Columbia Journalism Review*. Shepard also criticized CBS News' choice of assigning the story to Logan, who, Shepard noted, "gave an oddly impassioned . . . speech to about 1,100 influential people at a Better Government Association annual luncheon in Chicago" in October 2012, at which she "called for retribution" for the Benghazi attacks in order to "let the world know that the United States will not be attacked on its own soil."

In their Nov. 10, 2013 article, *New York Times* reporters Bill Carter and Brian Stelter speculated that the mistake would lead to increased internal oversight at "60 Minutes." They reported that in 2011, after Fager became chairman of the news division, CBS News cut executive staff in charge of standards "who screened every '60' report before broadcast."

Former CBS News anchor Dan Rather, who resigned after he was accused of using questionable documents to report in September 2004 that President George W. Bush had received preferential treatment during his time in the Texas Air National Guard, told CNN's Piers Morgan on Dec. 9, 2013 that Logan should not lose her job over this story. "Whatever one thinks of what Lara Logan did or didn't do with this story, in fairness, it should be put against her whole record," Rather said. (For more information on Dan Rather's resignation from CBS News, see "Dan Rather, Other Staff Members Depart '60 Minutes' in Wake of Ethics Controversy" in the Winter 2005 issue of the Silha *Bulletin*.)

News Organizations Criticize White House for Overreliance on In-House Photography

On Nov. 21, 2013, the White House Correspondents' Association sent an open letter to White House press secretary Jay Carney "to protest the limits on access currently barring photographers who cover the White House." Several dozen prominent news organizations, including the Associated Press, the National Press Club, *The New York Times* Company, and Reuters, signed the letter. The organizations alleged that "[j]ournalists are routinely being denied the right to photograph or videotape the President while he is performing his official duties. As surely as if they were placing a hand over a journalist's camera lens, officials in this administration are blocking the public from having an independent view of important functions of the Executive Branch of government."

The letter listed several public events from July to October 2013 at which the White House allowed exclusive access to Pete Souza, the president's official photographer, including meetings with foreign dignitaries, meetings with members of Congress and cabinet members, and a meeting with Pakistani human rights activist Malala Yousafzai. The letter's signatories argued that the fact that Souza was allowed to photograph the events and distribute the photos free of charge to news organizations on the White House Flickr account proves that the events were newsworthy and thereby undermines the administration's assertion that these events were "private" and not open to the press. "[I]mposing limits on press access, as your office has done, represents a troubling precedent with a direct and adverse impact on the public's ability to independently monitor and see what its government is doing," the letter said.

> "As surely as if they were placing a hand over a journalist's camera lens, officials in this administration are blocking the public from having an independent view of important functions of the Executive Branch of government."
>
> **— White House Correspondents' Association**

Members of the news media also have taken to their columns to criticize the practice. *Washington Post* columnist Dana Milbank wrote on Nov. 26, 2013 that the practice "raised questions about the integrity of images Americans see of their president." White House deputy press secretary Josh Earnest defended the practice when interviewed by Milbank for the column, telling him, "There are certain circumstances where it is simply not feasible to have independent journalists in the room when the president is making decisions." Milbank criticized Earnest's rationale, arguing that many of the events at which Souza was the sole photographer involved no decision-making whatsoever by the president.

Santiago Lyon, director of photography for the AP, called Souza's photographs "visual press releases" in a Nov. 21, 2013 post on the AP's blog. "Media organizations generally do not reproduce written press releases verbatim, so why should we settle for these official images?" he wrote. *New York Times* public editor Margaret Sullivan wrote on her blog for the *Times* on Dec. 6, 2013, "controlling the image is just another way of controlling the news. To put it bluntly, White House 'handout' photographs are closer to propaganda than to journalism." *New York Times* photographer Dana Mills told Jay Carney that the administration was acting "like Tass," the former state news agency of the Soviet Union, according to a Nov. 21, 2013 report by *National Journal* columnist Ron Fournier. Fournier called the administration "propagandists — in the purest sense of the word." He also argued that the administration's practice of freely distributing the photos via social media was "ironic," since it was "using technology that democratized and flattened the media to centralize and strengthen the powers [of] an institution, The Presidency."

On Nov. 25, 2013, *USA Today* deputy director of multimedia Andrew P. Scott sent a memo to the newspaper's staff stating that the organization would no longer use "handout photos originating from the White House Press Office, except in very extraordinary circumstances." The memo stated that such circumstances would include events that were "of very high news value," and instances where access to outside photographers was restricted for national security reasons, such as the May 2011 photograph of the president and members of his cabinet watching footage of the Navy SEAL raid in which Osama bin Laden was killed. Gannett, *USA Today*'s parent company, was one of the news organizations that signed the Nov. 21, 2013 open letter to press secretary Carney.

Following the release of the *USA Today* memo, the Poynter Institute published a Nov. 25, 2013 story containing the ethical codes of other prominent news organizations regarding the use of White House stock photos. The AP, the *Los Angeles Times* and *The New York Times* told Poynter that their policies were similar to those articulated in the *USA Today* memo. *New York Times* spokeswoman Eileen Murphy told Poynter that the *Times* would also use a photo from the White House "when a photo itself is a referenced part of a story." She gave the example of a Dec. 29, 2012 Souza photo depicting the president's nearly all-male advisory team with one of the men obscuring the only female member, Valerie Jarrett. The *Times* used that photo in a Jan. 9, 2013 story on the predominantly male nature of Obama's inner circle of advisers.

In its Nov. 21, 2013 open letter, the White House Correspondents' Association requested a formal meeting with Jay Carney to discuss their grievances. No meeting had been scheduled as the *Bulletin* went to press.

Former Columbia University Journalism Professor Faces Lawsuit for Revealing Source

Former Columbia University journalism professor and *Newsweek* reporter Bruce

Porter is being sued for libel and invasion of privacy following his attempt to atone for revealing the name of a confidential source for a story he wrote for *Newsweek* in October 1967. Maxim Waldbaum of the Manhattan law firm Eaton and Van Winkle filed the complaint against Porter in the United States District Court for the Southern District of New York on Oct. 31, 2013 on behalf of Margaret Won. The complaint also names the *Columbia Journalism Review* (*CJR*) and documentary filmmaker Daniel Loewenthal as defendants. *Won v. Columbia Journalism Review et al.*, 1:2013cv07723 (Oct. 31, 2013 S.D.N.Y.).

According to the complaint, Porter granted Won anonymity when he wrote the story "Gentle Marcy: A Shattering Tale" in 1967, yet he used her first name (Won goes by Marcy) and described her as being from Flint, Mich., making her "easily identifiable to her family and acquaintances." In the story, Porter reported that Won engaged in heavy drug use and casual sex, and paid $200 for an illegal abortion while living in New York City. Following the story, reporters with the Washington, D.C.-based radio station WNEW surreptitiously recorded Won making a phone call to her mother, asking her to "please still love [her]" after she read the story, and the conversation was rebroadcast repeatedly. The complaint states that Porter has admitted to publicly discussing Won's story "as an example of his own experience exercising poor ethics in journalism" in the classes he taught at both Brooklyn College and Columbia University. Part of the classes involved Porter playing the WNEW recording of Won for his students.

On Nov. 1, 2012, Porter published an article titled "Lost and found" in *CJR* in which he recounted his interactions with Won, including witnessing her take drugs. In the article, Porter admitted violating the conditions of confidentiality that he gave to Won and wanting to make amends by finding Won and apologizing. Porter sought the help of filmmaker Loewenthal to document his journey. They began by finding the names of Won's deceased parents in the *Flint Journal*, which they reported in the *CJR* article. Porter and Loewenthal found Won at her childhood home, where Loewenthal took her photo. On Dec. 4, 2012, Porter told Dick Gordon's radio program "The Story," "I don't think Marcy is really okay with this [apology attempt]. I think she feels that her life was invaded, and I feel that she felt she was taken advantage of."

The complaint alleges that several of the facts reported in the *CJR* article were false, including the reports that Won used the drug "stp," that she had a drug dealer, that she ran away from home, and that she was 17 at the time of the original article (she was 19). The complaint claims that because Porter knew the statements about Won were false when he originally reported them, his re-reporting of the statements amounted to reckless disregard for the truth or falsity of the statements — the standard that Won would need to prove to win a defamation case if she were a public figure, which, the complaint claims, she is not. The complaint also claims that because Porter and his co-defendants used Won's "name and picture for the purposes of trade without first obtaining her written consent," they "are guilty of invasion of [Won]'s privacy under New York Civil Rights Law § 51," which recognizes the privacy tort of misappropriation.

> "The word 'Redskin' is racist, and very much so. It is not a term of honor, but a term of hate."
>
> **— Editorial Board, Neshaminy *Playwickian* Langhorne, PA**

Waldbaum told the blog "Law360" on Nov. 1, 2013 that his client was "a woman who was really harmed in 1967. I don't know why *CJR* didn't fact check, but you don't clean something up by raising the harm again." Neither of the defendants had commented on the lawsuit as the *Bulletin* went to press.

News Media Debate Use of Nickname "Redskins" in Reporting on Washington, D.C. NFL Team

For years, politicians and academics have contended that the nickname of the Washington, D.C. National Football League (NFL) team, the Redskins, is racist toward Native Americans and should be changed. Meanwhile, team owner Daniel Snyder has said on many occasions that he is not open to changing the name. The debate heated up during the 2013 NFL season, with President Obama calling for the team to change its name. Now, some members of the news media have staked their position in the debate, opting not to use the name Redskins in their reporting.

In a June 10, 2013 column, sports reporter Tim Graham of *The Buffalo News* became the first journalist to publicly state that he would stop using the name in his reporting. "There are folks who'll see this and instinctively moan about political correctness and bleeding-heart liberalism or the loss of old-school traditions," Graham wrote. However, he reported, "Merriam-Webster's definition states the R-word is 'usually offensive,' and the Merriam-Webster dictionary for people learning the English language states: 'The word redskin is very offensive and should be avoided.'"

John Smallwood, sports reporter for the *Philadelphia Daily News*, stated in a June 16, 2013 column that he also would stop using the name in his reporting. Smallwood said he would "refer to the team as Washington, Washington's football team, the 'Skins, the R's or some other reference." Smallwood joked that his decision "could potentially make life on deadline a bit more troublesome for the copy editors if higher-ups don't agree with my stance and decide it is not my place to make personal policy a part of the newspaper." However, Smallwood argued that "[i]n practical use, the R-Word is no different from calling an African-American the N-Word, a Jewish person the K-Word, a Hispanic the W-Word, an Irish-American the M-Word, or an Italian American a different W-word."

Slate and *The New Republic* announced on Aug. 8, 2013 that their reporters would stop using the name, according to the Pew Research Center. *Sports Illustrated* reporter Peter King became one of the first prominent national reporters to announce he would no longer use the name. *USA Today* sports reporter Christine Brennan became the first national newspaper reporter to say, in a Sept. 12, 2013 column, that she would not use the name. In a Sept. 12, 2013 editorial, the *Washington Post* editorial board condemned the use of the name, but it did not say that it would encourage *Post* reporters not to use the word. Well-known NBC sports reporter Bob Costas called the Redskins name "an insult" in his traditional "Sunday Night Football" monologue during halftime of the Oct. 13, 2013 game between the Redskins and the Dallas Cowboys.

The Pew Research Center reported that as of Oct. 30, 2013, 24 news outlets or journalists have said they will "no longer use the term Redskins," and 12 news organizations "have policies restricting or banning the use of the name." However, not all journalists are speaking out against the name. ESPN columnist Rick Reilly argued in a Sept. 18, 2013 column that the name did not necessarily dishonor Native Americans, and that changing the name Redskins would set a precedent for changing names of sports teams simply because people found them offensive.

Reilly's column touched off a separate ethical issue after the alternative sports news website Deadspin reported on Oct.

Ethics, *continued on page 30*

Silha Lecture Links Pentagon Papers and the Obama Administration's Treatment of Leakers

Leading First Amendment lawyer James C. Goodale said that President Obama should take a lesson from the Pentagon Papers case and rethink his approach to conflicts between national security and the First Amendment. Goodale, who served as vice chairman of *The New York Times* and was the *Times*' general counsel during the Pentagon Papers litigation in 1971, made these remarks during the 28th Annual Silha Lecture on Oct. 16, 2013 at the University of Minnesota's Cowles Auditorium.

SILHA CENTER EVENTS

"All of a sudden in the last six months, all of the issues in that case have come to life and have been part of the news cycle," Goodale, who has been a partner in Debevoise & Plimpton LLP in New York City, served as chairman of the Committee to Protect Journalists, and has taught at Yale, NYU and Fordham law schools, said.

Goodale shared stories of the litigation surrounding the Pentagon Papers case and his thoughts on recent conflicts between national security and the First Amendment during the lecture, titled "The Lessons of the Pentagon Papers: Has Obama Learned Them?" The lecture, which was followed by a question-and-answer session, drew an audience of more than 300 people. Following the lecture, Goodale signed copies of his new book *Fighting for the Press: The Inside Story of the Pentagon Papers and Other Battles*.

The Pentagon Papers case, *New York Times Co. v. United States*, 403 U.S. 713 (1971), teaches two important lessons, according to Goodale. First, government officials "ignore the First Amendment at their peril." Second, individuals "should not buy claims of national security made by the government hook, line, and sinker."

Goodale began the lecture by providing an overview of the Pentagon Papers case and the circumstances surrounding it. He explained that the Pentagon Papers were a 47-volume history of American relations with Vietnam. Daniel Ellsberg, a military analyst, believed the American people needed to see them, and so he shared them with various newspapers around the country. The government tried to stop two of those papers, the *Washington Post* and *The New York Times*, from publishing them, which led to the case that reached the Supreme Court.

"It's a case for the ages," Goodale explained, because it determined that in cases of prior restraint, "unless the government can show directly, immediately, and irreparably that harm will happen to national security, then the government loses." He explained that the government failed to meet this heavy burden in the Pentagon Papers case. The Supreme Court allowed the publication of the Pentagon Papers to go forward, providing American citizens with more information about relations with Vietnam than they had ever seen before.

Goodale shared anecdotes highlighting why government claims of national security are not to be trusted. For example, he said the biggest lie the government told in the Pentagon Papers case was that the papers would show that the United States had broken the North Vietnamese code, which would be damaging to national security. To prove this, the government presented various judges with a classified document that it claimed would demonstrate the harm the leak would cause. When *Washington Post* reporter George Wilson saw the government present the United States Supreme Court with the document, he recognized it immediately: it had already appeared in the *Congressional Record*.

Incidents like this, Goodale said, have caused him to mistrust the "intelligence establishment," including the National

Ethics, *continued from page 29*

10, 2013 that Reilly misquoted his father-in-law, Bob Burns, who is Native American, to make his argument about the Redskins name not dishonoring Native Americans. Reilly quoted Burns as saying, "the whole issue is so silly. The name just doesn't bother me much. It's an issue that shouldn't be an issue, not with all the problems we've got in this country." However, according to the Deadspin story, Burns told the Indian Country Today Media Network on Oct. 10, 2013 that he actually had told Reilly, "it's silly in this day and age that this should even be a battle — if the name offends someone, change it." Burns also said that he told Reilly that he did think that the name Redskins demeans Native Americans, that it upset him that Reilly's column portrayed him "as an 'Uncle Tom' in support of this racial slur," and that he asked Reilly to correct the column, which Reilly never did. Reilly posted an extended message to his Twitter account on Oct. 12, 2013 in which he said that he stood by his reporting and that he thought he had "accurately quoted [his] father-in-law in the piece." He wrote that the Redskins name "is an incredibly sensitive issue, and Bob felt he had more to say on the subject after that column was posted on ESPN.com." Michael David Smith of NBC Sports wrote in an Oct. 12, 2013 column that the difference in the two quotes was "enormous," and that it was "hard to see how Reilly c[ould] 'stand by the reporting.'"

The boycott against the term Redskins has spread beyond coverage of the NFL. ABC News reported on Nov. 17, 2013 that student editors of the Neshaminy *Playwickian*, the newspaper of Neshaminy High School in Langhorne, Pa., announced that they would stop using Redskins, the nickname of the school's sports teams. "The word 'Redskin' is racist, and very much so," the students wrote in an editorial. "It is not a term of honor, but a term of hate." Fourteen of the 21 members of the paper's staff supported the boycott, according to ABC News. The students' decision has led to angry reactions on social media from parents and school board members, according to a Dec. 7, 2013 story by the *Philadelphia Inquirer*. The *Inquirer* also reported that some Neshaminy students have publicly ripped the paper to shreds in protest of the editorial board's decision.

The school's principal, Robert McGee, called the students' decision "valiant," but ordered them to reverse it. McGee told the AP on Nov. 16, 2013 that because each of the nearly 2,600 students at the school is required to write an article for the paper for course credit, he did not believe those students should be prevented from using the name. "I see it as a First Amendment issue running into another First Amendment issue," McGee said. Frank LoMonte, executive director of the Student Press Law Center, told the AP on Nov. 16, 2013 that the students' decision was "exactly what we tell young people in the abstract we want them to do: use their voices in positive ways to bring about social change. And yet when they tried to do it in practice, the school slapped them down. That's a bad place for an educator to be."

Brett Johnson
Silha *Bulletin* Editor

Security Agency. The intelligence establishment is "a unitary group which does not subject itself to criticism," Goodale said. "They get their own way through misdeeds and lying."

Goodale emphasized that the Pentagon Papers' lessons remain relevant today, particularly with the NSA in the media spotlight. He cited this year's revelations about the NSA surveillance programs and the Obama administration's prosecution of leakers. (For more information about this trend, see "Open Government Advocates Criticize Obama's Prosecution of Leakers" in the Winter/Spring 2011 issue of the Silha *Bulletin*, and "Manning, Kiriakou Face Punishment for Blowing the Whistle on the War on Terror" in the Winter/Spring 2013 issue.)

Goodale noted that the Obama administration has indicted seven individuals for leaking classified information. All previous administrations put together had indicted only three. These indictments have "created an atmosphere of fear in Washington, which has made it very hard for the press to gather news and write stories," he explained, citing an October 2013 report from the Committee to Protect Journalists that reached the same conclusion.

Goodale also offered opinions about many of the recent cases of reporters and leakers facing legal trouble. He said that President Obama has said "some strange things about the Espionage Act," which the administration has used to prosecute leakers. Leakers are not spies, Goodale said. Rather, "they are giving information as whistleblowers to the press to publish it" because they believe the public has the right to know about an issue.

In particular, Goodale discussed the case of James Risen, a *New York Times* reporter who the United States Court of Appeals for the Fourth Circuit has ordered to testify in a case against a source who allegedly leaked information about Iran's nuclear program. (For more information on the Fourth Circuit's decision, see "Reporters Struggle to Claim Privilege to Avoid Testifying About Confidential Sources" on page 10 of this issue of the Silha *Bulletin*.)

"Risen has said he will go to jail when push comes to shove," Goodale said, pointing out that Risen won a Pulitzer Prize in 2007 for National Reporting on a series of stories about the NSA. Goodale noted that if the Obama administration continues to try to force Risen to testify against his source should the United States Supreme Court hear Risen's case, Obama would be "in the driver's seat," and would be responsible for putting Risen in jail.

Goodale explained that he wrote his new book on the Pentagon Papers to issue a call for debate on the issues related to Wikileaks and the possible indictment of Julian Assange. "Obama is going to cause a lot of trouble if he prosecutes Julian Assange," Goodale argued. Former Assange lawyer Mark Stephens discussed the issues surrounding Assange at the 2011 Silha Lecture. (For more on Wikileaks and the possible indictment of Julian Assange, see "The Obama Administration Takes on Government Leakers; Transparency May be a Casualty" in the Winter/Spring 2012 issue and "WikiLeaks Founder Assange Seeks Asylum in Ecuador" in the Summer 2012 issue of the Silha *Bulletin*. For more information on Mark Stephens' lecture, see "Silha Lecture Highlights Free Speech in the Digital Age" in the Fall 2011 issue of the Silha *Bulletin*.)

> "The Pentagon Papers case teaches two important lessons. First, government officials ignore the First Amendment at their peril. Second, individuals should not buy claims of national security made by the government hook, line, and sinker."
>
> **— James C. Goodale**
> **28th Annual Silha Lecturer**

Goodale also discussed former defense contractor Edward Snowden's leaks about the NSA surveillance programs. (For more on Snowden's leaks, see "Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone and Internet Communication" in the Summer 2013 issue of the Silha *Bulletin*, and "Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms" on the first page of this issue.) "I think that Snowden has done a public service," he said. "If we did not have Snowden, we would not have the debate going on now" about surveillance, privacy and national security. However, Goodale said that he believes that Snowden should return to the United States to face prosecution. "He is a civil dissident, and a dissident has to face the risks of disobeying the law," Goodale explained. "He should come back and face the music."

Goodale also addressed the possibility of a federal shield law to protect reporters from having to divulge their sources. (For more information on the current status of a federal shield law, see "Senate Considers Federal Reporter's Privilege Bill" on page 8 of this issue of the Silha *Bulletin*). Goodale said he supports a federal shield law, but he acknowledged that new technology and the ability for any citizen to have a Twitter account, blog, or other means of sharing information make defining who qualifies for the shield law difficult. He explained that President Obama supported a federal shield law prior to becoming president. Since his election, President Obama only supports a shield law with a "huge gaping hole" in it for national security, Goodale explained.

"In every instance that I know about, Obama has chosen to favor national security over the First Amendment," Goodale said. "But isn't the lesson of the Pentagon Papers just the reverse?" Goodale concluded, therefore, that "President Obama has not learned the lessons of the Pentagon Papers."

A future president, Goodale hopes, would "push back."

"That's what Obama hasn't done," he said. "When faced with a choice of trying to balance national security and the First Amendment, he's always chosen national security — I hope we get a president the next time around who is more sophisticated about national security."

His hope is "that there will be some real debate . . . and . . . both sides of the aisle can see the issue with national security" trumping the First Amendment. At present, Goodale said he does not "see any end in the First Amendment fracas that Obama has geared up. He has ignored the First Amendment at his peril."

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.

– Cassie Batchelder
Silha Research Assistant

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

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

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

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 2014 and for the 2014-15 academic year will be due in **March 2014**.

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