THE SILHA Bulletin

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

Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone And Internet Communication

On June 5, 2013, the *Guardian* newspaper published the first in a series of articles disclosing massive data gathering efforts by the U.S. National Security Agency (NSA). Based on classified material leaked by former NSA contractor Edward Snowden, employed by the consulting firm Booz Allen Hamilton, the disclosures prompted a massive global debate over the NSA's collection and use of private electronic communications data. The orders leaked by Snowden indicated that President Barack Obama has continued (and potentially expanded) data collection programs begun under President George W. Bush. The programs Snowden revealed fall generally into two categories: (1) domestic collection of telephone and email "metadata" authorized under sections 214 and 215 of the USA PATRIOT Act, Pub. L. No. 94-12, 115 Stat. 272 (2001); and (2) generalized collections of Internet and other communications authorized under section 702 of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861 *et seq.* (1978).

According to the *Guardian*, Snowden's first disclosure was of a secret order from the Foreign Intelligence Surveillance Court (FISC) authorizing collection of telephone "metadata" — source and destination telephone numbers, location and routing data, and call time and duration — from telecommunications giant Verizon. The order appeared to be a routine renewal of an ongoing program that may have existed since at least 2006, according to a June 6, 2013 article in the *Washington Post*. The order did not authorize the collection of any data about phone call contents, but Snowden asserted that the contents of voice calls were gathered as well and could be accessed by any NSA analyst without supervisory approval, according to a June 17, 2013 article by CNET News. Citing documents provided to him by Snowden, *Guardian* reporter Glenn Greenwald stated in a speech on June 29, 2013 that the NSA gathered and stored the contents of as many as one billion phone calls per day. According to a June 7, 2013 article in the *Wall Street Journal*, similar orders authorized the NSA to collect data from other large telecommunications providers, and possibly to collect credit-card transaction details as well. The NSA's metadata collection program also targeted email communication, including the "to" and "from" addresses and the Internet protocol (IP) addresses of the parties to the communication, according to an Aug. 20, 2013 article in the *Wall Street Journal*.

The collection of metadata appears to be authorized by sections 214 and 215 of the USA PATRIOT Act. Section 215 authorizes the FBI to obtain FISC orders compelling telecommunications providers to disclose business records — such as phone records documenting dialed phone numbers and the duration of calls — so long as the court finds that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation … to protect against international terrorism or clandestine intelligence operations." It also prohibits telecommunications companies from revealing that they have been ordered to provide records. Section 214 authorizes similar orders allowing installation of automated "pen register" devices that capture information in real time, such as dialed telephone numbers. Telephone metadata may also contain location information, but the NSA has denied collecting or retaining location information under the metadata collection order, according to a July 31, 2013 article in the *Washington Post*.

Snowden's revelations of the NSA's global snooping activities have also cast a spotlight on other U.S. government information monitoring programs, some of which attempt to piggyback on the NSA's monitoring efforts. For example, the *Washington Post* reported on Aug. 5, 2013 that the NSA provides information to the Drug Enforcement Administration. According to an Aug. 5, 2013 article in the *Connecticut Post*, such disclosures appear to be permitted by statutory provisions in both the PATRIOT Act and the FISA that allow non-terrorism-related information to be shared with law enforcement if it relates to possible criminal activity. The *Connecticut Post* report noted that the NSA can turn over information to law enforcement, but law enforcement cannot "task" the NSA to collect information. However, *The New York Times* reported on Aug. 3, 2013 that other agencies, such as the Secret Service and the Department of Homeland Security, have complained that the NSA refuses to provide access to the information it collects because it treats their requests as "not … a high enough priority."

U.S. government data collection even targets old-fashioned "snail mail." The San Jose *Mercury News* reported on Aug. 2, 2013 that the U.S. Postal Service photographs "every piece of mail processed in the United States … and keeps [the photos] on hand for up to a month." Law enforcement agencies can request information on all mail delivered to particular individuals "without judicial review," according to an Aug. 3, 2013 report by *The New York Times*.

NSA, *continued on page 3*

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

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

Inside This Issue

Summer 2013: Volume 18, No. 3

Silha Center Staff

NSA, *continued from page 1*

The authorizing court order to collect metadata is not a warrant and the authorizing statutes do not require a warrant or a finding of probable cause before the court can issue orders authorizing the collection of telephone metadata. However, the NSA's telephone metadata collection programs probably do not run afoul of the Fourth Amendment. David Bender, who teaches privacy law at the University of Houston, argued in a July 16, 2013 article in *The Privacy Advisor* newsletter that "[t]he Supreme Court … has twice held that records voluntarily provided to a third party (such as telephony metadata) are not protected by the Fourth Amendment because there is no longer any expectation of privacy in them." Bender noted that the Supreme Court has also recognized exceptions to Fourth Amendment protections for "special needs" purposes, probably including national security, where "if the government does not collect the telephony metadata on an ongoing, real-time basis … necessary data may not be available when needed." In the words of U.S. Deputy Attorney General James Cole, defending the NSA's telephone metadata collection program in an Aug. 9, 2013 *Guardian* article, "If you're looking for the needle in the haystack, you have to have the entire haystack to go through."

COVER STORY

To the extent that the telephone metadata collection program gathers identifying data about Americans, Section 215 of the PATRIOT Act also requires the Attorney General to adopt "minimization procedures" prohibiting the retention and dissemination of such information absent consent, unless "necessary to understand the information" or "for law enforcement purposes." Therefore, although the NSA acquires a massive amount of information under the telephone metadata collection orders, analysts are not permitted "simply to 'wander through these records,'" and must instead state a "reasonable and articulable suspicion" that specific information is relevant to a terrorist investigation before they may query the database.

Snowden also revealed the existence of numerous programs designed to collect data through various forms of foreign surveillance. The most infamous disclosure involved a program called PRISM that Snowden claimed gave the NSA "direct access" to major Internet service providers, including "Google, Facebook and other U.S. Internet giants," such as Microsoft, YouTube, and Skype, according to a June 6, 2013 article in the *Guardian*. According to a July 10, 2013 *Washington Post* article, the monitoring scheme provided the NSA with "real-time notification" whenever a targeted user sent an email or logged in to an Internet chat program. The *Post* reported on July 10 that Google denied giving the "direct access" that Snowden asserted, and officials at Apple told the *Post* that they had "never heard" of any such program. Microsoft, Facebook, and several other major Internet providers also denied providing blanket data collection access to the NSA, stating that they only responded to legally authorized requests for data on specific individuals, according to a June 6, 2013 article by the online technology magazine *The Verge*. However, Snowden asserted that the companies were "misleading" with their denials, and he reiterated his claim that the NSA enjoyed "direct access" to Internet companies' servers, according to a June 17, 2013 report by Politico. Additional disclosures indicated that the relationship between NSA and major Internet service providers was close enough that NSA paid for the companies' costs when a court order compelled them to "meet new certification demands" as part of the PRISM program, according to an Aug. 22, 2013 report by the *Guardian*.

The same NSA documents about PRISM also mentioned the existence of several programs whereby the NSA monitored "communications on fiber cables and infrastructure as data flows past," according to a June 8, 2013 article by the *Guardian*. These programs, "code-named Blarney, Fairview, Oakstar, Lithium, and Stormbrew," are "designed to look for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the U.S." They have "the capability to track almost anything that happens online," but use filters to "let certain pieces of information through" while the rest of the data is discarded. Therefore, although the system has the theoretical capability to reach as much as 75 percent of all U.S. Internet activity, telecommunications providers can limit the streams of data that they provide to those they deem "responsive" to the foreign focus of these programs. When the NSA has requested access to data streams that "are more likely to include domestic communications," some telecommunications providers have denied the requests while others have provided the access. Accordingly,

> "If you're looking for the needle in the haystack, you have to have the entire haystack to go through."
>
> **— James Cole**
> **U.S. Deputy Attorney General**

although the "NSA is focused on collecting foreign intelligence, … some U.S. Internet communications are scanned and intercepted." However, the NSA is required to discard information gathered about Americans, unless a statutory exception applies, according to an Aug. 20, 2013 article by the *Wall Street Journal*.

On July 31, 2013, the *Guardian*'s Glenn Greenwald also reported on another putative NSA monitoring program called XKeyscore that "allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals." Citing documents provided by Snowden and purported to be NSA "training materials," Greenwald asserted that the XKeyscore program provided NSA analysts with the ability to "obtain ongoing 'real-time' interception of an individual's Internet activity" covering "nearly everything a typical user does on the Internet" without any court authorization or supervisory approval. The amount of data gathered is allegedly "staggeringly large," with various NSA databases containing over 850 billion "call events" and 150 billion "Internet records," with the NSA adding between one and two billion additional records every day in various databases. However, Marc Ambinder, editor-at-large for *The Week* magazine, argued in a July 31, 2013 post on the magazine's "Compass" blog that Greenwald and Snowden may have misinterpreted the NSA "training materials," and that XKeyscore may be nothing more than a system of user interfaces that provide narrowly-targeted search capabilities for the various databases that the NSA uses to try to organize its mass of data.

The NSA's foreign data gathering programs are authorized under section 702 of the FISA. Section 702 authorizes the U.S. government to monitor electronic communications by non-U.S. citizens "reasonably believed to be located outside the United States." It also authorizes the NSA to compel cooperation from "electronic communication service provider[s]," subject to the provider's right to petition the FISC for review. However, it also requires that the Attorney General adopt procedures designed to ensure that targets are located outside the United States, and it prohibits "intentional acquisition" of communications "as to which the sending and all intended recipients are *known* at the time of the acquisition to be located in the United States." This opens a loophole by which data gathering efforts that target foreigners

NSA, *continued on page 4*

NSA, *continued from page 3*

may result in inadvertent large-scale data gathering on Americans, according to a June 7, 2013 article in the *Atlantic*.

Section 702 of the FISA also requires that the Attorney General adopt "minimization" procedures designed to limit the unintentional acquisition and use of Americans' data. Accordingly, the Attorney General has promulgated procedures designed to minimize retention and use of inadvertently collected private data. The procedures require that intercepted domestic communications be "promptly destroyed upon recognition" unless the NSA Director "specifically determines, in writing," that the communication "is reasonably believed to contain significant foreign intelligence information," evidence of an imminent criminal act, evidence of a communications security vulnerability, or "information pertaining to a threat of serious harm to life or property."

Information regarding U.S. persons that is obtained from foreign communications intercepts can be retained if the information is "reasonably believed [to be] relevant to a current or future foreign intelligence requirement" or if it involves an imminent crime. Dissemination of information regarding U.S. persons is allowed only if all identifying information is removed or if any of several other criteria are met, including: when identifying information is "necessary to understand foreign intelligence information or understand its importance;" when there is evidence that the U.S. person is the agent of a foreign power or the target of foreign intelligence activity; when there is information that the U.S. person is "engaged in the unauthorized disclosure of classified national security information;" when there is information that the U.S. person is engaged in international terrorism; or when the information was acquired pursuant to a court-ordered surveillance.

Despite these procedures, there is extensive evidence that Americans' data has been collected and retained, according to a top-secret internal NSA audit leaked by Snowden that reported that from May 2011 to May 2012, there had been "2,776 incidents … of unauthorized collection, storage, access to or distribution of legally protected communications." However, according to an Aug. 15, 2013 article by the *Washington Post*, "most" of the incidents "were unintended" and "involved failures of due diligence or violations of standard operating procedures." For example, the *Post* reported that one incident involved the inadvertent interception of a "large number" of calls from the Washington, D.C. area as a result of a typographical error confusing Washington's area code (202) with the international dialing code for Egypt (20). The NSA's critics have nonetheless cast the violations in grave terms. Julian Sanchez of Politico characterized the NSA audit as the latest indication of a "systematic failure" of congressional oversight in an Aug. 16, 2013 op-ed.

The *Washington Post* reported on Aug. 21, 2013 that the NSA had "gathered as many as tens of thousands of e-mails and other electronic communications between Americans as part of a now-discontinued collection program" that the FISC declared to be unconstitutionally broad in October 2011. Reggie B. Walton, the chief judge of the FISC, told the *Post* on Aug. 15, 2013 that the court is unable to effectively limit any abuses because it is required to rely exclusively on the government's assertions of fact when considering its requests for orders authorizing surveillance. *The New York Times* reported on Aug. 21, 2013 that this limitation is particularly serious in light of the court's finding that the government had repeatedly misled the court in its filings and had failed to comply with the court's limitations on search terms used when querying databases. Nonetheless, Sen. Diane Feinstein (D-Calif.), chair of the Senate Intelligence Oversight Committee, stated on Aug. 16, 2013 that "the committee has never identified an instance in which the NSA has intentionally abused its authority to conduct surveillance for inappropriate purposes." However, on Aug. 23, 2013, the *Wall Street Journal* reported that "National Security Agency officers on several occasions have channeled their agency's enormous eavesdropping power to spy on love interests." The NSA responded to these reports of intentional violations by admitting that there had been "a couple" such violations, but that NSA had "zero tolerance" for them when they occurred. Sen. Feinstein riposted that the intentional violations had been "isolated cases" that in "most instances" did not involve Americans' personal information. "[T]hese small numbers of cases do not change my view that NSA takes significant care to prevent any abuses and that there is a substantial oversight system in place," she told the *Wall Street Journal* on Aug. 23, 2013. "When errors are identified, they are reported and corrected."

> "The NSA gathered as many as tens of thousands of e-mails and other electronic communiations between Americans as part of a now-discontinued collection program that the FISC declared to be unconstitutionally broad."
>
> **— *Washington Post***
> **Aug. 21, 2013**

Leaks Reveal International Monitoring Programs, Lead to International Outrage

Although Snowden has said multiple times that his motivation for the leaks centered upon concerns about threats to Americans' civil liberties posed by NSA monitoring programs, his disclosures have not been limited to programs that target Americans. Shortly after fleeing to Hong Kong following his initial leak, Snowden claimed that the NSA's monitoring extended to "people and institutions in Hong Kong and mainland China" and included "access to the communications of hundreds of thousands of computers," according to a June 14, 2013 report by the *South China Morning Post*. Snowden also asserted that the NSA was paying a British intelligence gathering agency to provide "access to and influence over Britain's intelligence gathering programmes" and to take advantage of "Britain's surveillance laws and regulatory regime," according to an Aug. 1, 2013 article in the *Guardian*. Snowden's disclosures were probably the source of reports that Germany's foreign intelligence service had been equipped with the XKeyscore application, according to a July 20, 2013 report by *Der Spiegel*. Snowden also charged that the NSA was eavesdropping on European Union offices, and monitored Internet traffic in Latin American countries, especially in Brazil, Venezuela, Colombia, and Mexico, according to a July 9, 2013 report by Reuters. However, Snowden did not describe the details of these international monitoring programs, and it is possible that they may be merely international components of the other programs he has claimed exist.

Snowden's disclosures about NSA spying have spawned global outrage and anger toward the United States. Reaction has been particularly strong in Europe, where data-protection officials have expressed concern that NSA monitoring of Internet traffic may violate Europeans' data privacy rights. The European Commission Vice-President expressed particular concern about the lack of "judicial redress" for European citizens targeted for surveillance, according to a June 18, 2013 report by Bloomberg News. The European political newspaper *New Europe* reported on Aug. 20, 2013 that the European Union's main data protection

advisory board has "demand[ed] answers" about how programs such as PRISM and XKeyscore affect European citizens. U.S. and EU officials plan to meet "to discuss the matter further" and to complete an "umbrella agreement" for law-enforcement activities, according to the June 18 Bloomberg News report. Of particular concern is the fate of the U.S.-EU "safe harbor" program, which "allows [U.S.] companies to transfer personal data without running afoul of the EU Data Protection Directive." In particular, the "national security exception" that allows companies to "deviate" from EU data-protection requirements "for national security reasons" may be reexamined, according to an Aug. 21, 2013 report in Bloomberg News' *Electronic Commerce and Law Report*. A final EU response to NSA data monitoring activities may not be possible until the EU finalizes reforms to its data protection regime, now stalled in the European Parliament.

Outrage toward the NSA's data gathering program has been particularly strong in Germany, where the scandal has become a significant issue in national elections. Opponents of Chancellor Angela Merkel have seized upon disclosures of German cooperation with NSA data gathering as a political weapon that resonates among Germans generally suspicious of government monitoring, though the issue appears unlikely to torpedo Merkel's reelection chances, according to an Aug. 21, 2013 report by Politico. Responding to the political crisis, Germany's Intelligence Minister acknowledged on Aug. 12, 2013 that Germany shares phone data with the United States, but denied that the data was specific enough to make Germany complicit in the United States' controversial drone attacks. On Aug. 2, 2013, Germany took the symbolic step of canceling a longstanding but rarely used agreement with U.S. and British intelligence agencies that allowed U.S. officials to request surveillance on German citizens. On July 29, 2013, the German Federal Data Protection Commissioner announced that Germany "would not approve data transfers [to non-EU countries] until the German government demonstrated that foreign intelligence services' access to German information is limited in a way that complies with the main purposes of the country's data protection laws: 'necessity, proportionality, and limitation to purpose.'" On Aug. 5, 2013, German Justice Minister Sabine Leutheusser-Schnarrenberger called for enhancements to the country's data protection laws that would bar U.S. companies from the German market if they violate German data privacy laws by participating in surveillance programs.

Russia, where Edward Snowden fled after he left Hong Kong, has also responded forcefully to his disclosures. A "top official of the parliamentary majority party" called for an investigation and for legislation imposing "an obligation to store all information of official bodies only on servers that physically are on the territory of the Russian Federation," according to a June 19, 2013 report from the online news site RT. The leaks led Russia to renew its previous demand that the United Nations "assume control of the Internet," and led Russia's Federal Guard Service to revert to using typewriters and paper documents for drafting its more classified communications, according to a July 11, 2013 report by *USA Today*.

Reactions in other European countries have been more muted. The European Parliament voted to open a formal inquiry, led by its Civil Liberties Committee, "to investigate the U.S. government's PRISM Internet surveillance program and other government surveillance programs." Concerns about PRISM may also have contributed to delays in the European Parliament's consideration of a new set of data protection rules, according to a July 1, 2013 report by Bloomberg News. On Aug. 5, 2013, the Irish Data Protection Commissioner rejected a request that it investigate Facebook and Apple (which have major offices in Ireland) for their participation in the PRISM program.

Rather than objecting to the NSA's monitoring methods, France attempted to imitate them, implementing an extensive telephone metadata gathering and analysis program of its own, according to a July 4, 2013 article in the *Guardian*. The United Kingdom has responded to revelations of NSA monitoring not by criticizing the United States, but by opening a criminal investigation into the London-based *Guardian* newspaper where many of Snowden's revelations have been published, according to an Aug. 22, 2013 AP story. On Aug. 18, 2013, the UK government detained Glenn Greenwald's partner, David Miranda, who had been acting as a courier for Snowden's files, while he was in transit through London's Heathrow Airport. Officials seized Miranda's computer equipment, which was purported to contain materials provided by Snowden. The Council of Europe condemned the detention, predicting a "chilling effect on journalists' freedom of expression as guaranteed by … the European Convention on Human Rights." Greenwald also vowed to accelerate publication of Snowden's leaks after Miranda was detained.

Officials in Brazil demanded that the United States explain its monitoring of Brazilian citizens' emails and phone calls, asserting on July 8, 2013 that any companies that cooperated in the monitoring "violated Brazilian law and acted against [its] constitution." On Aug. 13, 2013, Brazilian government officials threatened to cancel an impending purchase of U.S. fighter planes over the controversy. The Brazilian reaction prompted a call from U.S. Vice President Joe Biden to Brazilian President Dilma Rousseff on July 19, 2013 in an attempt to smooth relations. Al-Jazeera's Paula Daibert reported on July 14, 2013 that the NSA scandal might revive an "Internet Bill of Civil Rights" that has been stalled in the Brazilian Congress since 2011.

China, where Snowden originally fled, condemned the United States on July 28, 2013 for "double standards in the area of cyber security." Coming on the heels of U.S. criticism of cyber attacks originating from China, Snowden's revelations allowed China to cast itself as "the biggest victim of hacking in the world" in a campaign to turn the tables on the United States, according to a June 18, 2013 report by NPR.

Although not disclosed by Snowden, Canadian programs for gathering telephone metadata have come to light after Snowden's initial leaks. After a report from an internal watchdog disclosed violations of individual privacy rights in 2008, the programs were briefly suspended, according to classified documents leaked to the Toronto *Globe & Mail*. The *Globe & Mail* reported on June 15, 2013 that "although [Canadian intelligence] has never adopted the U.S. agency's methods or software wholesale," it "borrows [the NSA's] approach and language, as well as quite a bit of its technology." Canadian Defence Minister Peter McKay stated in a June 10, 2013 parliamentary hearing that Canadian monitoring "is specifically prohibited from looking at the information of Canadians" and is focused instead only on "foreign intelligence."

Congress, President Obama Struggle to Frame Reaction to NSA Disclosures

In the aftermath of Edward Snowden's initial disclosures about widespread NSA monitoring of domestic and global electronic communications, U.S. lawmakers have debated various proposals on how to reform the government's intelligence gathering programs. Congressmen Justin Amash (R-Mich.) and John Conyers (D-Mich.) co-sponsored a bill to reform Section 215 of the PATRIOT Act to require that the FISC restrict the government's acquisition of telephone records and other "tangible things" to only those pertaining to an already-identified target of an investigation. The new restrictions would have related only to the NSA's gathering of "metadata" such as dialed telephone numbers; acquisition of

NSA, *continued on page 6*

NSA, *continued from page 5*

foreign intelligence authorized under Section 702 of the FISA would be unaffected. To borrow Deputy Attorney General James Cole's haystack analogy, the Amash-Conyers amendment would have permitted the government to acquire only the portions of the haystack where metal-detection equipment had already indicated the presence of needles.

The House rejected the Amash-Conyers amendment 205-217 on July 25, 2013, but the vote marked the beginning of an increase in congressional opposition to NSA monitoring programs. On July 31, 2013, the Senate Judiciary Committee convened hearings to "sharply challenge[] the National Security Agency's collection of records." Responding to later disclosures of thousands of NSA "compliance incidents," Judiciary Committee Chair Sen. Patrick Leahy (D-Vt.) vowed additional hearings after the Senate returned from its August recess. Sen. Richard Blumenthal (D-Conn.) announced on July 24, 2013 that he is preparing a bill that would introduce "adversarial process" into the FISC's considerations of government requests for surveillance orders. Rep. Amash also predicted that more NSA reform bills would be introduced in the House, according to an Aug. 20, 2013 article by *U.S. News & World Report*.

These efforts expand pre-existing legislative attempts to protect Americans' online privacy. Senators Ron Wyden (D-Ore.) and Mark Udall (D-Colo.) have pressed "for more than a year" to close a legal loophole that allows the NSA to retain and search records of Americans' communications that are "incidentally collected" from foreign intelligence surveillance programs, according to an Aug. 9, 2013 article by the *Guardian*. Since January 2011, Sen. Leahy has proposed updating the 1986 Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 119, to require that the government obtain a search warrant before accessing stored email messages.

President Obama has indicated he is willing to consider proposals to reform NSA surveillance practices and oversight. During an Aug. 9, 2013 press conference, he expressed support for adding an "adversarial voice" to proceedings before the FISC. He conceded that the lack of an adversarial system caused the court to "only hear one side of the story," and that the court "may tilt … too far in favor of security" and "may not pay enough attention to liberty." At the press conference, the President also announced the establishment of a so-called "panel of outsiders" — former intelligence officials and civil liberty and privacy advocates — who would "assess [NSA] programs and suggest changes by the end of [2013]." On June 26, 2013, the President directed the Director of National Intelligence (DNI) James Clapper to determine what information could be declassified and disclosed to "provide a better context for [NSA] programs and to correct misrepresentations." Pursuant to that direction, the DNI has declassified a number of documents relating to NSA monitoring programs. Clapper even has created a blog through the popular online service Tumblr called "IC on the Record" to "provide[] immediate, ongoing and direct access to factual information related to the lawful foreign intelligence activities carried out by the U.S. Intelligence Community."

However, the *Guardian* reported on Aug. 9, 2013 that the President's proposals would not "materially alter the NSA's ongoing mass collection of phone data and surveillance of Internet communications in the short term." In an Aug. 12, 2013 editorial, the *Atlantic*'s Conor Friedersdorf accused the President of dissembling about the true scope of NSA monitoring and offering the mere illusion of reform. Andrew Malcolm of *Investor's Business Daily* argued in an Aug. 13, 2013 editorial that the presence of the DNI's Clapper at the lead of President Obama's new privacy board may produce a "whitewash" where accountability is frustrated. Andrea Peterson, contributor to the *Washington Post* technology blog "The Switch," reported on Aug. 22, 2013 that Obama's privacy board was comprised largely of former intelligence professionals and White House staffers, which prompted concerns among privacy advocates that the board would not be independent.

At least two panels of intelligence advisors existed well before the President's announcement. The first, the President's Intelligence Advisory Board, contained 14 members until 2012, but has since withered to only four members, all with "close ties" to the President, according to an Aug. 15, 2013 report by Politico. This board appears to be distinct from the new body of outside experts that the President announced, which Reuters reported on Aug. 27, 2013 included former counterterrorism adviser Richard Clarke, former CIA deputy director Michael Morell, former technology policy adviser Peter Swire, and University of Chicago law professors Geoffrey Stone and Cass Sunstein. Reuters reported that the five-member panel will present interim findings on surveillance and privacy issues by the end of October to DNI Clapper, and will given a final report, complete with policy recommendations, to President Obama by the end of the year. (Professor Stone delivered the 21st Annual Silha Lecture in October 2006.)

The second panel, the Privacy and Civil Liberties Oversight Board, held its first meeting on June 21 and its first public meeting on July 9, receiving testimony from "three panels of legal experts, former government officials, and civil rights proponents," according to Bloomberg News. Former FISC Judge James Robertson endorsed the appointment of an "advocate (with security clearance) to argue against the government at FISA Court hearings" and stated that civil liberties concerns prompted his resignation from the court, according to David Bender's July 16, 2013 article in *The Privacy Advisor*. Other panelists suggested removing the gag order that prevents telecommunications providers from disclosing that the government has requested phone records and making orders of the FISC public, Bender reported.

NSA Disclosures Provoke Legal Action

On June 11, 2013, the American Civil Liberties Union (ACLU) filed suit in U.S. District Court for the Southern District of New York, seeking a declaratory judgment that the NSA's collection of U.S. phone records violates the First and Fourth Amendments of the U.S. Constitution, an injunction barring the NSA from further collection of phone records, and an order directing the NSA to delete phone records already acquired. According to the complaint, the ACLU alleged that the NSA's "dragnet" collection of U.S. phone records "gives the government a comprehensive record of our associations and public movements, revealing a wealth of detail about our familial, political, professional, religious and intimate associations" that "is likely to have a chilling effect on whistleblowers and others who would otherwise contact the ACLU."

The ACLU's suit "could set up an eventual U.S. Supreme Court test," according to a June 11, 2013 article in *The New York Times*. In *Clapper v. Amnesty Int'l USA et al.*, 133 S.Ct. 1138 (2013), the Supreme Court rejected a similar challenge, ruling that the plaintiffs lacked standing because they could not show that they had been injured. However, because it dismissed the case on standing grounds, the court did not address whether the surveillance programs themselves were constitutional. Disclosures of widespread NSA collection of Americans' phone records could overcome the standing barrier and force the Supreme Court to address the constitutional merits of the NSA's programs, according to the *Times*. (For more information about the *Clapper* case, see "U.S. Supreme Court Rejects Challenge to Federal Surveillance Law" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

Snowden's disclosures and the ensuing firestorm of public debate have also emboldened some telecommunications providers to make a stand before the FISC. The *Electronic Commerce and Law Report* reported on July 17, 2013 that at least three major internet companies — Yahoo!, Google, and Microsoft — argued that the court should "unseal court documents related to the companies' response to government surveillance directives" because doing so would "offer more complete information about the process" and allow the companies to demonstrate that they resisted the government's demands. The three companies have filed petitions with the court claiming that they have a First Amendment right to publicly disclose the government's demands for business records.

Snowden Saga Is Latest Chapter in Battle between Leakers, Obama Administration

Before the *Guardian* published his initial leaks on June 5, 2013, Edward Snowden left his home in Hawaii for Hong Kong, where he had made unnamed contacts who arranged to keep him safe, according to a June 24, 2013 *Washington Post* article. On June 23, 2013, Snowden left Hong Kong for Moscow, after the U.S. Justice Department and the FBI began pressuring officials in Hong Kong to arrest him. Details emerged in an Aug. 26, 2013 *Guardian* article that Snowden's original plan was to fly from Moscow to Cuba, where the Cuban government had promised him asylum. However, the *Guardian* article cited a report by the Russian newspaper *Kommersant* that Cuban officials refused to allow Snowden to board the flight to Havana after bowing to pressure from U.S. officials.

On June 14, 2013, federal prosecutors filed a criminal complaint in the U.S. District Court for the Eastern District of Virginia, charging Snowden with theft of government property, unauthorized communication of national defense information, and willful communication of classified communications and intelligence information to an unauthorized person. The latter two charges come under the Espionage Act of 1917, 18 U.S.C. § 793. To avoid extradition to the United States, Snowden sought asylum from several countries while holed up at the Moscow airport, including Ecuador and Bolivia, before accepting an offer from the Russian government for one year of asylum on Aug. 1, 2013.

The asylum-seeking process has led to diplomatic tensions. In a June 24, 2013 press conference, White House press secretary Jay Carney called the facilitation of Snowden's travel from Hong Kong to Moscow "a deliberate choice by the [Chinese] government to release a fugitive," saying that "that decision unquestionably has [had] a negative impact on the U.S.-China relationship." On July 3, 2013, the plane of Bolivian President Evo Morales, flying to La Paz from Moscow, where Morales was attending a conference, was forced to land in Vienna, where officials searched it. The *Guardian's* Glenn Greenwald reported on July 3, 2013 that the plane had been diverted after France, Spain, and Portugal withdrew airspace rights to the flight due to rumors that Snowden might be aboard, purportedly bound for asylum in Bolivia. However, the *Washington Post* reported on July 3, 2013 that the pilots may have chosen to land due to faulty fuel indicators, and EU officials obtained consent to search the plane. Regardless of what actually happened, President Morales called the incident an act of "American imperialism," which has soured relations between the United States and many of Latin America's leftist governments. Finally, after Russia granted Snowden one year of asylum, President Obama cancelled a September summit with President Vladimir Putin, although Andrew Weiss of the Carnegie Endowment for International Peace argued in an Aug. 8, 2013 *Euronews* article that relations between the U.S. had been growing sour over disagreements on policy toward Iran and Syria before the Snowden issue.

Snowden's slate of revelations about NSA data gathering is almost certainly not yet complete. Greenwald told the Brazilian Senate on Aug. 8, 2013 that Snowden provided him between 15,000 and 20,000 documents from NSA servers that will provide the source material for continuing revelations about NSA monitoring activities around the globe. The scope and extent of Snowden's reports have led some to believe that "[t]he state … monitors and records everything everywhere," and that we live in an environment of "total surveillance" with "zero privacy." Greenwald said that Snowden's files have been given, in encrypted form, to "several people" and that "[i]f anything happens to Snowden, the files will be unlocked," according to a June 25, 2013 report by *The Daily Beast*.

Whatever happens to Snowden, the fallout from his leaks has sparked a debate on the extent to which the government should hire private contractors like Snowden to work with classified information on national security. The *Baltimore Sun* reported on June 10, 2013 that nearly "70 percent of the money spent by intelligence agencies flows to contractors, … and nearly one-quarter of the 4.9 million people who hold security clearances work for contractors." The *Sun* noted that those numbers do not include NSA contractors like Snowden, because the NSA does not disclose its budget. However, according to an Aug. 30, 2013 report by the *Washington Post*, purportedly based on documents leaked by Snowden, the NSA requested $10.8 billion from the federal government in 2013.

Particularly at a time when the Obama administration has been cracking down on leakers, some have debated whether private contractors should be more closely monitored due to their perceived "outsider" status. (For more Silha *Bulletin* coverage of the Obama administration crackdown on leakers, see "Open Government Advocates Criticize Obama's Prosecution of Leakers" in the Winter/Spring 2011 issue and "Manning, Kiriakou Face Punishment for Blowing the Whistle on the War on Terror" in the Winter/Spring 2013 issue.) Stan Soloway, CEO of the Professional Services Council, a trade association representing more than 330 private contractors working for the government, told Politico on June 10, 2013 that Snowden's leaks should not lead to harsher treatment for government contractors because contractors and government employees go through the same security clearance process. Loren Thompson, a defense consultant for the Lexington Institute, an Arlington, Va.-based think tank specializing in national security policy, told Politico for its June 10 article, "Bradley Manning was still in the government while he was leaking, and Mr. Snowden got most of what he knew from the government. So the fact that he was working for a contractor seems incidental." However, Thompson criticized the government for "going out and hiring hackers [like Snowden], which is not a great way to keep secrets." Lee Stone, a vice president of the International Federation of Professional and Technical Engineers, a union representing many federal employees with security clearance, took Thompson's criticism a step further. Stone told the *Washington Post* on June 10, 2013 that the Snowden story "is yet another example of why outsourcing our national security to mercenary rent-a-cops is a bad idea."

Silha Center Director Jane Kirtley and Silha Bulletin *Editor Brett Johnson contributed to this story.*

– Jason Steck
Special Contributor to the Silha *Bulletin*

Britain Seeks to Update "Snooper" Legislation

British Prime Minister David Cameron's government is seeking to reintroduce the 2012 Regulation of Investigatory Powers Act (RIPA), labeled the "Snooper's Charter" by its opponents, in order to expand the ability of law enforcement to access individuals' phone and email data. The May 2013 murder of a young British soldier in the London neighborhood of Woolwich, allegedly by two self-proclaimed jihadists, prompted many politicians to call for the resurrection of the RIPA to help prevent such attacks, according to a May 28, 2013 report by the UK-based organization Big Brother Watch, which campaigns against the expansion of government surveillance. However, the revelation of the U.S. National Security Agency's PRISM program sparked renewed criticism of this initiative, according to a June 7, 2013 article by the *Huffington Post*.

SURVEILLANCE

Home Secretary Theresa May introduced RIPA in June 2012 with an express goal of "maintain[ing] the ability" of authorities "to access vital communications data under strict safeguards to protect the public." The bill would extend the range and time that certain types of data must be stored by telecommunication firms, according to a May 9, 2012 article in the *Daily Telegraph*. Currently, UK firms are expected to keep phone records and information about messages sent via their own email services for 12 months. The data retained allows law enforcement officials to gain insight into targets of criminal and terrorism investigations. However, the RIPA would extend the current requirements and include not only emails and phone call data, but also details of text messages, information sent on social media and webmail, and voice calls made through the Internet, and gaming, according to a July 19, 2012 report by the BBC. The data collected would include the time, duration, author and receiver of the communication, and the location of the device where the communication originated. Additionally, only officers from four law enforcement agencies would have access to the information: the police, the Serious and Organised Crime Agency, the intelligence agencies, and HM Revenue and Customs agencies. However, officers still will need a warrant before viewing or listening to the actual content of the messages.

The RIPA has been strongly criticized since its introduction in June 2012. Privacy groups have been quick to accuse the government of overreaching and sacrificing personal liberty at the expense of "snooping." Privacy watchers are especially vocal in their outcry against law enforcement agencies having the ability to use a "request filter," which could allow officials to fish and trawl for information concerning a suspect's Internet browsing habits, contacts, and movements, according to the BBC. Although May promised that the government will not be using one central database to house the information, some still believe that the ability of the government to pull from both government and private databases effectively gives it access to one large receptacle of information. Dr. Julian Richards, co-director of Buckingham University's Centre for Security and Intelligence Studies, told the BBC on July 19, 2012 that the request filter would function more or less as a search engine for law enforcement authorities. Former Shadow Home Secretary David Davis told the BBC on July 19, 2012 that the law would not be effective against terrorists because they already use proxy servers and multiple phones to avoid detection.

Nick Pickles, director of Big Brother Watch, also told the BBC on July 19, 2012, "The filtering provisions are so broadly worded and so poorly drafted that it could allow mining of all the data collected, without any requirement for personal information, which is the very definition of a fishing trip." Jim Killock, of the Open Rights Group, a UK-based organization that advocates for freedom of expression and personal privacy on the Internet, told the BBC on July 19, 2012 that government snooping has the potential to "compromise journalistic sources, deter whistleblowers and increase the risk of personal details being hacked." These concerns are in addition to the more subtle concern that individuals' speech inadvertently may be chilled if they believe "Big Brother is watching," Killock said.

Privacy advocates are not the only groups who have expressed worries about the implications of the bill. Microsoft, Twitter, and Yahoo!, among others, wrote an open letter to Home Secretary May on May 31, 2013 in which they labeled the bill "controversial" and argued that it would be too expensive to implement. They wrote, "We do not want there to be any doubt about the strength of our concerns in respect of the idea that the UK government would seek to impose an order on a company in respect of services which are offered by service providers outside the UK."

Supporters have argued that the bill is needed for law enforcement to catch up to changing technology and effectively fight terrorism and other crimes, and that much of the criticism stems from lack of trust in government institutions, not necessarily in their methods. Supporters also point to the increased use of social media sites and online gaming among criminals and terrorists, and argue that the government needs improved access to these technologies to level the playing field, according to a June 13, 2012 report by the BBC. The current legislation does not allow the tracking of communication on Skype, Facebook, or Google Chat, which are becoming some of the most prolific ways to communicate ideas and plans with others. Supporters argue that the government is not interested in reading the content of these messages without a warrant, but rather wants to track the originating and receiving information, according to the BBC. Jamie Bartlett, head of the Violence and Extremism Programme and the Centre for the Analysis of Social Media, wrote in a *Huffington Post* op-ed on April 26, 2013 that "[m]aking sure security service and policing powers are up to date and adequate — of course while avoiding unnecessary intrusion, misuse and expense — is something we all have a very big interest in."

The May 2013 Queen's Speech seemed to point to a desire for Internet service providers and Parliament to reach an agreement together on government Internet surveillance policies. The Queen stated, "In relation to the problem of matching Internet protocol addresses, my Government will bring forward proposals to enable the protection of the public and the investigation of crime in cyberspace." However, the bill faces many political hurdles. Liberal Democrats and Conservatives have called for the death of the draft bill, citing privacy, cost, and security concerns, according to a May 28, 2013 report by the online magazine *Info Security*. Some have suggested that the Conservative Party and Labour might be able to find common ground on the issue, though it almost certainly would alienate the Liberal Democrats from the coalition, according to *Info Security*. Without the Liberal Democrats, the Conservatives would have a difficult time maintaining the needed majority to retain control of the government if a vote of confidence was called.

Silha Center Director Jane Kirtley contributed to this story.

– Jason Steck
Special Contributor to the Silha *Bulletin*

Manning Sentenced to 35 Years in Prison for Leaks

LEAKS

While NSA leaker Edward Snowden faces the possibility of espionage charges while in asylum in Russia, U.S. Army leaker Bradley Manning was convicted of espionage in military court at Fort Meade, Md. on July 30, 2013. On Aug. 21, 2013, U.S. Army Judge Col. Denise Lind sentenced Pfc. Manning, who in 2010 leaked more than 700,000 government documents to Wikileaks, to 35 years in prison, to be dishonorably discharged from the Army, and to be demoted from the rank of Private First Class to Private. Lind had found Manning guilty of six counts of violating the Espionage Act, 18 U.S.C. § 793, as well as 14 lesser charges relating to theft of military property and improper use of a military computer, for which Manning had faced up to 136 years in prison. Lind found Manning not guilty of the charge of aiding the enemy, the most serious of the charges sought by military prosecutors, which carried a life sentence. In November 2012, Manning opted for Lind to decide the case instead of a jury comprised of military officers. (For more information on the Bradley Manning case, see "Judges Rebuke Government on Leaks Prosecutions" in the Summer 2011 issue of the Silha *Bulletin*, "The Obama Administration Takes on Leakers; Transparency May Be a Casualty" in the Spring 2012 issue, and "Manning, Kiriakou Face Punishment for Blowing the Whistle on the War on Terror" in the Winter/Spring 2013 issue.)

Prosecutors had sought a sentence of 60 years and a $100,000 fine. According to an Aug. 21, 2013 article in *The New York Times*, prosecutors wanted the 60-year sentence to act as a deterrent for would-be leakers, and they sought the $100,000 fine to cover some of the costs incurred by officials who reviewed the documents that Manning leaked in an effort to "mitigate damages." Manning's defense asked Judge Lind for a sentence of 20 years, which Manning had faced in February 2013 when he pleaded guilty to 10 of the 22 charges against him. Lind ruled that Manning would receive a credit of 1,294 days for the time he spent in prison awaiting trial and for the 112 days in which he was held in solitary confinement following his arrest, according to the *Times*. Military convicts become eligible for parole after they have served one-third of their sentence, the *Times* reported. Therefore, according to Manning's lawyer, David Coombs, Manning would become eligible for parole in a little over seven years because his 1,294-day credit would be applied to the first third of his sentence.

In the sentencing phase of the trial, Coombs argued that Army officials should be held responsible for the leaks because they did not cancel Manning's top-secret security clearance after Manning showed signs of mental instability. Coombs also argued that Lind should be lenient in her sentencing because Manning was "naïve" and "idealistic" and did not know how serious his actions were. Navy psychiatrist Capt. David Moulton testified for the defense during the Aug. 14, 2013 sentencing hearing that Manning "underestimated how much trouble he would get in." According to the BBC, Moulton told the court that Manning "was under the impression that the leaked information was going to change how the world saw the war in Iraq," and that he "was really relying on his morals and his ideology and not thinking beyond that."

Manning's defense team also tried to argue during the sentencing phase that because of Manning's documented history of issues with gender identity, the Army could have and should have removed his security clearance — on the grounds that he was too mentally unstable to hold such a clearance — before he had the opportunity to leak the documents. The defense pointed to an email that Manning sent to a superior officer in April 2010 with an attached photo of Manning wearing a woman's wig with the subject line "My Problem," and the fact that the superior officer did not report the email, as evidence of the Army's mishandling of Manning. It is unknown whether this line of defense succeeded in reducing Manning's sentence, as Judge Col. Lind did not state a reason for her sentence of 35 years. On Aug. 22, 2013, Manning announced that he was, in fact, female, wanted to be known as Chelsea Manning, and that he wanted to begin hormone therapy to transition to becoming female.

On Aug. 14, 2013, Manning made an unsworn statement to the court during his sentencing hearing. "I'm sorry that my actions hurt people," he said, according to multiple media reports. "I'm sorry that [the actions] hurt the United States. I'm apologizing for the unexpected results of my actions. The last three years have been a learning experience for me."

The 35-year sentence is the longest handed down against a leaker of government documents. In January 2013, former CIA officer John Kiriakou received a 30-month sentence for leaking the name of an undercover CIA agent, the longest sentence until Manning's. In a tweet following the sentencing, WikiLeaks called the sentence a "significant strategic victory," due to its relative leniency. Some analysts argued that despite the 35-year sentence, the fact that Manning was found not guilty of aiding the enemy was a victory for whistleblowers. BBC North America editor Mark Mardell wrote in a July 30, 2013 column that had Manning been found guilty of aiding the enemy, "the way would have been opened to treat the public leaking of any secrets as treason."

Others have argued that the 35-year sentence likely will not deter future leakers. Gary Solis, a law professor at Georgetown University who served as a military prosecutor and judge, told the AP on Aug. 21, 2013 that potential future cases against civilian leakers such as Edward Snowden need not "look to a court-martial for precedent." However, Coombs told the AP that the 35 years would indeed act as a "strong deterrent." Coombs told multiple media that he planned to file a request for President Obama to either pardon Manning or commute his sentence.

Advocates of government transparency have called Manning a "hero" for leaking the documents and argued that he did not deserve punishment. In an Aug. 12, 2013 op-ed in the *Los Angeles Times*, Robert Meeropol, son of Ethel and Julius Rosenberg, who were executed in 1953 for violating the Espionage Act, argued that the secrecy surrounding his parents' case has taught him "very valuable lessons both about security failures and the increased need for constitutional protections in times of crisis." Comparing his parents' leaks to Manning's, Meeropol argued his parents were "misguided" in placing their faith in another nation (the Soviet Union), and he praised Manning for leaking information to "humanity as a whole."

Activist and columnist Norman Solomon stated in an Aug. 13, 2013 op-ed for the news website Truthout that he would formally nominate Manning for the Nobel Peace Prize. "Opening heart and mind to moral responsibility — seeing an opportunity to provide the crucial fuel of information for democracy and compassion — Bradley Manning lifted a shroud and illuminated terrible actions of the USA's warfare state," Solomon wrote.

Brett Johnson
Silha *Bulletin* Editor

Department of Justice Revises Guidelines for Investigating Journalists

In a May 23, 2013 speech on national security, President Barack Obama directed Attorney General Eric Holder to "review Justice Department guidelines for investigations that involve journalists," (28 C.F.R. § 50.10) according to a report by the *Huffington Post* from the same day. The call to evaluate the DOJ's policies came after DOJ officials secretly subpoenaed the AP's phone records in April and May 2012, and executed a search warrant to seize emails of Fox News reporter James Rosen on May 20, 2013, under the theory that Rosen was a "co-conspirator" in a criminal case involving the leak of State Department documents. (For additional information about 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*.)

REPORTERS' PRIVILEGE

Holder announced the release of the revised guidelines on July 12, 2013. (The new guidelines are available online at http://www.justice.gov/ag/news-media.pdf). The guidelines declare that the DOJ's view is that "the use of tools to seek evidence from or involving the news media as an extraordinary measure" that would be used "only as a last resort." The guidelines also state that when searching news organizations' materials, the scope of those searches must be limited, so that the need of the media to gather information is balanced with the need of law enforcement to gather evidence.

Section one of the new guidelines, titled "Reversing the Existing Presumption Regarding Advance Notice," deals with the DOJ's policy on issuing subpoenas for journalists' phone or other communication records held by third parties such as phone companies. Under the old guidelines, negotiation with the news media prior to issuing a subpoena for records relating to newsgathering activities related to criminal or civil investigations by the DOJ was expected to occur when the responsible Assistant Attorney General decided such negotiations would not "pose a substantial threat to the integrity of the investigation." Under the revised guidelines, prior notification will always take place, unless the Attorney General determines that doing so would pose a "clear and substantial threat" to the investigation in question. The guidelines provide that "only [in] the rare case" would the Attorney General delay notification for an initial 45-day period. An additional 45-day delay can be permitted, but only after review by the newly established News Media Review Committee. No further delays can be granted beyond a total of 90 days.

The News Media Review Committee, described in section three, is to advise the Attorney General and the Deputy Attorney General when DOJ attorneys seek authorization to obtain news media records in investigations related to the unauthorized disclosure of government information. The committee also will provide advice when DOJ attorneys are seeking testimony from a journalist that could disclose the identity of a confidential source, or when the DOJ is seeking news media records relating to any law enforcement investigation. Members of the News Media Review Committee will include senior DOJ officials who are not directly involved in the investigations under current review.

Section two of the revised guidelines concerns searches and seizures related to the Privacy Protection Act of 1980 (PPA), 42 U.S.C. § 2000aa. Under that law, search or seizure of a journalist's work product or documentary materials is generally prohibited, unless it falls under the "suspect exception." The suspect exception applies to cases where there is "probable cause to believe that the person possessing such materials has committed or is committing a criminal offense," and where the materials include "the receipt, possession, or communication of information relating to national defense, classified information, or restricted data." Under the previous DOJ guidelines, a Deputy Assistant Attorney General could authorize an application for a search warrant for materials covered by the PPA with no higher review. However, under the revised guidelines, such materials may only be sought under the "suspect exception" of the PPA, and only when the journalist is the focus of a criminal investigation that is not related to newsgathering activities.

In addition, section two of the revised current DOJ guidelines stipulates that search warrants and court orders pursuant to the 1986 Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703(d), and seeking to obtain journalists' Internet communication records from a third party must be approved by the Attorney General. The information sought must be essential to the investigation, and other reasonable investigative steps must be taken before seeking a reporter's materials. The request also must be narrowly tailored to obtain only what information is necessary to the investigation in question.

Other sections of the new guidelines deal with oversight of investigations related to the news media, the safeguarding of information gathered from journalists, and training DOJ personnel to comply with the revised guidelines. Following the release of the revised guidelines, Attorney General Eric Holder stated, "The Department of Justice is firmly committed to ensuring our nation's security, and protecting the American people, while at the same time safeguarding the freedom of the press. These revised guidelines will help ensure the proper balance is struck when pursuing investigations into unauthorized disclosures." However, Holder also stated that "there are additional protections that only Congress can provide. For that reason, we continue to support the passage of media shield legislation."

On July 12, 2013, the AP released the following statement regarding the revised guidelines: "The Associated Press is gratified that the Department of Justice took our concerns seriously. The descriptions of the guidelines … indicate[] they will result in meaningful, additional protection for journalists. We'll obviously be reviewing them more closely … but we are heartened by this step." Other media organizations, such as the Newspaper Association of America and the Radio Television Digital News Association, also applauded the revisions to the DOJ's guidelines, but called upon Congress to enact a federal shield law. The "Free Flow of Information Act of 2013," S. 987, was introduced by Sen. Charles Schumer (D-N.Y.) on May 16, 2013, and is scheduled to be reviewed by the Senate Committee on the Judiciary on Sept. 12, 2013. The *Bulletin* will track updates as the story unfolds.

Elaine Hargrove
Silha Center Staff

D.C. Circuit Upholds FOIA Denial on Bin Laden Photos

On May 21, 2013, the U.S. Court of Appeals for the District of Columbia Circuit released a *per curiam* opinion that upheld the U.S. government's power to deny Freedom of Information Act (FOIA) requests for the release of photographs taken of the burial at sea of Osama bin Laden. In *Judicial Watch, Inc. v. U.S. Dep't of Def.*, 715 F.3d 937 (D.C. Cir. 2013), the court affirmed an earlier district court decision, holding that 52 photographs of the corpse and burial of bin Laden could be withheld by the government under a national security exception to the FOIA.

FOIA

After the Navy SEAL mission in Abbottabad, Pakistan, led to the killing and sea burial of bin Laden, many news outlets and political groups sought the release of the photographs via FOIA requests. The CIA classified the photographs as top-secret and denied the requests. John Bennett, director of the National Clandestine Service agency of the CIA, justified withholding the photographs in a Sept. 26, 2011 statement, saying the photographs "reasonably could be expected to result in exceptionally grave damage to the national security." Bennett argued that releasing the "gruesome images of [bin Laden's] corpse … would provide terrorist groups and other entities hostile to the United States with information to create propaganda, which, in turn, could be used to recruit, raise funds, inflame tensions, or rally support for causes and actions" which threaten the United States. Additionally Bennett stated that some of the photographs that were used to identify bin Laden could reveal techniques used in the "CIA's facial recognition technology, which is highly classified."

Conservative government watchdog group Judicial Watch challenged the FOIA denial on May 4, 2011. Judicial Watch promotes government transparency and accountability in large part through FOIA requests and litigation. Judicial Watch President Tom Fitton wrote in a May 6, 2011 post on the organization's blog that the mission to kill bin Laden was "arguably the most important military operation in our lifetimes and we need to complete the public record."

On April 26, 2012, the CIA's denial was upheld in federal district court. *Judicial Watch, Inc. v. U.S. Dep't of Def.*, 857 F. Supp. 2d 44, (D.D.C. 2012). The district court found that the government had fulfilled requirements of FOIA exemption 1, which permits the government to withhold classified information that might threaten national security. Judge James E. Boasberg wrote, "The test is not whether the court personally agrees in full with the CIA's evaluation of the danger — rather, the issue is whether on the whole record the Agency's judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence."

> "The opinion is craven, absurd, and undermines the rule of law. There is no provision of the Freedom of Information Act that allows documents to be kept secret because their release might offend our terrorist enemies."
>
> **— Judicial Watch**

On appeal, the D.C. Circuit affirmed that the government had properly withheld the photographs under FOIA exemption 1. The court found that there were no First Amendment rights at stake in the case, because the issue was access to records under FOIA, not government restrictions on private speech. The court found the government demonstrated that the documents in question pertained to one of eight subject-matter classification categories, and justified top-secret classification by showing the information could "reasonably be expected to cause … 'exceptionally grave' harm that is identifiable or describable."

According to the appellate panel, "[a]t least some of the images 'pertain to … intelligence activities (including covert action), [or] intelligence sources or methods,' and all 52 images plainly 'pertain[] to … foreign activities of the United States." Because the photographs related to foreign activities, the court found that they fell within that subject-matter category. As to the expectation of "exceptionally grave" danger, the court relied on declarations of government officials who argued that "reasonably analogous disclosures have led to widespread and fatal violence in the Middle East, some of it directed at U.S. interests." The officials cited publication of a Danish cartoon depicting the prophet Muhammad and an erroneous article in *Newsweek* in 2005 that alleged American soldiers had desecrated a Quran as similar releases that had prompted violence. (For more on the controversy surrounding the Danish cartoon, see "Controversial Cartoons Lead to Worldwide Concern For Speech, Press Freedom, and Religious Values" in the Winter 2006 issue of the Silha *Bulletin*.)

The court noted that "Judicial Watch protests that the government's declarations show nothing more than that release of the images may cause 'some individuals who do not like the United States' to commit violence overseas, and that the courts should not succumb to this kind of blackmail." However, the court found the government's examples were not "generalized claims" predicting violence, but rather "specific, reasonably analogous examples." "Finally," the court found, "it is undisputed that the government is withholding the images not to shield wrongdoing or avoid embarrassment, but rather to prevent the killing of Americans and violence against American interests." The court found that any "statement of threatened harm to national security will always be speculative to some extent" and that the court's role "is to ensure that those predictions are 'logical' or 'plausible.'" Because the government fulfilled this standard, it satisfied its substantive burden under FOIA exemption 1.

To classify documents as top-secret, as the CIA did with the bin Laden photographs, government agencies must either cite the reasoning for the classification from the classification guide, or an official with classification authority must certify that the documents are sufficiently sensitive to be classified. In this case, the CIA initially failed to properly mark the photographs with either. However after the documents were requested, CIA Director Bennett personally reviewed and classified the images. Although this was not normal classification procedure, the court deferred to Bennett's decision and found the procedure sufficient. The court therefore found the substantive and procedural elements of classification proper and denied Judicial Watch's challenge of the CIA's decision to withhold the photographs.

In a May 21, 2013 press release in response to the circuit court's decision, Judicial Watch said, "The opinion is craven, absurd, and undermines the rule of law. … There is no provision of the Freedom of Information Act that allows documents to be kept secret because their release might offend our terrorist enemies." On Aug. 19, 2013, Judicial Watch announced that it filed

FOIA, *continued on page 12*

FOIA, *continued from page 11*

a *certiorari* petition with the U.S. Supreme Court asking for review of the decision.

Although many news outlets filed requests for the photographs after bin Laden's 2011 death, Judicial Watch was the only organization to mount a legal challenge, and the public reaction to the circuit court's decision has been muted. Neither the left-leaning American Civil Liberties Union (ACLU) nor the right-leaning American Center for Liberty and Justice (ACLJ), two organizations that promote freedom of speech and government accountability, had acknowledged the decision through their websites as the *Bulletin* went to press.

Bin Laden Records Purged From Department of Defense, Possibly Violating FOIA

In the wake of the Judicial Watch decision, allegations have emerged that the Department of Defense improperly destroyed records relating to the bin Laden raid and burial, allowing the department to circumvent subsequent FOIA requests for the records. In response to an Aug. 9, 2011 inquiry by Rep. Peter King (R-N.Y.), Chairman of the House Committee on Homeland Security, the Department of Defense Inspector General commissioned a report investigating leaks of classified information about the bin Laden operation to the makers of the film "Zero Dark Thirty." The film, released in January 2013, portrays the CIA's search for bin Laden. A draft of that Defense Department report, acquired in June 2013 by government watchdog group Project on Government Oversight, revealed that government officials destroyed records and information regarding the raid. The report stated that Commander of U.S. Special Operations William McRaven ordered that the names and photographs related to the raid not be released. "This effort included purging the combatant command's system of all records related to the operation and providing these records to another Government Agency." This language was left out of the final Inspector General's report, released June 14, 2013. A spokesman for McRaven declined to comment to the AP. However, on July 8, 2013, AP reporter Richard Lardner reported that "current and former Defense Department officials knowledgeable about McRaven's directive and the inspector general's report told the AP the description of the order in the draft report was accurate." These sources also confirmed that the report's reference to "another Government Agency" was code for the CIA.

The report characterized the transfer as an effort to protect the identities of those involved in the bin Laden operation, but it also might have allowed the Department of Defense to deny FOIA requests for the records. According the to AP's Lardner, "The Freedom of Information Act generally applies to records under an agency's control when a request for them is received." Depending on the timing of the purge, the Defense Department may have been able to respond to FOIA requests accurately claiming it did not have the requested records. Although many media organizations and civil liberties groups, including the AP and Judicial Watch, also filed FOIA requests with the CIA, the CIA classified the information and denied the requests. Lardner reported that pursuant to the 1984 CIA Information Act, 50 U.S.C.A. § 431, the CIA has greater freedom than the Department of Defense to deny such FOIA requests as to its operational files. The CIA's denials were challenged by Judicial Watch in 2011 and upheld by both the District Court for the District of Columbia and a Court of Appeals for the District of Columbia Panel in *Judicial Watch*.

> "Welcome to the shell game in place of open government. Guess which shell the records are under. If you guess the right shell, we might show them to you. It's ridiculous."
>
> **— Thomas Blanton**
> **Director,**
> **National Security Archive**

The CIA denied any wrongdoing, stating that because the Navy SEALs who performed the operation were overseen by then-CIA Director Leon Panetta they were effectively CIA operatives. CIA spokesman Preston Golson said in an emailed statement to the AP, "Records of a CIA operation such as the (bin Laden) raid, which were created during the conduct of the operation by persons acting under the authority of the CIA Director, are CIA records." Golson called the allegations that the records were transferred to the CIA and purged from Department of Defense files to avoid the legal requirements of FOIA "absolutely false."

However, even if the CIA's characterization of the mission is true, the Department of Defense's actions may have violated federal law. A provision of the Federal Records Act, 44 U.S.C. 31 § 3301, requires heads of Federal agencies to obtain the approval of the National Archives before transferring records and purging the files. Because the Department of Defense and the CIA are in different departments, such approval would have been required for the bin Laden records transfer. According to the AP's Lardner, Archives spokeswoman Miriam Lieman said the Archives was not aware of a request by the Special Operations Command to transfer records to the CIA.

Dan Metcalfe, a former director of the Justice Department's Office of Information and Privacy who oversaw U.S. Compliance with FOIA, said in an interview with the AP for a July 8, 2013 article, "I don't think there's an exception allowing an agency to say, 'Well, we didn't destroy it. We just deleted it here after transmitting it over there.' High-level officials ought to know better." Thomas Blanton, director of the National Security Archive, a private research institute at George Washington University, told the AP for the July 8, 2013 report that the actions reveal a larger strategy of avoidance by federal officials. "Welcome to the shell game in place of open government," Blanton said. "Guess which shell the records are under. If you guess the right shell, we might show them to you. It's ridiculous."

Meanwhile, Judicial Watch filed another FOIA claim for records of the bin Laden raid, seeking disclosure of the names of government agents that had been redacted from public documents. In *Judicial Watch v. Dep't of Def.*, No. 1:12-cv-00049-RC (D.D.C. Aug. 28, 2013), the organization argued that although the names of several SEAL and CIA officers involved "would normally be exempt from disclosure … the government placed their names in the public domain by disclosing them to the filmmakers" of "Zero Dark Thirty." However, District Court Judge Rudolph Contreras found in a memorandum opinion released Aug. 28, 2013 that the narrow legal question at stake was "whether a FOIA requester that knows information has been disclosed to a private party is necessarily entitled to that same disclosure." Judge Contreras ruled that the names were not part of the public domain, because although they had been disclosed to the civilian filmmakers, "the general public does not know the names." The court found that had the filmmakers released the names to the public, "this would be a much harder case, one that might turn on the question

of whether those names had been 'officially acknowledged'" by government officials. To overcome a legitimate government exemption, a FOIA requester must demonstrate that the information is "truly public," which Judge Contreras ruled Judicial Watch was unable to do. As the *Bulletin* went to press, Judicial Watch had not announced whether it would appeal the decision.

Department of Defense Releases Names of Guantanamo Prisoners Being Held Indefinitely

On June 17, 2013, the *Miami Herald* released a list of 48 men being held indefinitely as prisoners at the Guantanamo Bay Naval Base in Cuba. The list was created by an Obama Administration task force in 2010. It identifies 48 prisoners, two of whom are now deceased, who the government considered too dangerous to transfer from the facility, and against whom the government believed it did not have enough evidence to convict in court. The government has imprisoned the men indefinitely as war prisoners, pursuant to the 2001 Authorization for Use of Military Force, 50 U.S.C. § 1541. Although the names of all Guantanamo prisoners are public, information on which inmates had been selected for indefinite detention had never been released.

Miami Herald reporter Carol Rosenberg, who has reported extensively on Guantanamo, filed a Dec. 31, 2012 FOIA request for the release of the list. After the Department of Defense did not approve or deny the request within the 20 days required by FOIA, Rosenberg filed a lawsuit in the United States District Court for the District of Columbia against the Department seeking the records. After U.S. District Judge Gladys Kessler set a July 8, 2013 deadline for the government to review its FOIA decision, the Department released the list to the *Herald* on June 17, 2013.

The list may shed some light on the Obama Administration's failure to close the Guantanamo detention facility despite repeated promises in the first years of Obama's presidency to do so. In 2010, Congress effectively barred the administration from transferring Guantanamo detainees to facilities within the United States, even for criminal prosecution. In addition, the *Miami Herald* reported that Army Brig. Gen. Mark Martins, the Pentagon's chief war crimes prosecutor, said the military has been restricted from pursuing war crimes prosecutions against many detainees. Thus, according to Human Rights Watch senior counterterrorism counsel Andrea Prasow in an interview with the *Herald*, "Many of the detainees designated for prosecution can only be prosecuted in civilian court. So unless Congress lifts the restrictions banning their transfer they are effectively 'indefinite detainees.'"

Human rights groups have described the release as a positive development that sheds light on an unacceptable practice. Amnesty International's Zeke Johnson told the *Herald* that "[u]nder international human rights law, all of the detainees should either be charged and fairly tried in federal court, or released." Dixon Osburn, director of the Law and Security Program at Human Rights First, said in a June 17, 2013 statement, "It is fundamental to democracy that the public know the identities of the people our nation is depriving of liberty and why they are being detained." He added that the "[r]evelation is welcome, though long overdue."

> "The more we understand about our ugliness, the better chance we have to overcome that ugliness. Suppression of horrific content, as this bill dictates, invites history to repeat itself."
>
> **— Ed Meyer**
> **Conn. State Senator,**
> **(D - Guilford)**

Rosenberg was assisted in her FOIA proceedings by Yale University's Media Freedom and Information Access Clinic (MFIA). In an interview with the Reporters Committee for Freedom of the Press (RCFP), the Yale law students credited Rosenberg with crafting a reasonable and narrow FOIA request that led to the list's release. "Sometimes FOIA can turn into a fishing expedition where you're trying to loop in as much as you can because you don't really know what you're going to get," law student and MFIA member John Langford told the RCFP. "This was not that case. [Rosenberg] came in, said she wanted 48 names and that was very, very useful. It focused the whole process and got things moving quickly."

Connecticut Restricts Freedom of Information Law in Response to Gun Violence

Since the December 2012 massacre at Sandy Hook Elementary School in Newtown, Conn., many states have confronted the issue of what information relating to guns and violent crime should be made public. In response to political advocates who urged the families of Sandy Hook victims to use images of their relatives to sway the gun control debate, several affected families posted an online petition, which garnered over 100,000 signatures, to give victims' families control over the release of crime scene photos. The Connecticut legislature responded by swiftly passing Public Act No. 13-311: An Act Limiting the Disclosure of Certain Records of Law Enforcement Agencies and Establishing a Task Force Concerning Victim Privacy Under the Freedom of Information Act, which was signed into law by Gov. Daniel Malloy on June 5, 2013.

The law exempts from the state's Freedom of Information (FOI) law, Conn. Gen. Stat. § 1-200 *et seq.*, any "photograph, film, video or digital or other visual image depicting the victim of a homicide, to the extent that such record could reasonably be expected to constitute an unwarranted invasion of the personal privacy of the victim or the victim's surviving family members." It also allows police to restrict release of 911 calls by victims, and establishes a task force designed to monitor the balance of victims' rights and freedom of information. The bill was initially designed to protect only the Sandy Hook victims, but was broadened to include all homicide victims. (For more on the rights of deceased victims and their families with regards to freedom of information requests, see "Citing Family Members' Privacy, Supreme Court Allows Government to Withhold Foster Photos" in the Spring 2004 issue of the Silha *Bulletin*.)

The law passed the Connecticut legislature with broad bipartisan support. According to a spokesman for John McKinney (R-Fairfield), the state senator who represents Newtown, the state's Freedom of Information Commission will now have to weigh victims' rights when deciding whether to publicly disclose images. "The families have shown tremendous courage in coming to the Capitol and publicly asking the legislature to protect their privacy rights with respect to the graphic evidence and crime scene photographs of their murdered children and loved ones," McKinney told CNN on June 5, 2013.

However, the bill has been criticized by freedom of information advocates. State senator Ed Meyer (D-Guilford), one of only two senators to vote against the bill, disputed that suppressing such information was the best way to deal with tragedy. "The

FOIA, *continued on page 14*

FOIA, *continued from page 13*

more we understand about our ugliness, the better chance we have to overcome that ugliness. Suppression of horrific conduct, as this bill dictates, invites history to repeat itself," Meyer said in a statement on June 5, 2013.

The RCFP reported on June 7, 2013 that Connecticut Freedom of Information Commission head Colleen Murphy believes the law changed the burdens of FOI requests. "Essentially, the law shifts the burden of proof away from government agencies by requiring requesters of information to establish that disclosure is warranted," Murphy said. Instead, Murphy believes the law leaves unanswered questions as to "how much leeway … public officials have if they're getting requests for a certain record, and whose privacy [they are] looking at to see if it's invaded."

Louisiana Law Restricts Press Rights Regarding Gun Permit Holders

In Louisiana, proponents of Second Amendment gun rights have passed a law that many argue violates First Amendment speech rights. On June 19, 2013, Gov. Bobby Jindal signed HB 8 and HB 98 into law, criminalizing any publication of a gun permit holder's identity or personal information. Enacted together, the laws make it "unlawful for any person to intentionally release, disseminate, or make public in any manner any information contained in an application for a concealed handgun permit or any information regarding the identity of any person who applied for or received a concealed handgun permit." Violators face up six months in jail and $10,000 fine. The law contains some exceptions, such as when a gun owner is charged with a crime or consents to the disclosure.

The bills' sponsor, state representative Jeff Thompson (R-Bossier Parrish) proposed the bill in response to the actions of *The Journal News*, a New York newspaper that, in December 2012, published a map of the publicly available names and addresses of gun permit holders in New York's Westchester, Rockland, and Putnam counties. (For more information about *The Journal News* story, see "Media Organizations' Use of Public Data Draw Privacy Concerns from Courts, Legislatures" in the Winter/Spring 2013 issue of the Silha *Bulletin*.) Although all gun permit information is already secret in Louisiana, Thompson believed that criminal penalties were needed to ensure privacy. "Responsible, law-abiding citizens should not be villainized [sic] simply because they are concealed carry permit holders," Thompson told the New Orleans *Times-Picayune* on June 19, 2013.

Gun advocates applauded the law as a reasonable protection for gun owners' privacy. According to a June 21, 2013 blog post by Heather Ginsberg of Townhall.com, "Louisiana is now a state that protects the second amendment and the privacy of its gun owners." State senator Jonathan "J.P." Perry (R-Kaplan) acknowledged the law's potential conflict with the First Amendment, saying during a state senate judiciary committee hearing on the bills on May 7, 2013, "[I]n very recent history, the way that this country has gone, I'll tell you right now, I'll protect my Second Amendment before I protect my First Amendment. And I think that's where a lot of the difference is going to start going."

> "In very recent history, the way that this country has gone, I'll tell you right now, I'll protect my Second Amendment before I protect my First Amendment. And I think that's where a lot of the difference is going to start going."
>
> **— Jonathan Perry**
> **La. State Senator,**
> **(R - Kaplan)**

Media advocates have been highly critical of the law. Louisiana media lawyer Loretta Mince argued that the law is overly broad, and would restrict legitimate journalism. "Even a reporter who wasn't trying to directly violate the statute might nonetheless find themselves in violation of the statute just pursuing their regular journalism activities," Mince told the RCFP for a June 24, 2013 story.

Many First Amendment scholars believe the law is likely to be struck down for constituting a prior restraint on speech. Such laws are presumptively unconstitutional. Mince told the RCFP on June 24, 2013 that the law will face a legal challenge, estimating that there is "zero chance that that provision could be upheld." Mince argued that "[i]f you lawfully obtain information about who has a concealed weapons permit, you get to publish it. That's what the First Amendment is about." However, Gregg Leslie, legal defense director at the RCFP, argued the constitutional challenge is more uncertain. "In some ways [the bill] works as prior restraint, but in others, if they make it a law that penalizes you for publishing [the information], you're being penalized after the fact," Leslie told *Mother Jones* on May 22, 2013. "So it's not actually keeping you from publishing it." However, even if the law is not a prior restraint, Leslie said the state "would have to show a compelling interest" to justify the gun laws' content-based restrictions on speech, a legal standard that is rarely satisfied.

Journalists in Missouri may face a similar threat of punishment for publishing stories that identify a person as a gun owner. The St. Louis *Beacon* reported on July 5, 2013 that Missouri Gov. Jay Nixon vetoed the so-called "Second Amendment Preservation Act," HB 436, which, among other things, would make publishing "the name, address, or other identifying information of any individual who owns a firearm or who is an applicant for or holder of any license, certificate, permit, or endorsement which allows such individual to own, acquire, possess, or carry a firearm" a class A misdemeanor, which carries a fine of up to $1,000. However, William H. Freivogel of *Gateway Journalism Review* reported on Sept. 6, 2013 that Republicans in the Missouri Legislature believe they have enough votes to override Gov. Nixon's veto.

Gov. Nixon argued that the bill "violated the U.S. Constitution" when he vetoed it, according to the July 5, 2013 report by the St. Louis *Beacon*. Freivogel argued in his Sept. 6, 2013 *Gateway Journalism Review* piece that the bill would make it "a crime for a news organization to publish a story stating that the governor owned a gun. It would be a crime to run a column by a state legislator proudly stating he owns a gun. It would be crime to run a photo identifying a group of young hunters at their first deer hunt." Freivogel reported that civil liberties groups are expected to challenge the law in court if the Missouri Legislature overrides Nixon's veto. The Legislature was scheduled to meet in a veto session on Sept. 11, 2013, after the *Bulletin* went to press. The *Bulletin* will continue to follow this story as it develops.

Alex Vlisides
Silha Research Assistant

England and Wales Reform Archaic Libel Laws

On April 25, 2013, the British Parliament passed the Defamation Act 2013, which the Secretary of State is expected to allow to go into force by the end of the year. The Act incorporates several key reforms into the British libel system, which has been described by many reform advocates as "archaic," and which historically had favored plaintiffs.

LIBEL REFORM

Three British interest groups devoted to expanding freedom of expression – Index on Censorship, English PEN, and Sense about Science – officially launched the Libel Reform Campaign on Dec. 9, 2009. The joint organization operated as the primary lobbying force for the new law, according to the Index on Censorship's website. Both the Conservative Party and the Liberal Democratic Party promised to reform Britain's libel law when the two parties formed a coalition government in 2010. On May 27, 2010, Liberal Democratic peer Lord Anthony Lester introduced the bill that would eventually become the 2013 Act. He was influential in steering the bill through Parliament, particularly in March 2013 when he rescued the bill from being killed after Labour peer Lord Puttnam sought to attach amendments that would have implemented reforms called for by the 2012 Leveson report. Prime Minister David Cameron had said he would have prevented a bill that included the Leveson amendments from being heard in the House of Commons. (For more on the Leveson report, see "Leveson Inquiry Report Calls for New System of Press Regulation in United Kingdom" in the Fall 2012 issue of the Silha *Bulletin*.)

The 2013 Act maintains the traditional premise of British libel law that the defendant bears the burden of proof, unlike the U.S. model where the burden is on the plaintiff to prove falsity. However, section 1 of the 2013 Act requires plaintiffs to prove that a statement caused "serious harm" to their reputation for the statement to be considered defamatory. For-profit corporations must now prove "serious financial loss" to meet the serious harm standard. According to an April 22, 2013 article in the *Guardian*, the coalition government had initially opposed this Labour-backed provision regarding corporations, but softened its position in order to ensure the bill's passage. Notably, the Act only requires for-profit companies to prove serious financial loss. In an April 23, 2013 article in the *Guardian*, members of the Libel Reform Campaign expressed their disappointment that the new law would not "bar private companies contracted to run schools, prisons or healthcare from suing ordinary citizens who criticised the work they do for the taxpayer." Jo Glanville, director of English PEN, argued in the same article that with the increase in the privatization of social services in the United Kingdom, the for-profit/non-profit distinction could have a chilling effect on criticism of non-profit companies. Conservative MP and libel lawyer Sir Edward Garnier told the online magazine *Chemistry World* on April 29, 2013 that the Act would "create additional litigation around defining serious financial loss" and that "[d]efendants who fail against big corporations will have an even bigger bill to pay." The "bigger bill" Garnier speaks of refers to the fact that under British law, the loser of a defamation suit must pay the winner's attorney's fees. Garnier, who represented Lord Alistair McAlpine in his libel case against Sally Bercow (discussed below), introduced amendments to the bill in early April 2013 that would have eliminated the serious financial harm standard if they had been passed.

The Act also strengthens the defenses of truth and opinion. Section 2 of the Act creates a defense "for the defendant to show that the imputation conveyed by the statement complained of is substantially true." Section 3 of the Act protects statements of opinion, provided that "an honest person could have held the opinion on the basis of … any fact which existed at the time the statement complained of was published." Opinions are further protected as "privileged statements" if they appear in a publication of public interest, in a peer-reviewed scientific or academic journal, or if the defendant reasonably believed that the statement was in the public interest.

Index on Censorship (IOC), an organization that promotes freedom of speech around the world, credited the 2009 case *British Chiropractic Association v. Singh*, [2009] EWHC 1101 (QB), as spurring this particular reform. In that case, the BCA sued journalist Simon Singh over an April 19, 2008 column Singh wrote for the *Guardian* in which he denounced the BCA for promoting "bogus treatments" backed by "not a jot of evidence." Justice David Eady of the High Court found in favor of BCA in May 2009, holding that Singh's comments were statements of fact that implied that the BCA was being deliberately misleading in promoting its treatments. In April 2010, an appeals court found in favor of Singh, holding that his comments were protected under the common law fair comment defense, a defense that section 3 of the 2013 Act now has abolished. *British Chiropractic Association v. Singh*, [2010] EWCA Civ. 350. Singh told the *Guardian* for an April 1, 2010 article following the appeals court ruling that it was "extraordinary that this action ha[d] cost £200,000 to establish the meaning of a few words." Singh, who called English libel law "a vulture circling the world" in a March 10, 2011 column for the *Guardian*, began campaigning for libel reform after the appeals court ruling. The IOC credited the Singh case for "galvanizing" the reform movement.

The Act also effectively ends the practice in England and Wales of so-called "libel tourism," whereby a non-British plaintiff brings a libel suit against a non-British defendant for statements that happened to be published in the United Kingdom. Section 9 of the Act stipulates that British courts do not have jurisdiction to hear a libel case unless they are satisfied that "of all the places in which the statement complained of has been published, England and Wales is clearly the most appropriate place in which to bring an action in respect of the statement."

Several cases of libel tourism involving high-profile plaintiffs made headlines in recent years. In 2003, U.S. journalist Rachel Ehrenfeld published the book *Funding Evil: How Terrorism is Financed - and How to Stop It*, alleging that Saudi Billionaire Khalid bin Mahfouz had funded the terrorist organization al-Qaeda. Excerpts of the book were published online, and 23 copies of the book were sold in Britain, allowing Mahfouz to sue Ehrenfeld for libel in London in 2004. In May 2005, Justice Eady granted judgment in default to Mahfouz and his two sons, awarding them £10,000 each. In Dec. 2004, five months before Justice Eady's ruling, Ehrenfeld counter-sued in the United States District Court for the Southern District of New York, arguing that the First Amendment protected her from the judgment. The district court and the United States Court of Appeals for the Second Circuit held that Ehrenfeld could not prevent Mahfouz from enforcing the British libel judgment against her in the United States, *Ehrenfeld v. bin Mahfouz*, 518 F.3d 102 (2nd Cir. 2008), which led Congress to pass the Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, Pub. L. No. 111-223, on Aug. 10, 2010. The law prohibits U.S. courts from recognizing foreign libel judgments that are inconsistent with the free speech protections of the First Amendment.

Libel Reform, *continued on page 16*

Northern Ireland Rejects Libel Reform

The Legislative Assembly of Northern Ireland voted not to have the Defamation Act apply to Northern Ireland, leading some to believe that libel tourism and a chilling effect on the press will survive in Belfast.

Mike Harris of the IOC told the Belfast *Telegraph* on April 26, 2013, "Our concern is that Northern Ireland will continue to have antiquated libel laws and become a libel tourism capital where cases that can't be taken in England will be taken to Belfast." Harris told the Belfast *Newsletter* on June 13, 2013 that the biggest loser from Northern Ireland's decision would be "the person in the street," who could be sued for libel for online publications. The *Guardian* reported that Lord Anthony Lester told the House of Lords on June 27, 2013, "If libel law in Northern Ireland remains unreformed, its chilling effects will interfere with the fundamental rights not only of those who seek to publish information and opinions on matters of public interest and concern, but also everyone living within Northern Ireland and the rest of the UK." Lord Guy Black told the House of Lords on June 27, 2013 that more than 6,000 jobs in publishing and broadcasting in Northern Ireland "may well be at risk if some of those companies decide that it is now too dangerous to operate in a jurisdiction that stifles freedom of expression." Viscount Charles Colville warned the House of Lords on June 27, 2013, "If journalists and authors are going to receive letters threatening defamation in [trivial] cases, imagine the fear in publishing anything more critical of politicians."

However, Belfast libel lawyer Paul Tweed told the Belfast *Telegraph* on May 11, 2013 that the more important issue was "allowing the ordinary man in the street redress if their reputation has been damaged," and called the libel reform movement "a result of pressure from the United States." Peter Weir, a Member of the Legislative Assembly (MLA) of the Democratic Unionist Party (DUP), who opposed adopting the reforms in Northern Ireland, told the Belfast *Newsletter* on June 13, 2013, "There is little or no basis in fact for the scare stories that have been peddled in the press in relation to current practice in Northern Ireland. Much of the commentary in the press has been self-serving and a way to avoid paying damages when they publish material which is untrue."

Libel Reform, *continued from page 15*

Jonathan Heawood, then-director of English PEN, told the website Journalism.co.uk on Aug. 11, 2010 that the passage of the SPEECH Act was "hugely embarrassing" for those in the United Kingdom who believed libel tourism was not a problem. However, Ashley Hurst, a partner at the London-based firm Olswang, told the *Huffington Post* on June 25, 2013 that libel tourism is an issue that news media have exaggerated. Hurst said that the 2013 Act certainly would make it more difficult for foreign nationals to sue in England or Wales, but "most cases of forum shopping are already stopped at an early stage anyway so [the Act] will not be a dramatic change in practice." (For more on libel tourism, see "Federal 'Libel Tourism' Law to Nullify Anti-Speech Rulings" in the Summer 2010 issue of the Silha *Bulletin*, and "'Libel Tourism' Suit Leads Publisher to Destroy Book on Terrorism Funding, Pay Damages and Apologize" in the Fall 2007 issue.)

The 2013 Act also addresses defamation in the age of Internet communications, specifically the liability of operators of websites for defamatory statements posted there. Section 5 stipulates that an operator of a website is not liable if he or she can prove that he or she did not generate the defamatory statements. However, if the plaintiff notified the operator of the website of the defamatory statements, asked the operator to remove the statements, and the operator failed to remove the statements, then the operator could be held liable. By contrast, section 230 of the 1996 Communications Decency Act (CDA), 47 U.S.C. § 230, protects such operators (referred to as interactive computer services in the CDA) from liability for defamatory comments made by users on their website. Andrew McDiarmid, a senior policy analyst for the Washington, D.C.-based Center for Democracy and Technology, which promotes "public policies that will keep the Internet open," praised the overall reforms of the Act but argued that protections for third-party liability do not go far enough. He argued that section 5 gave a "troubling incentive for intermediaries to disfavor anonymous or pseudonymous content. Website operators will face a choice between opting for real-name policies or risking possible liability for users' content. Legal certainty is of great value to Internet intermediaries, so absent compelling alternatives, most will choose the former."

Another section of the Act that protects online speech from libel suits is section 8, which establishes a single publication rule that requires plaintiffs to file a defamation suit within one year of the first publication. This rule "replaces the longstanding principle that each publication of defamatory material gives rise to a separate cause of action which is subject to its own limitation period," according to the explanatory notes accompanying the legislation. Plaintiffs have used the former multiple publication rule to claim a cause of action each time an article with a defamatory statement was downloaded from the Web. Subsection 5 of section 8 creates a two-part test to determine whether a republication of a defamatory statement is substantially different from the original. The court must assess "the level of prominence that a statement is given" and "the extent of the subsequent publication." The explanatory notes for the section state that a possible example of a statement that passes this test "could be where a story has first appeared relatively obscurely in a section of a website where several clicks need to be gone through to access it, but has subsequently been promoted to a position where it can be directly accessed from the home page of the site, thereby increasing considerably the number of hits it receives." In an April 28, 2013 post on the *Guardian*'s "Media Blog," English PEN's Jo Glanville hailed the end of "a 19th-century anomaly whereby each time an article was republished a new cause of action could be triggered." However, Ashley Hurst's assessment of the new rule was more tempered when he told the *Huffington Post* for its June 25, 2013 article that the single publication rule's "main impact will be to give publishers who run archives a bit of comfort that they're not going to be sued over material from several years ago."

Reactions to the passage of the Defamation Act 2013 were mixed. Kate Briscoe, founder of the consumer watchdog website Legal Beagles, told the Libel Reform Campaign website that she "was finally able to feel safe and positive about the responsibility of [criticizing] major companies for poor treatment of consumers," and that the 2013 Act gave her staff the ability "to write without 'looking over our shoulder' in fear of the next threat." However, proponents of the law also expressed concern that more reforms were still needed. Sense about Science, in a statement released on June 12, 2013, argued that "work still needs to be done. We still need to see new effective regulations for websites passed by Parliament, civil procedure rules to help early strike out of trivial claims quickly and cheaply, and costs protection rules to ensure fairness and access to justice." Kirsty Hughes, chief executive of IOC, called on the government "to publish its proposals to stop people suing online intermediaries for content they didn't publish, cut the dispro-

portionate costs of libel actions and rules to strike out bullying cases early on" on the Libel Reform Campaign website. Peter Wilmshurst, a cardiologist who had faced four libel suits from NMT Medical, a now-defunct U.S. company that manufactured heart devices, echoed Hughes during a presentation at a June 12, 2013 meeting of the Libel Reform Campaign, saying, "Only when the costs of defamation actions are brought down … will the law be just."

Lord McAlpine Wins Twitter Libel Case Against Sally Bercow

Two high-profile libel cases decided soon after the Defamation Act 2013 was passed have offered clues as to what kinds of libel cases could still be heard once the new law goes into effect. On May 24, 2013, former Conservative MP Lord Alistair McAlpine won a £100,000 judgment from Sally Bercow, wife of House of Commons Speaker John Bercow, after High Court Justice Michael Tugendhat found that Bercow defamed McAlpine in a tweet she wrote that implied McAlpine had molested young boys. On Nov. 4, 2012, Bercow tweeted, "Why is Lord McAlpine trending? *innocent face*," after the BBC 2 program "Newsnight" aired a story alleging that an unnamed former high-profile politician had sexually abused boys at a care home in the town of Wrexham in the 1970s and 80s. McAlpine had been the target of similar allegations in the mid-1990s, yet an official inquiry by Lord Ronald Waterhouse in 1997 exonerated him. In a Nov. 10, 2012 column in the *Observer*, David Leigh, executive editor for investigations at the *Guardian*, accused the BBC of improvidently "reheating" what had been a settled story without checking its facts. The "Newsnight" allegation was ruled to be libelous for insinuating that McAlpine was the unnamed politician in question, and the BBC paid McAlpine £185,000 in damages.

In his judgment against Bercow, Justice Tugendhat, Britain's most senior libel judge, wrote, "I find that the tweet meant, in its natural and ordinary defamatory meaning, that the claimant was a paedophile who was guilty of sexually abusing boys living in care. If I were wrong about that, I would find that the tweet bore an innuendo meaning to the same effect." Tugendhat said that there was no sensible reason behind Bercow's use of the words "*innocent face*" in her tweet. He said the words would have been interpreted as "insincere and ironical" by Bercow's Twitter followers, making the tweet the "last piece in the jigsaw" that would allow her followers to wrongly link McAlpine with the abuse allegations. *McAlpine v. Bercow*, [2013] EWHC 1342 (QB). Bercow had initially defended her tweet as "conversational and mischievous," according to the *Guardian*. Bercow's lawyer, William McCormick QC of the London-based firm Ely Place Chambers, had argued in court that Twitter was a medium through which people simply write "random thoughts without necessarily meaning anything," according to the *Guardian*. "It's the sort of random thought if one was sitting in one's room with one's family, you might just come out with." After the judgment came down against her, Bercow said that the "ruling should be seen as a warning to all social media users."

Reactions to McAlpine's victory and its implications for free speech on Twitter in the UK were mixed. Columnist Patrick Strudwick wrote a May 24, 2013 column for the *Guardian* criticizing the judgment, which, he argued, meant that "Twitter's cheeky impulsiveness must be replaced with caution. Told off, it will become a no-smoking pub, a meat-free sausage, a city without any sex." However, Barbara Ellen, a columnist for the *Observer*, wrote on May 25, 2013 that Twitter is no more than "an interesting communication tool that, for too many, swiftly turned into a licence to browbeat, bully or bore[.] People fight for the right to free speech, sometimes they die for it. How anyone could have the gall to equate this with someone tapping out sarky remarks of 140 characters or less is beyond me." Joshua Rozenberg, the BBC's former legal correspondent, wrote in a May 24, 2013 column for the *Guardian*, "One hopes Twitter users are beginning to learn what a powerful and potentially dangerous weapon they have at their fingertips. A tweet is more like a broadcast than an email and is subject to the law of libel in the same way." Roy Greenslade, professor of journalism at London's City University, wrote on his "Greenslade Blog" published on the *Guardian's* website that Bercow's tweet should be treated no differently than the BBC's allegation against McAlpine. Greenslade argued that the "ruling may give heart to people who feel that tweeters who mention them are not observing the law as strictly as mainstream media." Gerard Cukier of the London-based law firm Kingsley Napley LLP told the *Guardian* on May 24, 2013 that the outcome of the case did not affect the principles of free speech in any way. "Anyone is entitled to comment freely on any matter of public interest as long as the comments can be recognized as comments — as opposed to statements of facts or imputations such as the judge held Bercow's comments to be — and as long as the comments are based on facts which are true," Cukier said.

***British Psychic Wins Libel Settlement from* Daily Mail**

On June 20, 2013, Sally Morgan, who performs on TV and on stage as "Psychic Sally," won a £125,000 settlement from the London *Daily Mail* after the newspaper admitted to falsely reporting that Morgan used an earpiece to receive messages from aides in order to scam an audience in Dublin, Ireland in September 2011. Magician Paul Zenon made the allegation in a Sept. 22, 2011 opinion article, which has since been removed from the *Daily Mail's* website. According to a June 20, 2013 article in the *Guardian*, the allegation stemmed from comments made by callers to an Irish radio program, who said they "thought they had heard two crew members saying something which Morgan then repeated on stage" while attending the Dublin show. The two crew members were later found to be under contract with the Dublin theater and not Morgan. Morgan sued Associated Newspapers, the publisher of the *Daily Mail*, for £150,000 in January 2012, claiming the article "caused substantial damage to her reputation, as well as hurt, distress and embarrassment," according to a Jan. 26, 2012 *Press Gazette* article.

Many in the United Kingdom reacted with incredulity that a psychic could win a libel settlement. Richard Dawkins, an English ethologist and evolutionary biologist, tweeted following the settlement, "England, libel capital of the world. Psychics — and charlatans of all kinds — rich pickings to be had in the English law courts." David Banks, a journalist and media law consultant, wrote in a June 21, 2013 column for the *Guardian* that people can freely express their opinions about psychics and their abilities, but the *Daily Mail* column went too far because it made a specific allegation that Morgan acted out of improper motives. "[I]f you go further than talking about your own opinion and state or imply that the psychic concerned knows that she has no such powers and is therefore deceiving and defrauding her audience, then you have gone too far," Banks wrote. Banks added that he would have rather seen Morgan's abilities scientifically tested than see the dispute resolved in a libel court. Science journalist Martin Robbins wrote in the British public affairs magazine *New Statesman* on June 21, 2013 that Morgan's victory was the result of shoddy journalism. "In a supreme fit of irony, rationalists accused [Morgan] of fraud without bothering to collect the evidence they needed to substantiate the claim," he wrote. "She sued, she won, and she deserved to win."

Brett Johnson
Silha *Bulletin* Editor

College Athletes Mount Challenges Seeking Control of Likenesses

Ryan Hart played quarterback for the Rutgers University football team from 2002 to 2005, setting school records during his college career. Hart is now a financial representative at New York City-based Acorn Financial Services, but an animated Ryan Hart continues to play quarterback for Rutgers. Electronic Arts (EA), a highly successful video game producer, used Hart's likeness in its popular football video game, NCAA Football 06. In NCAA Football 06, which has sold over 1,840,000 copies, the quarterback for Rutgers resembles Hart and reflects his height, weight, playing number, physical abilities and biographical information, including his home town and class year. The game features annually updated rosters for over 100 college football teams. The rosters are filled with virtual players who, although nameless, have similar physical and biographical traits as the real-life college athletes they are meant to represent.

RIGHT OF PUBLICITY

In October 2009, Hart filed a complaint in New Jersey state court, arguing that EA's use of his likeness without permission violated his right of publicity under the New Jersey common law. The right of publicity doctrine is based in the idea that an individual has a limited property right in his or her likeness. EA removed the case to federal court, where the U.S. District Court for the District of New Jersey granted EA summary judgment on the theory that NCAA Football was protected against right of publicity claims by the First Amendment. *Hart v. Elec. Arts, Inc.*, 808 F.Supp.2d 757, 764 (D.N.J. 2011).

Hart is not the first former NCAA athlete to file suit over their right of publicity. Sam Keller, a former Nebraska University football player, filed a similar suit in the United States District Court for the Northern District of California, alleging violations of his right to publicity and seeking to represent a class of similarly situated former NCAA athletes. In *In re Student-Athlete Name & Likeness Litig.*, MDL 2212, 2011 WL 346950 (Feb. 4, 2011), Keller and other former student-athletes sought to combine their claims with Hart's into a multidistrict litigation action which could adjudicate some of their claims against EA in front of one judge. However, Hart opposed the consolidation and pursued his claim separately, while Keller's suit was combined with another putative class action led by former UCLA basketball star Ed O'Bannon. The consolidated suit is pursuing two main claims: violations of athletes' right of publicity by EA, the NCAA and the Collegiate Licensing Company (CLC), an independent licensing organization of NCAA member schools; and federal antitrust allegations against the NCAA for its requirement that all college athletes release some of their identity rights in perpetuity.

On May 21, 2013, a divided panel of the U.S. Court of Appeals for the Third Circuit overturned the district court decision and held that Hart's right of publicity prevents EA from using his likeness without permission. *Hart v. Elec. Arts, Inc.*, WL 2161317 (2013). The opinion attempted to strike a balance between an individual's right to control commercial use of his or her likeness and First Amendment protection for content producers.

EA conceded for the purpose of the appeal that they had used Hart's likeness, but maintained that its use is protected expression under the First Amendment. In *Brown v. Entm't Merchs. Ass'n*, 131 S.Ct. 2729 (2010), the U.S. Supreme Court found that video games enjoy the full First Amendment protection given to more conventional expressive works such as books or films. (For more on *Brown v. Entm't Merchs. Ass'n*, see "U.S. Supreme Court Strikes Down Ban on Violent Video Game Sales to Minors" in the Summer 2011 issue of the Silha *Bulletin*.) Although an individual's right of publicity is limited by a speaker's First Amendment rights, different federal courts have applied different tests when attempting to balance these competing interests. Some courts have applied the so-called predominate use test, from *Doe v. TCI Cablevision*, 110 S.W.3d 363 (Mo. 2003), which asks whether use of a likeness is predominately for commercial or expressive purpose. Other courts have applied the *Rogers* test, from *Rogers v. Grimaldi*, 875 F.2d 994 (2nd Cir. 1989), which allows for unconsented use of a person's likeness, except where an advertiser uses a likeness to promote a product unrelated to that person.

Writing for the majority in *Hart*, Judge Joseph A. Greenaway analyzed the case by adopting a right of publicity test that courts have borrowed from copyright law: the transformative use test. This test, established in the case *Comedy III Prods., Inc. v. Gary Saderup, Inc.*, 25 Cal.4th 367, 106 Cal.Rptr2d 126 (Cal. 2001), asks whether the challenged work is "so transformed that it has become primarily the defendant's own expression rather than the celebrity's likeness." The Third Circuit, citing *Comedy III Prods., Inc.*, held that "the balance between the right of publicity and First Amendment interests turns on 'whether the celebrity likeness is one of the raw materials from which an original work is synthesized or whether the depiction or imitation of the celebrity is the very sum and substance of the work in question.'" The court sought to protect creative expression, while differentiating work whose value "'derives primarily from the fame of the celebrities depicted.'"

Applied to Hart's claim, the court found that EA had not sufficiently transformed Hart's likeness to overcome his right of publicity. The court emphasized that EA was animating Hart's digital likeness to do exactly what Hart did: play quarterback at Rutgers. The court held that NCAA Football 06 attempted to create a realistic depiction of college football games for users to manipulate, and it used Hart's identity as a known athlete to construct the realistic world of the game. Although the game contained creative content such as digitized game play and sounds, these did not alter Hart's likeness. Because the game did not transform Hart's identity in a meaningful way, his right of publicity overcame the First Amendment concerns at stake. The case was remanded to the U.S. District Court for the District of New Jersey in Trenton.

In his dissent, Judge Thomas Ambro agreed that the transformative test should be applied, but he argued that EA's expressive rights overcame Hart's right of publicity. Ambro argued that the game "'contain[s] significant expressive content other than [his] mere likeness[],'" and thus found the use of Hart's likeness transformative. According to a June 1, 2013 report by *The New York Times'* Adam Liptak, EA attorney Jake Schatz will ask the full appeals court to hear the decision *en banc* and reconsider the panel's decision.

The Third Circuit's decision has been hailed as a victory for the rights of famous individuals. Writing for *Forbes Magazine*'s "Sportsmoney" blog on May 22, 2013, Mark Edelman, associate professor of law at the Zicklin School of Business, City University of New York, praised the decision for protecting the

rights of college athletes. Edelman wrote that the decision has the potential to "partially offset a current injustice where the NCAA shamelessly licenses its intellectual property rights to video game publishers" while preventing athletes from sharing in the revenues.

The decision has been widely condemned by content producers and free speech advocates. If the Third Circuit's analysis is adopted by other federal courts, they argue, content producers may have less freedom to depict individuals without their permission. "The reach of this decision goes far beyond video games," EA Vice President and Deputy General Counsel Jake Schatz said in a statement following the Third Circuit's ruling. "If it stands, all creators of expressive works that depict real individuals, including filmmakers, biographers and journalists, would face a stark choice: liability or self-censorship." In a June 4, 2013 blog post for the free speech advocacy group Electronic Frontier Foundation (EFF), Dave Maass, EFF's Media Relations Coordinator, called the decision "a perilous precedent for all forms of media that depict real people — including unauthorized biopics (for example Oscar-winning 'The Social Network'), documentaries, and even journalism that includes representations of real people."

In a May 22, 2013 EFF blog post, EFF Intellectual Property Director Corryne McSherry also criticized the decision, arguing that a sympathetic plaintiff led the court to apply the wrong test in a right of publicity case. McSherry argued that borrowing the transformation concept from copyright law is inappropriate. Unlike in copyright cases, where each party has competing speech interests, the right of publicity is an economic right. McSherry argued that such economic rights should not be balanced equally when the countervailing interest is a speech right protected by the First Amendment. Instead, she argued, courts should analogize to trademark law and apply the *Rogers* test, holding that "where the invocation of an identity is part of the expressive purpose, the court should not punish it unless it is in essence a disguised advertisement, e.g., the user is just trying to use a person's name to call attention to a product."

The *Hart* court explicitly rejected the *Rogers* test. The court argued that tests applied in trademark cases are inappropriate in right of publicity cases because the right of publicity "protects a greater swath of property interests." The court did not believe the *Rogers* test was a sufficient safeguard, because it protects the right of publicity only "if the name or likeness is used solely to attract attention to a work that is not related to the identified person." EFF's McSherry also argued that publicity rights should not be considered property, writing that "[p]ublicity rights are, at most, a limited right to control the use of aspects of your identity for commercial purposes. … By treating publicity rights as equivalent to a real property right (in your home, for example), the court gave far too much weight to celebrities' interest in control over their image and far too little weight to free speech."

> "By treating publicity rights as equivalent to a real property right (in your home, for example), the court gave far too much weight to celebrities' interest in control over their image and far too little weight to free speech."
>
> **— Corryne McSherry**
> **Intellectual Property Director,**
> **Electronic Frontier Foundation**

Hart's case faces several remaining challenges before a potential class of players would receive compensation for use of their likenesses. Allyssa Rosenberg of ThinkProgress.com wrote on May 24, 2013 that "Hart may end up winning the debate over whether EA needs to license the images of college players it's including in its games. But precisely who EA pays that money to is a problem that we're at least a year away from solving." Rosenberg is referring to the resolution of *In re Student-Athlete Name & Likeness Litig.*, which will decide the issue of whether college athletes have rightfully assigned their likeness rights to the NCAA. The NCAA has argued that the language in the amateurism agreement that college athletes sign grants the NCAA the use of the players' likeness, including the ability to license it to EA. If this theory prevails, athletes like Hart, Keller, and O'Bannon would have no right of publicity claim against EA.

On July 31, 2013, the United States Court of Appeals for the Ninth Circuit affirmed the U.S. District Court for the Northern District of California's denial of EA's motion to dismiss that case. *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, No. 10-15387, 2013 WL 3928293 (9th Cir. July 31, 2013). The appeals court applied the same test as the *Hart* court, the transformative use test, and found that "EA's use does not qualify for First Amendment protection as a matter of law because it literally recreates Keller in the very setting in which he has achieved renown." The court did not determine that the plaintiffs' right of publicity had necessarily been violated, but rather that there was a "reasonable likelihood" they would prevail under California law and thus the case could proceed to trial. The case will be remanded to the U.S. District Court for the Northern District of California, where several key issues remain to be decided.

First, the district court will need to decide the motion for class certification, which was still pending as the *Bulletin* went to press. Class certification is crucial in the case, as individual claims may not be financially worth pursuing for plaintiffs, whereas a class action victory could lead to an award worth tens or even hundreds of millions of dollars, to be split amongst the plaintiffs. Members of a class must share certain legal and factual commonalities, which the NCAA argues do not exist here. The NCAA argues that the plaintiffs' differing levels of exposure, and thus their differing levels of alleged infringement of their right of publicity, make the class too diverse to certify. In addition, current NCAA athletes have been added as plaintiffs, another difference the defense will emphasize. The plaintiffs argue that every plaintiff shares the same claim, because each plaintiff signed the same NCAA amateurism agreement, which allegedly violated federal antitrust laws. Differing levels of exposure could be dealt with at the damages stage, plaintiffs argue, either by distributing damages equally amongst athletes or by using companies that evaluate a person's level of media exposure.

If the class is certified, the court then will need to determine at trial whether the plaintiffs' right of publicity in fact has been violated by video games like NCAA Football, college athletics telecasts, and other NCAA promotions. The plaintiffs also claim that the amateurism agreements required by the NCAA to participate in college athletics are invalid. The plaintiffs argue that the nature and scope of the contracts, requiring 17- and 18-year-olds to license their identity rights in perpetuity, make them unenforceable.

Athletes, *continued on page 20*

Athletes, *continued from page 19*

They also argue that the NCAA and CLC's monopolistic control on the market for collegiate athletic licensing violates the 1890 Sherman Act, 15 U.S.C. § 1. In their July 19, 2013 Third Amended Complaint, the plaintiffs alleged "a conspiracy by Defendant National College Athletic Association ("NCAA"), its member schools and conferences, and its vertical business partners, such as Defendants Electronic Arts, Inc. ("EA"), and the [CLC], to license and sell the names, images, and likeness of current and former student-athletes without compensation to those student-athletes, under the guise of 'amateurism.'" In a July 21, 2009 *Sports Illustrated* article, Vermont Law School professor and *Sports Illustrated* legal analyst Michael McCann summed up the plaintiffs' antitrust claims. "[S]tudent-athletes, but for their authorization of the NCAA to license their images and likenesses, would be able to negotiate their own licensing deals after leaving college," McCann wrote. "If they could do so, more licenses would be sold, which would theoretically produce a more competitive market for those licenses." Trial has been set for June 9, 2014, although the NCAA has filed a motion seeking to delay the trial date until August 2015.

On July 17, 2013, the NCAA announced that it would not renew its contract allowing EA to use its name and logo in the NCAA Football series. However, the same day, EA announced that it would continue its licensing agreements with the CLC for the rights to CLC member universities' teams and uniforms, athletic conferences and college football bowl games. In a July 19, 2013 statement to video game news website Polygon.com, a CLC representative denied that it had ever licensed athletes' likenesses and said that in the new contract, "participating collegiate institutions are not granting — and have never granted — any license or rights to utilize the name, face, image or likeness of any athlete, whether a current or former student athlete."

> "Student-athletes, but for their authorization of the NCAA to license their images and likenesses, would be able to negotiate their own licensing deals after leaving college. If they could do so, more licenses would be sold, which would theoretically produce a more competitive market for those licenses."
>
> **— Michael McCann**
> **Legal Analyst,**
> ***Sports Illustrated***

Professional Athletes' Right of Publicity

The same right of publicity analysis applied in *Hart* to unpaid college athletes could also protect plaintiffs who are professionals. In *Dryer v. Nat'l Football League*, CIV. 09-2182 PAM/AJB, 2013 WL 1408351 (D. Minn. Apr. 8, 2013), a class action suit is being brought by former National Football League (NFL) players against the league. Like the actions brought by Hart and O'Bannon, the plaintiffs seek compensation for use of their likenesses without consent. The former players claim that the NFL has continued to use their likeness without consent in promotions, advertisements and products long after their playing contracts expired. If the district court is persuaded by the analysis in *Hart*, it could lead to a similar victory based on a plaintiff's right of publicity. According to a June 4, 2013 article in *The New York Times* by sports reporter Ken Belson, the NFL has offered a $42 million settlement, which some plaintiffs believe is an insufficient offer. The settlement would also create a licensing agency for former NFL players that would represent players in future negotiations. However, the Approval of Settlement Order issued by Federal District Court Judge Paul Magnuson may indicate poor prospects for these and similar plaintiffs, such as those in *O'Bannon* who seek class action certification. Though he approved the settlement for the purported class, Judge Magnuson explained that "[t]he Court has stated on more than one occasion that the certification of a class action in this matter is highly doubtful, at best." As with other similar class action claims that pit athletes against powerful sports organizations, "absent class treatment, it is unlikely that any single Plaintiff's claim is so valuable as to warrant engaging in the protracted litigation that is likely to follow if this case is not resolved."

Alex Vlisides
Silha Research Assistant

The 28th Annual Silha Lecture
will feature

James C. Goodale,

Vice Chairman and General Counsel of *The New York Times* during the Pentagon Papers litigation

October 16, 2013
7:30 p.m. - 9:00 p.m.
Cowles Auditorium, University of Minnesota West Bank
Free and open to the public. No reservations required.

(See story on page 39 of this issue of the Silha Bulletin.)

Defamation Round-up: Recent Decisions and Pending Cases Put Defamation in Spotlight, Have Potential to Reshape Media-Friendly Laws

High-profile defamation cases, involving prominent parties or having the potential to alter media-friendly defamation law, made headlines in the summer of 2013. Issues included whether journalists in Texas had a privilege to accurately report on allegations made by a third party; whether the District of Columbia anti-SLAPP statute could be applied in federal court; and whether a moderator of defamatory comments posted on a gossip website was entitled to immunity under section 230 of the Communications Decency Act. Celebrity plaintiffs included former Minnesota governor Jesse Ventura and Mathew Knowles, father of pop star Beyoncé Knowles. Acquitted murder suspect Casey Anthony is also a defendant in a defamation case.

DEFAMATION

Texas Supreme Court Strikes Down Third-Party Doctrine

On June 28, 2013, the Texas Supreme Court held that journalists were not protected by a so-called "third-party allegation rule" established in a 1990 Texas case, which had insulated journalists from liability for defamation suits when they reported accurately on allegations made by third parties, even if the allegations turned out to be false. At issue in the 2013 case was whether an inaccurate report still could be considered substantially true and therefore protected under the third-party allegation rule. *Neely v. Wilson*, 2013 Tex. LEXIS 511, 56 Tex. Sup. J. 766, 2013 WL 3240040 (Tex. 2013).

In 2004, a Travis County district judge granted Austin, Tex. broadcaster KEYE summary judgment after Dr. Byron Neely, a neurosurgeon, sued the station for defamation following a January 2004 investigative report by KEYE reporter Nanci Wilson that revealed that Neely had prescribed himself narcotic painkillers while he was practicing. Wilson reported that the Texas Medical Board had placed Neely on three years probation in 2003 for prescribing himself the medications. In the report, Wilson interviewed Paul Jetton, a former patient of Neely who suffered a debilitating infection after Neely placed a shunt in his brain to drain fluid from a tumor. Jetton told Wilson, "[T]hey don't even let people operate machinery or drive cars when they're … taking [narcotics] and this guy's doing brain surgery on people," according to a transcript of the broadcast included in the Texas Supreme Court's opinion. The Texas Third Court of Appeals upheld the summary judgment ruling for the defendant in 2011. The appellate court relied on the Texas Supreme Court's holding in *McIlvain v. Jacobs*, 794 S.W.2d 14 (Tex. 1990), that journalists should be granted summary judgment if they report on allegations made by a third party, and the report is "substantially correct, accurate and not misleading." In *McIlvain*, Houston broadcasters had aired a story about city employees being investigated for doing private work on city time. The Texas Supreme Court held that the report was "factually consistent with [the] investigation and its findings," and therefore the broadcasters were entitled to summary judgment.

In *Neely*, a divided Texas Supreme Court reversed the appellate court ruling, holding that the gist of KEYE's broadcast — that Neely had used painkillers while operating on patients — was substantially false. Writing for the majority, Justice Eva Guzman distinguished *Neely* and *McIlvain*, holding that McIlvain entitled journalists to summary judgment against defamation actions only when they reported on allegations that a government investigation later proves to be true. The majority held that although KEYE's reports that Neely prescribed himself painkillers and that he had been under investigation and put on probation by the Texas Medical Board were true, the allegation that Neely operated under the influence of painkillers was conjecture and provably false. The majority held that Jetton's comments in his interview with Wilson implied that Neely operated on his patients while under the influence of painkillers, and therefore they were actionable. The majority also held that Neely was not a public figure, and therefore only had to prove that KEYE made its report with negligence and not with the higher standard of actual malice: the knowledge that the report was false, or the reckless disregard for its truth or falsity. The majority said that KEYE still could prevail at trial with a substantial truth defense, even though it could not do so at the summary judgment level.

Writing a dissenting opinion joined by two other Justices, Chief Justice Wallace Jefferson argued that the majority's interpretation of *McIlvain* was "restricted." Jefferson wrote that "[t]he 'gist' that bothers the Court is actually an inference reasonably drawn from uncontested facts. The broadcast neither presents an inaccurate gist nor distorts the substantial truth." Jefferson argued that the majority's holding chills investigative reporting on matters of public concern, and therefore it "collides violently with the First Amendment."

Free press advocates agree with the dissenters that the *Neely* decision will place a chilling effect on reporting on allegations involving matters of public concern in Texas. Following oral arguments in *Neely*, Tom Leatherbury, a media lawyer with the Dallas-based firm Vinson and Elkins LLP, told the RCFP for the Winter 2012 issue of *The News Media and the Law* that *McIlvain* had "'recognize[d] the practical reality of reporting' that the press must be able to report allegations as allegations … without assuming responsibility for the truth or falsity of the allegations themselves."

D.C. Circuit Holds that D.C. Anti-SLAPP Law Does Not Apply in* Sherrod *Case

The United States Court of Appeals for the D.C. Circuit held on June 25, 2013 that a District of Columbia anti-SLAPP (strategic lawsuit against public participation) statute (D.C. Code § 16-5501) could not be invoked to prevent a former U.S. Dept. of Agriculture (USDA) official from suing a blogger and colleagues for defamation because the defendants filed their motion outside the statute's 45-day window. *Sherrod v. Breitbart*, 2013 U.S. App. LEXIS 12959, 41 Media L. Rep. 2007, 2013 WL 3185062 (D.C. Cir. 2013).

On Feb. 11, 2011, former USDA Georgia Director of Rural Development Shirley Sherrod filed suit for defamation, false light invasion of privacy and intentional infliction of emotional distress in U.S. District Court for the District of Columbia against the conservative blogger Andrew Breitbart and Breitbart's producer, Larry O'Connor. Sherrod alleged that Breitbart, who died in March 2012, defamed her by posting a "heavily edited" video clip of a speech she gave to the Georgia NAACP in March 2010 on his blog "BigGovernment" in July 2010. Sherrod claimed that the clip portrayed her as a "racist" who "racially discriminated in carrying out her federal job," according to her complaint. The clip showed Sherrod talking about how she helped a white farmer save his farm from foreclosure in 1986. Sherrod said she "was trying to decide just how much help [she] was going to give him," and

Defamation, *continued on page 22*

Defamation, *continued from page 21*

that she "took him to one of his own" (a white lawyer) to help him. Sherrod claimed that immediately before those statements she had said, "the struggle is really about poor people," and that immediately after the statements she said that the people she worked with "could be black or they could be white," and that working with the white farmer "made [her] realize that [she] needed to work to help poor people." Sherrod accused Breitbart and O'Connor of defaming her by taking her words "out of context" to portray her as racist, whereas she was describing the experience that showed her that race did not matter to her job. The extensive media coverage of the blog post led the Obama administration to demand Sherrod's resignation, for which President Obama later apologized. (For more information on the *Sherrod* case, see "Recent Cases Put Online Defamation in the Spotlight" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

By deciding the case on procedural grounds, the appeals court did not address two key issues on which U.S. District Judge Richard Leon had ruled in July 2011. First, the appellate court did not decide whether the D.C. statute could apply to federal cases. Leon concluded in 2011 that the statute was not applicable in federal court. Several media organizations, including NBC Universal, NPR, and the RCFP, had filed an *amicus curiae* brief urging the D.C. Circuit to apply the law to federal cases. However, on the same day that the Sherrod case was decided, U.S. District Judge Reggie Walton ruled that the D.C. anti-SLAPP statute did apply in federal court. In *Boley v. Atlantic Monthly*, 2013 U.S. Dist. LEXIS 88494, 2013 WL 3185154 (D.D.C. June 25, 2013), Walton granted an anti-SLAPP motion by the Atlantic Monthly Group, Inc. after a former public official from the Republic of Liberia sued the *Atlantic* for defamation after one of the magazine's articles described the official as a "warlord." Judge Walton's ruling may factor into another pending case before the D.C. Circuit in which the applicability of the anti-SLAPP statute in federal court will also be at issue. That case, *Farah v. Esquire*, 863 F.Supp. 2d 29 (D.D.C. 2012), involved an online publisher, Joseph Farah, who sued *Esquire* for defamation over one of the magazine's blog posts that referenced Farah's challenge that Barack Obama was not eligible to serve as president. U.S. District Judge Rosemary Collyer granted *Esquire*'s anti-SLAPP motion in June 4, 2012. Arguments before the D.C. Circuit had not been scheduled as the Bulletin went to press.

Second, the D.C. Circuit did not rule on whether the defendants could immediately appeal a denial of an anti-SLAPP motion. Zoe Tillman of the "Blog of Legal Times" posted on June 25, 2013 that some courts have allowed immediate appeals of a denial of an anti-SLAPP motion even though appellate courts typically avoid hearing an appeal until after a case is decided. For example, Nevada governor Brian Sandoval recently signed into law an anti-SLAPP bill that would allow for immediate appeal of a denial of an anti-SLAPP motion, according to the Digital Media Law Project (DMLP) blog.

"Pink Slime" Case to Be Heard in South Dakota State Court

A federal judge ruled on June 12, 2013 that a $1.2 billion defamation lawsuit by Beef Products Inc. (BPI) against ABC News should be heard in state court in South Dakota, where BPI's main plant is located. The move to state court is significant because South Dakota has an agriculture disparagement law, which states that "[a]ny person who disparages a perishable agricultural food product with intent to harm the producer is liable to the producer for treble the damages so caused." SDCL § 20-10A. The $1.2 billion in potential damages reflects the tripling of damages sought by BPI: $400 million. *Beef Prods. v. ABC*, 2013 U.S. Dist. LEXIS 82635, 2013 WL 2627133 (D.S.D. June 12, 2013).

BPI sued ABC News for defamation following a series of broadcast and online stories in March 2012 on BPI's Lean Finely Textured Beef (LFTB) product, which ABC News referred to as "pink slime." LFTB is "a low-fat product made from chunks of beef, including trimmings, and exposed to tiny bursts of ammonium hydroxide to kill E. coli and other dangerous contaminants," and is used in processed foods in fast food restaurants and school cafeterias, according to a March 5, 2013 article by MSN News. ABC News first reported on March 7, 2012 on the presence of LFTB in ground beef, stating that the product was found "in nearly 70% of ground beef found at the supermarket." The report interviewed former BPI "number-2" employee Kit Foshee, who compared the product to "Play-dough" and "gelatin," and said the product was not "any good for you."

In its complaint, BPI claimed that ABC News' report caused its business to suffer, leading the company to lay off more than 700 employees and lose "more than $20 million in revenue every month" following the report. BPI alleged that ABC disparaged LFTB by reporting that it was not nutritious, that it was "filler," that it constituted "food fraud," that it was low quality, and that it was once used to make dog food. BPI also claimed that ABC reporter Jim Avila defamed the company in some of his tweets about the story. The complaint pointed to a March 7, 2012 tweet in which Avila said "[pink slime]'s just not what it purports to be. Meat." In its motion to dismiss the case, ABC News contended that it never reported LFTB to be unsafe. This contention is important because South Dakota's agriculture disparagement law defines disparagement as a false statement or implication "that an agricultural food product is not safe for consumption by the public or that generally accepted agricultural and management practices make agricultural food products unsafe for consumption by the public."

The definition of the word "slime" may prove integral to the outcome of the case. BPI alleged in its complaint that ABC News used the term "pink slime" 137 times in its broadcasts, online stories, and social media postings, and that the repeated use of the term conveyed the impression that LFTB "was an unsafe and unhealthy substance added to ground beef." In its complaint, BPI cited the Oxford Dictionary definition of slime ("a moist, soft, and slippery substance, typically regarded as repulsive"), and the American Heritage Dictionary definition of the term ("a vile or disgusting matter"). In its motion to dismiss, ABC cited another, more neutral, American Heritage Dictionary definition of slime: "a thick, sticky, slippery substance." ABC contended in its motion to dismiss that its use of the term was "rhetorical hyperbole" and "imaginative expression," and because it was not a provably false statement of fact, it was not actionable. ABC News did not create the term, but rather used it to refer to the product after U.S. Department of Agriculture microbiologist Gerald Zirnstein used the term in a 2002 email to a colleague. The term resurfaced in December 2009, when *The New York Times* ran a story about BPI and quoted from Zirnstein's email. BPI's lawsuit names Zirnstein as a defendant.

ABC News had tried to get the case removed to federal court in order to avoid the South Dakota agriculture disparagement law and to have the case heard before a jury that might be more sympathetic to a media defendant, according to multiple news reports. ABC News had argued that diversity of citizenship required that the case be heard in federal court. However, U.S. District Judge Karen Schreier ordered that the case be heard in South Dakota state court because there was no diversity of citizenship in the case. Although BPI is incorporated in Nebraska, its sister company BPI Technology Inc. is incorporated in Delaware, where ABC also is incorporated. Schreier ruled that BPI Technology was in fact a "real party in interest" in the case, thereby denying federal jurisdiction and allowing BPI to bring its action in state court.

Many First Amendment advocates have argued that ABC News is likely to prevail if the case goes to trial. South Dakota University law professor Patrick Garry told the *Wall Street Journal* on Sept. 13, 2012 that BPI would have difficulty winning the case because "[t]here is no precedent of successful lawsuits based on the agriculture-libel statute" in the state, and because BPI would have to prove that ABC News knowingly made false reports about LFTB. Curtis Brainard of the *Columbia Journalism Review* wrote on Oct. 3, 2012 that ABC's emphasis on the "ick factor" in its story might not have been ethical, but BPI's lawsuit seemed "like another SLAPP suit designed to prevent journalists and the public from asking important questions."

On July 9, 2013, ABC News filed a three-page motion to dismiss the case in Union County (S.D.) Circuit Court, arguing that BPI had failed to state a claim. On Aug. 9, 2013, BPI filed a motion opposing ABC News' motion to dismiss, arguing that ABC News and its reporters "knew their statements and implications were false." Oral arguments on the motion to dismiss had not been scheduled as the *Bulletin* went to press.

Ex-Cincinnati Bengals Cheerleader Wins Internet Defamation Case; Website Will Appeal

On July 12, 2013, a federal jury in Covington, Ky. awarded Sarah Jones, a former cheerleader for the Cincinnati Bengals of the National Football League, $338,000 in damages for defamatory comments made about Jones on the gossip website TheDirty.com in 2009. The owner of the website, Hooman Karamian (who goes by the online alias "Nik Richie"), said he will appeal the verdict. *Jones v. Dirty World Entm't Reco.*, No. 2:09cv219 (E.D. Ky. July 12, 2013).

In December 2009, anonymous comments posted comments about Jones on TheDirty.com, saying that Jones had had sex with every Bengals player and that she probably had chlamydia and gonorrhea. According to a Dec. 9, 2009 article by the AP, TheDirty.com solicits "dirt" on celebrities from users, which the site calls its "Dirty Army." The posts did not appear to have been provoked by any news made by Jones. A disclaimer at the bottom of each page of TheDirty.com reads, "The content that is published [here] contains rumors, speculation, assumptions, opinions, and factual information. Postings may contain erroneous or inaccurate information. All images are credited to their original location. The owner of this site does not ensure the accuracy of any content presented on TheDirty.com." The original posts about Jones have since been removed from TheDirty.com, but newer posts about Jones are still up on the website. Jones, also a former teacher at Dixie Heights High School in Fort Mitchell, Ky., sued Richie for defamation in December 2009, and a trial in January 2013 ended with a hung jury.

In the latest trial, U.S. District Judge William Bertelsman instructed the jury that TheDirty.com was not protected by section 230 of the Communications Decency Act (CDA), 47 U.S.C. § 230. The CDA distinguishes between an "information content provider" and an "interactive computer service" in the realm of Internet communications. The former is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." The CDA further defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." Section 230 protects interactive computer services from liability for defamatory content posted on their servers by other information content providers.

The *Cincinnati Enquirer* reported on July 12, 2013 that Bertelsman had told the jury to consider Richie an information content provider and not an interactive computer service because Richie encouraged readers to submit "dirt" on celebrities involved in scandals. Bertelsman also had ruled in January 2012 that Richie was an information content provider because he acted as editor of the anonymous comments that the website received and published them without checking their accuracy, likening him to the moderators of the website Roommates.com. The U.S. Court of Appeals for the Ninth Circuit held the moderators were not immune under the CDA from violating the 1968 Fair Housing Act, 42 U.S.C. § 3601, because they encouraged users to discriminate against potential roommates based on race, gender, or other characteristics. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*). (For more information about the *Roommates.com* case, see "Federal Court Decisions Add Uncertainty to Internet Law" in the Spring 2008 issue of the Silha *Bulletin*.) Bertelsman also held that the fact that Richie added his own comments to those submitted by anonymous users made him an information content provider. Bertelsman wrote that the comment Richie made about Jones after the 2009 posts ("Why are all high school teachers freaks in the sack?") could be interpreted by a jury "as adopting the preceding allegedly defamatory comments concerning her alleged sexual activities."

On Aug. 12, 2013, Bertelsman upheld the jury's verdict in a 12-page ruling. "[A] website owner who intentionally encourages illegal or actionable third-party postings to which he adds his own comments ratifying or adopting the posts becomes a 'creator' or 'develop[er]' of that content and is not entitled to immunity," Bertelsman wrote. Richie criticized Bertelsman in an Aug. 12, 2013 email to the AP following the ruling. "The judge didn't even know what Facebook was," Richie said. "It's sad that a United States federal judge completely ignored the law just because he didn't like it. That's Kentucky for you."

First Amendment advocates have argued that the verdict is inconsistent with the provisions of section 230 of the CDA and that it will be short-lived. David Gingras, Richie's attorney, called the verdict "a judicial muzzle on free speech." Eric Goldman, professor of law at Santa Clara University, told the *Cincinnati Enquirer* on July 12, 2013 that "holding Nik Richie accountable for his users' comments unambiguously violates federal law. The judge made a clearly wrong ruling on that point earlier in the case, and that mistaken ruling provides an important ground for appeal." Jack Greiner, an attorney specializing in media law for the Cincinnati-based firm Graydon Head, told the AP on July 12, 2013 that the verdict "could put some limits on the ability of a website operator to feel free to post comments that might be offensive or controversial or even just critical. People might err on the side of caution and not take a risk, even if comments are acceptable." Greiner wrote on his firm's blog on July 12, 2013, "By the CDA's express terms, the question about who created the content focuses on the particular content at issue — in this case, the third party posts. And so the only question should be whether [Richie] had anything to do with the creation (not the posting) of that specific comment. Given that the poster was anonymous, [TheDirty.com] had nothing to do with creating that specific post."

However, Jeffrey Layne Blevins, a professor of media law and ethics at the University of Cincinnati, argued in an Aug. 3, 2013 op-ed in the *Cincinnati Enquirer* that Richie "was acting more like an editor, if not the speaker [him]self for some of the defamatory comments," and therefore was not entitled to section 230 immunity. Blevins said he hoped the *Jones* case would set a precedent on when operators of interactive computer services cross the line and act as editors. "For too long the anonymity afforded to third-party posters and the broad immunity provided to online operators has fed an untruthful and irresponsible environment for online dialogue," Blevins wrote.

Defamation, *continued on page 24*

Defamation, *continued from page 23*
"Let's hope that the recent court decision will improve the quality of online speech by encouraging all of us to construct our comments with more care for the truth, and take responsibility for what we say."

Jones made headlines in October 2012 when she was convicted of having sex with a 17-year-old male student, Cody York. Although not sentenced to prison, she was ordered never to teach again. Jones and York became engaged in June 2013, according to the *Cincinnati Enquirer*. Jones' lawyer, Eric Deters of a self-titled firm, asked the jury to disassociate the 2009 comments from the 2012 scandal involving his client. Professor Goldman told the *Cincinnati Enquirer* on July 12, 2013, "It's amazing the jury was able to overlook that key fact [that Jones was convicted of having sex with a minor] and believed her reputation could be damaged by obviously nonsense online posts to the tune of hundreds of thousands of dollars."

Defamation Actions Involving High-Profile Parties Make Headlines

Papers have been filed in several defamation causes of action involving high-profile plaintiffs and defendants, setting up potential trials in the near future that will put defamation law in the spotlight of entertainment media.

Jesse Ventura

On July 18, 2013, a federal judge ruled that former Minnesota governor and professional wrestler Jesse Ventura could continue his defamation action against the widow of a famed U.S. Navy SEAL sniper. Ventura sued Chris Kyle, who is believed to be the deadliest sniper in U.S. military history and who was shot dead at a Texas shooting range on Feb. 2, 2013, allegedly by a fellow former serviceman, in the U.S. District Court for the District of Minnesota in August 2012. Ventura claims that Kyle defamed him in Kyle's 2012 book *American Sniper*. Kyle wrote in the book that in 2006, he punched someone he called "Scruff Face" at a California bar after the latter made disparaging remarks about the SEALs and U.S. policy in the Middle East. In a January 2012 interview with Fox News' Bill O'Reilly, Kyle said that "Scruff Face" was Ventura. Ventura admitted he was at the bar when Kyle was there, but in his May 22, 2013 motion to substitute Kyle's widow, Taya Kyle, as defendant, Ventura claimed that Kyle's story was "a complete fabrication and is a vicious, deliberate, and calculated assault on his character, honor, and reputation." Ventura is also seeking damages for invasion of privacy and unjust enrichment. *Ventura v. Kyle*, 2012 U.S. Dist. LEXIS 179929, 2012 WL 6634779 (D. Minn. Dec. 20, 2012).

In December 2012, U.S. District Judge Richard Kyle (no relation to Chris) denied Chris Kyle's motion to dismiss those two charges, according to the St. Paul *Pioneer Press*. In his order, Judge Kyle wrote that he could not dismiss the unjust enrichment claim because "it depends on the truth or falsity of Kyle's statements, which the court cannot decide at this stage." The St. Paul *Pioneer Press* reported on July 2, 2013 that both parties failed to reach a settlement by a July 15, 2013 deadline. In his July 18, 2013 ruling, U.S. Magistrate Judge Arthur Boylan said that Taya Kyle was a "proper substitute" in the case because she had been appointed executor of her husband's estate.

On Aug. 5, 2013, Taya Kyle filed a motion in the Minnesota federal district court to have the case moved to U.S. District Court for the Northern District of Texas, in Dallas, which is 25 miles from her residence in Midlothian, Tex. In a memorandum accompanying the motion, Kyle argued that traveling to Minnesota from Texas for a trial would be burdensome for her and her two children, aged seven and eight. Kyle's attorney, Leita Walker of the Minneapolis-based firm Faegre Baker Daniels, argued that moving the trial to Texas would be less burdensome on Ventura, who spends January to May in Baja California. Judge Kyle announced he will hear oral arguments on the motion to change venue on Sept. 24, 2013. On Aug. 15, 2013, Taya Kyle filed a motion for summary judgment. Judge Kyle announced he would hear oral arguments on that motion on Jan. 30, 2014, according to the St. Paul *Pioneer Press*.

Mathew Knowles

Mathew Knowles, father of renowned singer Beyoncé Knowles, has filed a defamation action against the British tabloid *The Sun*, alleging that the tabloid falsely reported on March 24, 2013 that a decision for father and daughter to go their separate ways was "incredibly painful" for Knowles. The tabloid also reported that Knowles had "yet to meet his 14-month-old granddaughter Blue Ivy, Beyoncé's child with rapper husband Jay-Z."

In his complaint, filed in U.S. District Court in Houston, Knowles claimed that these statements were false and that *The Sun* knew this when they were published. Knowles' complaint cited footage from an HBO documentary on Beyoncé ("Life is But a Dream") showing Knowles holding Blue Ivy as evidence of the falsity of the claim that he had not yet meet his granddaughter. Knowles also claimed in the complaint that he emailed the story's reporter, Georgina Dickinson, after the story ran to confront her about the alleged falsity. Dickinson replied to Knowles that she could "only apologize that someone in London [changed the story], not me." According to the complaint, Dickinson also sent Knowles a copy of the original story she had written for *The Sun*, which reported that Knowles and his daughter had separated only their business ties, and that Knowles "remains close to his family and loves nothing more than being a granddad to his daughter's newborn baby girl Blue Ivy." *Knowles and Music World Entm't v. The Sun*, No. 4:2013cv01845, (S.D. Tex. June 25, 2013).

Casey Anthony

A Florida bankruptcy judge ruled on June 25, 2013 that a defamation case against Casey Anthony, who was found not guilty in July 2011 of murdering her two-year-old daughter, Caylee Anthony, would be heard in his court because Anthony, in the judge's words, is "destitute." Zenaida Gonzalez and Roy Kronk have said that the repeated use of their names in Anthony's trial associated them with the sensationalized murder trial and therefore damaged their reputation, according to multiple media reports. Gonzalez claims that her reputation was damaged because Anthony had testified that a nanny with the same name as Gonzalez was the last person to see Anthony's daughter. Kronk, who discovered Caylee Anthony's body, claims that he was defamed after Casey Anthony's attorneys suggested in court that he might have had something to do with the child's murder.

The *Huffington Post* reported on Jan. 26, 2013 that Anthony filed for bankruptcy on Jan. 25, 2013, claiming $1,000 in assets and $792,000 in liabilities stemming primarily from attorney fees, investigative and court fees. In his June 25 ruling, bankruptcy Judge K. Rodney May said there was no point in trying the defamation cases in Orange County Circuit Court because Anthony had no money to pay judgments, according to the *Orlando Sentinel*. The *Sentinel* reported that by hearing the case in bankruptcy court, Judge May can "decide if the suits are dischargeable claims, which her bankruptcy would clear out, before determining their merits."

On July 22, 2013, the *Orlando Sentinel* reported that Gonzalez and Kronk filed motions with Judge May to exempt their claims from Anthony's bankruptcy. Gonzalez v. Anthony, No. 8:13-ap-00626 (Bankr. M.D. Fla. July 22, 2013); *Kronk v. Anthony*, No. 8:13-ap-00629 (Bankr. M.D. Fla. July 22, 2013).

Brett Johnson
Silha *Bulletin* Editor

Bloomberg News Confronts User Privacy in Wake of Financial Terminal Data Scandal

On May 10, 2013, the *New York Post* revealed that Bloomberg News reporters had been accessing user data from Bloomberg LP's financial data terminals. The terminals are leased by Wall Street traders and financial institutions and provide access to Bloomberg's financial data. The *Post* reported that a Bloomberg reporter asked a "Goldman Sachs executive if a partner at the bank had recently left the firm — noting casually that he hadn't logged into his Bloomberg terminal in some time." Goldman complained to Bloomberg management, forcing Bloomberg to address a reporting tactic that its reporters had apparently been using since the 1990s, according to a May 10, 2013 report by *The Atlantic Wire*.

DATA PRIVACY

According to a May 12, 2013 article by Matt Winkler, Bloomberg News' editor-in-chief, the reporters had access to user login activities, which financial tools they were using, and help desk inquiries. He emphasized that "at no time did reporters have access to trading, portfolio, monitor, blotter or other related systems."

According to a May 10, 2013 *New York Times* article by Amy Chozick and Ben Protess, "[a] preliminary analysis at Bloomberg revealed that 'several hundred' reporters had used the technique." A May 10, 2013 article in *Business Insider* revealed Bloomberg reporters also made use of user terminal data in breaking a 2011 story about a JP Morgan trader who had destabilized markets with a massive bet on credit derivatives. In his article, Winkler explained that reporters originally had access to the data in order to gauge what stories would be relevant to users. Winkler called the continued access for reporters "inexcusable" and said that under Bloomberg's changed policies "reporters now have no greater access to information than our customers have."

The data terminals at the center of the scandal are the bedrock of Bloomberg's business, generating about $6.2 billion of the company's $7.9 billion revenue, according to Kevin Roose of *New York Magazine*. According to a May 10, 2013 article by Phillip Bump in the *Atlantic Wire*, privacy concerns could threaten this lucrative business. "If companies thought that Bloomberg was tracking their information to break stories for its news service, it would undermine confidence in the terminals as a tool even as people more broadly become wary of data-sharing," Bump wrote.

Bloomberg acted quickly to quell user privacy concerns. Bloomberg hired Samuel Palmisano, a former CEO of IBM, to conduct a review of its data security and privacy practices. It also appointed Clark Hoyt, a former public editor at *The New York Times*, to look into the relationship between Bloomberg's news and commercial operations." Hoyt's report was released on Aug. 21, 2013, and made numerous proposals to create greater separation between the commercial and reporting aspects of Bloomberg.

> "The Bloomberg terminal is more than a mere work aid — it's an entire information ecosystem, into which a generation of Wall Street traders have wrapped their habits and routines. Terminal clients who are offended at the breach of privacy can take some steps, ... but unless they're willing to radically overhaul their company's work flow at great expense and annoyance, they can't just *leave*."
>
> **— Kevin Roose**
> **Reporter,**
> ***New York Magazine***

On Aug. 20, 2013, Bloomberg released a separate but related outside review of the scope of reporters' access and Bloomberg's data compliance conducted by Promontory Financial Group and law firm Hogan Lovells. The report found reporters had access to "anonymous chat room[s] for commodities traders, and, in other cases, were made privy to discussions about how much revenue the company was earning from specific clients." The report found that top Bloomberg executives were aware of the access and decided to stop the practice in 2011, but no action was taken "due to misunderstandings about who was responsible for doing so."

Bloomberg competitors seized the opportunity to attempt to undermine Bloomberg's dominance in the lucrative financial data terminal market. "Thomson Reuters Financial and Risk business and Reuters [news] division operate completely independently with reporters having no access to nonpublic data on its customers, especially any data relating to its customers use of its products or services," said Yvonne Diaz, a Thomson Reuters spokeswoman. United Press International (UPI) indicated on May 17, 2013 that large financial institutions such as Goldman are working on replacing some features of Bloomberg terminals with other services or even designing networks within the company. "We always thought that traders couldn't live without Bloomberg, but maybe that's not true," a Goldman Sachs official said.

However, the unique structure of Bloomberg which helped give Bloomberg financial reporters access to user information may also keep users from abandoning the service. According to *New York Magazine*'s Kevin Roose, the terminals are difficult to explain: they are part financial data service, part exclusive social network. Terminal users must pay subscription fees starting at $20,000 per year and master a complicated and arguably outdated interface for access to Bloomberg's data and admission to a kind of fraternity. One portfolio manager told the *New York Magazine* in a May 13, 2013 article, "It's a yard stick in our industry. If you can't use it, you suck." In the May 13 *New York Magazine* article, Roose wrote, "The Bloomberg terminal is more than a mere work aid — it's an entire information ecosystem, into which a generation of Wall Street traders have wrapped their habits and routines. Terminal clients who are offended at the breach of privacy can take some steps — renegotiating their contracts with Bloomberg, moving certain extra-sensitive functions like IM [instant messaging] off the terminal — but unless they're willing to radically overhaul their company's work flow at great expense and annoyance, they can't just *leave*." Like users of Facebook or other social media, wrote Jeff Bercovici of Forbes.com on May 13, 2013, Wall Street

Data Privacy, *continued on page 26*

Data Privacy, *continued from page 25*

Bloomberg subscribers' privacy concerns are likely to be somewhat compromised for the utility and convenience the service provides.

Some have compared the revelations to other media privacy scandals such as the News Corp. phone hacking scandal. Political strategist Stuart Stevens wrote in a May 13, 2013 article in *The Daily Beast* that the Bloomberg scandal "looks worse, an abuse not by a handful of story-crazed reporters and editors but a corporate collusion between the news and business divisions of Bloomberg's empire." However, Stevens argued that the media downplayed the scandal, for reasons including journalists' career self-interest. In addition to rumors that Bloomberg owner Michael Bloomberg has considered acquiring *The New York Times* and the *Financial Times*, "in a world of decreasing media employment opportunities, Bloomberg's growing empire of well-paid jobs is a bright spot in a bleak horizon. … The Bloomberg who journalists criticize today may be the employer they want to interview with tomorrow."

Columbia Journalism Review staff member Ryan Chittum wrote in a May 14, 2013 article that such comparisons to the News Corp. scandal are inappropriate. Stevens' article was "over-the-top," Chittum wrote, and though the snooping was unacceptable, "it's stretching it to say what Bloomberg News was up to here was spying on the 'personal activities' of clients." Chittum called the scandal "a serious ethics problem," but pointed out that the data collection was legal and "the information Bloomberg reporters could get at was quite limited." (For more information on the News Corp. phone hacking scandal, see "Not Just a 'Rogue Reporter': 'Phone Hacking' Scandal Spreads Far and Wide" in the Summer 2011 issue of the Silha *Bulletin*.)

Guardian U.S. Finance and Economics Editor Heidi Moore wrote in a May 13, 2013 column that there is little evidence of unethical behavior by reporters, and that Bloomberg's management's decisions deserve criticism. "It's easy to see that if the information was made available to Bloomberg reporters as part of their work tools, they wouldn't question its use," Moore wrote. Moore argued that the explanation for the scandal lies in Bloomberg News' unique evolution from financial industry sales network, with a side news outlet, to a news industry force. "For a sales business, access to customer information is essential," Moore wrote. "For a news business, it looks like prying." Moore also downplayed the importance of the information gathered and disputed the snooping's role in breaking the JP Morgan story, writing that the scoop was "clearly not information that could be gathered from a terminal."

> "News organizations will need to think increasingly about how [the division between editorial and business staff] applies to other parts of the business side, not just the ad department."
>
> **— Jeff Bercovici**
> **Reporter,**
> **Forbes.com**

Some believe that rather than being a simple mistake, this type of snooping was part of the culture of Bloomberg. Bloomberg excels by promoting what it calls "transparency." Zachary M. Seward wrote in a May 12, 2013 article for the online business news source *Quartz* that this transparency promotes information flowing in only one direction: to Bloomberg. "Data comes into the company — as much as possible, from wherever possible — but it doesn't leave because, at Bloomberg, information is money," Seward wrote. Bloomberg is valuable to its clients because it can provide information no one else can. One much-cited example is the satellite that Bloomberg commissioned to take photos twice a week of the largest American oil reserve in Oklahoma and provide that information to oil speculators. The beginning of a chapter from *The Bloomberg Way*, a 2011 book written by editor-in-chief Winkler that serves as a mission statement for Bloomberg journalists, reads, "If we don't know the people on our beats, what they do, where they're doing it, when they're doing it, and how they do it, we don't know our beats." With this mission in mind, Seward wrote that the practice of reporters gathering terminal data was a natural fit "with Bloomberg's broader culture."

Although Bloomberg's unique position may allow it to survive the scandal with a mere "public scolding," wrote Forbes.com's Bercovici on May 13, 2013, other news organizations must learn how to derive value from consumer data while avoiding privacy violations. "The news business … is rapidly transitioning away from reliance on advertising toward subscriptions and other models that involve extracting value directly from consumers," Bercovici wrote. "News organizations will need to think increasingly about how the [the division between editorial and business staff] applies to other parts of the business side, not just the ad department."

Alex Vlisides
Silha Research Assistant

Director's Note

This issue of the Silha *Bulletin* features several articles on data privacy prepared by research attorney Jason Steck, J.D. (University of Minnesota Law School, class of 2012) and Silha Center Research Assistant Alex Vlisides under the supervision of Silha Professor Jane Kirtley. These articles will also appear, in a slightly different form, in "Global Privacy and Advertising Developments," a chapter in the three-volume course handbook for the Practising Law Institute's *Communications Law in the Digital Age 2013* conference. The PLI conference takes place Nov. 14-15, 2013 in New York City, where Professor Kirtley will be the principal speaker for the panel discussion on these and related topics.

The Silha Center is very grateful to Jason and Alex for sharing the product of their hard work and expertise with readers of this issue of the Silha *Bulletin*.

Jane E. Kirtley,
Silha Professor and Silha Center Director

Busy FCC Reviews Indecency Policy, Rules on Mobile Data Privacy

The Federal Communications Commission (FCC) had a busy summer in 2013. The Commission collected public comments on a potential revision of its policy on indecent speech, and issued a declaratory order requiring wireless carriers to protect customers' personal data, all while awaiting the confirmation of new chairman Tom Wheeler.

MEDIA POLICY

FCC Reviews Policy on Indecent Speech

On April 1, 2013, the FCC issued a public notice announcing it would take comments from the public regarding a potential relaxation of its policy on isolated or fleeting expletives on radio and broadcast TV, as well as incidents of brief nudity on broadcast TV. The period for initial public comments ended on June 19, 2013. The public notice asked people to comment on two potential policies. The first was a return to the more relaxed policy toward isolated expletives set forth in 1987 (*Pacifica Foundation, Inc.*, Memorandum Opinion and Order, 2 FCC Rcd 2698, 2699 (1987)), which stated, "If a complaint focuses solely on the use of expletives, we believe that … deliberate and repetitive use in a patently offensive manner is a requisite to a finding of indecency." The second was a continuation of the Bush-era policy of cracking down on isolated expletives (*Complaints Against Various Broadcast Licensees Regarding Their Airing of the "Golden Globe Awards" Program*, Memorandum Opinion and Order, 19 FCC Rcd 4975 (2004)). The notice stated that then-Chairman Julius Genachowski had instructed the FCC's Enforcement Bureau "to focus its indecency enforcement resources on egregious cases and to reduce the backlog of pending broadcast indecency complains" until an official policy was announced. This interim policy represented a continuation of recent FCC policy toward indecency. The notice stated that the Enforcement Bureau had cut its backlog of indecency complaints by more than one million (70% of pending complaints) since Sept. 2012 by closing complaints that were beyond the statute of limitations, that were too stale to pursue, that were outside FCC jurisdiction, that were based on insufficient information, or that had been foreclosed by settled precedent.

The review of the FCC's policy is the result of the U.S. Supreme Court's decision in *FCC v. Fox Television Stations*, 132 S. Ct. 2307 (2012), in which the high court held that the FCC violated the Fifth Amendment's "due process" clause by not giving broadcasters "fair notice" that they would be fined under the FCC's revised indecency policy. The high court declined to rule on the constitutionality of the FCC's indecency policy. (For more information on *FCC v. Fox* and the evolution of FCC's indecency policy, see "Supreme Court Fleeting Expletives Ruling Leaves Constitutional Questions Unanswered" in the Summer 2012 issue of the Silha *Bulletin*; "FCC Defends Regulatory Regimes in Court" in the Fall 2011 issue; "Second Circuit Strikes Down FCC's 'Fleeting Expletives' Rule as 'Arbitrary and Capricious" in the Summer 2007 issue; and "FCC Crackdown on Indecency Leads to Historic Fines" in the Winter 2004 issue.)

Some comments urged the FCC to continue penalizing incidents of fleeting expletives. "The media has already effectively destroyed American society," one person wrote. "I request that the FCC refuse to loosen its programming decency standards. America must recover its morality if our nation has any hope of surviving." The Parents Television Council (PTC) wrote in its comment, "[H]ow can material that meets the FCC's own standard of 'patently offensive' not meet a would-be standard of 'egregiousness?' It is also unclear what the definition of 'egregious' as used by the Enforcement Bureau to dismiss more than 1 million duly-filed indecency complaints was. … It has created a new de facto standard out of whole cloth and only now seeks public comment on the issue." Dan Isett, director of public policy for the PTC, told online magazine TheWrap on June 19, 2013, "It is pathetic that the best [broadcasters] can do is muster up the same arguments they lost on at the Supreme Court. These guys need to accept reality and stop airing indecent content." Tim Winter, head of the PTC, and Patrick Trueman, head of Morality in the Media, urged Congress to take action against the FCC's proposed policy shift in a May 8, 2013 letter to the Senate Committee on Commerce, Science, and Transportation and the House Energy and Commerce Committee. "We urgently request that you do all you can to stop the proposed enforcement standard, including opposing any nominee to the Federal Communications Commission who supports changing the current standard," Winter and Trueman wrote.

College Broadcasters Inc. (CBI), an advocacy organization for both high school and college radio stations, was among the many media organizations that asked the FCC to relax its indecency standards. CBI argued that the educational mission of student broadcasting involves the acknowledgment that student broadcasters inadvertently may allow a fleeting expletive to be aired. In a June 27, 2013 post on its blog, CBI called for the FCC to "provide student stations with a lot of latitude before commencing action" on indecency incidents due to "financial considerations and the lack of financial resources of student stations." On July 1, 2013, CBI filed a motion asking the FCC to extend the deadline for reply comments (comments filed by members of the public in response to initial public comments) from July 18 to Aug. 2, 2013, citing the difficulty of student radio stations filing comments during the summer, when most students are away from campus. On July 14, 2013 the FCC did extend the deadline to Aug. 2, 2013. KUCR, the student radio station at the University of California-Riverside filed a comment with the FCC on June 19, 2013 expressing its concern that "with all the training, all the precautions, all the good faith, intelligence and devotion of our volunteer staff, and an 8-second delay — with all of that — accidents may still occur. … The legal costs of responding to an FCC inquiry would be crippling, even if no fine were imposed. Clearly, the maximum $325,000 per incident fine is meant to chasten a corporate broadcaster who may have previously viewed a mere $32,500 fine simply as a cost of doing business by providing a racy language edge in the competitive world of drive-time morning zoo sensationalistic commercial radio."

The Student Press Law Center (SPLC) filed a comment with the FCC on June 19, 2013, urging the Commission to extend a recently established leniency policy toward student broadcasters for paperwork errors to also encompass indecency violations. The SPLC cited the FCC's May 13, 2013 Order (*In re William Penn Univ.*, Docket No. DA 13-1074), which created "a limited 'safe harbor' for first-time violators of recordkeeping standards such as 'public file' requirements, enabling them

FCC, *continued on page 28*

FCC, *continued from page 27*

to enter into voluntary compliance plans that ameliorate their financial exposure." The SPLC pointed out that Commission had justified this policy by reasoning that "[s]tudent volunteers at these stations are young and unlikely to have had any work experience in regulatory compliance matters, particularly those involving the FCC requirements to which [educational] stations are subject." In its comment, the SPLC's also argued that vague standards and harsh penalties for indecency incidents, particularly for inadvertently airing fleeting expletives, amounted to a chilling effect on the speech of student broadcasters, forcing them "to adopt policies that favor self-censorship over free speech." The SPLC also argued that a "fleeting expletive enforcement regime is constitutionally suspect" and that the FCC should amend the policy for all broadcasters.

Other major broadcasters have also urged the FCC to relax its indecency policy. CBS wrote in its June 19, 2013 comment, "More restrained enforcement is necessary if any order is to be brought to the chaotic state of indecency regulation. … An appropriately restrained policy regarding indecency enforcement will also require the commission to resist the temptation — and political pressures — to act as the ultimate arbitrator of whether a program has been too frank in the depiction of sexuality." NBC Universal wrote in its June 19, 2013 comment, "Unless it can establish any other legitimate basis for singling out broadcast for second-class constitutional protection, the Commission cannot continue to regulate broadcast indecency without demonstrating that its policy is the least restrictive means to achieve a compelling governmental interest." In its June 19, 2013 comment, Fox Entertainment Group and Fox Television Holdings urged the FCC "to conclude it is legally required and logically bound to cease attempting broadcast indecency limits once and for all. … Time and technology have moved inexorably forward, but the commission's untenable effort to define indecent content through a hodgepodge of inconsistent and uneven rulings remain stuck in a bygone era." National Public Radio (NPR) wrote in its June 19, 2013 comment that "a more restrained approach to indecency and profanity enforcement would better accommodate the protected speech of public radio broadcasters."

Outside of official comments filed with the FCC, scholars, interest groups, and industry experts continue to debate whether the FCC's regulatory policies for broadcasters remains relevant at a time when consumers utilize dozens of different media. Former FCC commissioner Harold Furchtgott-Roth, now a senior fellow at the Hudson Institute, told TheWrap for a June 21, 2013 article, "Broadcasting is this much diminished share of the public's attention, and while its true that 30 years ago one could make a compelling case about the massive amount of time the public spent watching broadcast media that share is now going to a lot of other media, none of which are regulated in the same way as the broadcasting industry." However, Patrick Trueman of Morality in the Media argued that broadcast media must remain distinct from other media, particularly cable. In the same June 21, 2013 article for TheWrap, Trueman said, "If people think TV is bad [now], just wait until the day when the FCC sanctions so-called 'isolated incidences' of nudity and profanity. From that day on, the networks will be competing to push the envelope on indecency, and nudity, as well as profanity, will be standard fare." Andrew Schwartzman, a D.C. attorney formerly with the nonprofit law firm Media Access Project (MAP) who has represented writers and directors in indecency cases, told TheWrap on June 21, 2013 that it will only be a matter of time before the Supreme Court rules on the FCC's indecency standards. "The best bet is that the FCC will attempt to ratchet up enforcement standards to some degree, and it will be litigated by broadcasters, probably successfully," Schwartzman said.

> "Unless it can establish any other legitimate basis for singling out broadcast for second-class constitutional protection, the FCC cannot continue to regulate broadcast indecency without demonstrating that its policy is the least restrictive means to achieve a compelling governmental interest."
>
> **— NBC Universal**

Former FCC chairman Genachowski indicated his support for relaxing the Commission's policy on fleeting expletives in a tweet in response to one such expletive. Following the April 15, 2013 bombing at the Boston Marathon, Boston Red Sox star David Ortiz told a crowd at Fenway Park, "This is our fucking city, and nobody is going to dictate our freedom." The broadcast was aired live and the expletive was not bleeped out. Genachowski tweeted on April 20, 2013 in response to Ortiz's comment, "David Ortiz spoke from the heart at today's Red Sox game. I stand with Big Papi [Ortiz's nickname] and the people of Boston – Julius."

FCC Approves Rule Requiring Wireless Companies to Protect Personal Data

On June 27, 2013, the three sitting FCC commissioners voted unanimously to require wireless companies to follow the Commission's 1996 Customer Proprietary Network Information (CPNI) rules. The declaratory ruling means that wireless companies must follow the same rules as traditional phone companies and Internet-based phone (VoIP) services when it comes to protecting customers' personal data. In the ruling, the commissioners stated that the new policy was necessary because "consumers' sensitive information, such as the numbers a wireless customer has called, the time calls are made, and where the customer was located when he or she made a call, can be disclosed to third parties without consumers' knowledge or consent." The ruling acknowledged that wireless carriers can use consumer data to improve their services, but warned that consumer data is "sensitive information [that] is potentially vulnerable to acquisition by others." The ruling also stated that only "individually identifiable" CPNI would be protected under the new policy, not aggregate customer information, and that CPNI would be protected whether it was stored on a mobile device or on a wireless company's servers. In a press release following the passage of the declaratory ruling, the FCC noted that the new ruling "does not impose any requirements on non-carrier, third-party developers of applications that consumers may install on their own." However, the ruling does require wireless companies to take "reasonable precautions" to prevent third-party applications from gaining unauthorized access to customer data, although the order does not give specific examples of what reasonable precautions may mean.

CPNI comes from section 222 of the 1996 Telecommunication Act, 47 U.S.C.

§ 222, and includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship," and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." Section 222 requires phone companies to "protect the confidentiality of proprietary information of, and relating to … customers." The declaratory ruling is the result of the FCC's review of mobile privacy policy that began in 2011 following the revelation that wireless companies were using a software called Carrier IQ to collect detailed data on how customers used their mobile devices, which sparked outrage among privacy advocates. In public comments filed with the FCC in 2012, Verizon, AT&T, and the telecommunications industry lobby group Cellular Telecommunications and Internet Association (CTIA) urged the FCC to allow wireless companies to self-regulate.

In a July 1, 2013 post on "CommLaw Blog," Paul J. Feldman, a lawyer specializing in telecommunications law with the Arlington, Va. firm Fletcher, Heald & Hildreth, criticized the policy in the wake of the recent revelation that wireless companies supplied personal data to the NSA. "So even as the government acknowledges that its own treatment of such information may not have been as confidential as had previously been represented, the government is imposing arguably new confidentiality burdens on both large and small mobile carriers," Feldman wrote. "Essential governmental principle at work: do as we say, not as we do." The declaratory order does not affect legal requests for personal data. Following the passage of the declaratory order, the law firm Davis Wright Tremaine, LLP, which advises wireless companies on privacy and data security matters, issued a statement suggesting that wireless companies "should promptly update their CPNI procedures and refresh their training programs, but need not make any new filing with the FCC until the next CPNI certification is due on March 3, 2014." (For more information on current issues involving mobile privacy, see "FTC, State Attorneys General Set Their Sights on Consumer Privacy in the Mobile Industry" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

Tom Wheeler Set to Become New FCC Chairman

Venture capitalist Tom Wheeler is expected to become the new chairman of the FCC, pending a confirmation vote by the Senate. Wheeler would replace Julius Genachowski, who stepped down on May 17, 2013. Wheeler previously served as the head of the National Cable and Telecommunications Association and the Cellular Telecommunications and Internet Association, where he lobbied on behalf of the industry. At his confirmation hearing before the Senate Commerce Committee on June 18, 2013, Wheeler said that his business experience would guide his policy as FCC chairman, but he also supported strong regulation when necessary. "While competition is a basic American value, it is not always sufficient to protect other American values," he said.

> "Even as the government acknowledges that its own treatment of [private] information may not have been as confidential as had previously been represented, the government is imposing arguably new confidentiality burdens on both large and small mobile carriers."
>
> **— Paul J. Feldman**
> **Fletcher, Heald & Hildreth**

Wheeler's testimony at his confirmation hearing and posts about FCC policy that he wrote on his blog "Mobile Musings," which he kept from 2007 to 2012, offer clues about the policies Wheeler may espouse as FCC chairman. *National Journal* reporter Brian Fung republished several of Wheeler's blog posts. The posts appeared to show that Wheeler supported net neutrality, thought news media's use of paywalls was ill-fated, and argued that network operators would be better stewards of personal data than content providers or web companies such as Google. When asked about the future of the FCC's policy on indecency at his confirmation hearing, Wheeler hinted that he supported broadcasters adopting voluntary codes. "I'm old enough that when I see some things to kind of grit my teeth and say, 'Is this what I want my grandkids to be seeing,' whether it be violence or obscenity or indecency or whatever," Wheeler said. "I do believe, however, that it is possible to call upon our better angels with some leadership."

One policy area on which Wheeler did not offer clues during his confirmation hearing was his position on using the FCC to require tax-exempt organizations backing political ads to disclose their top donors. Sen. Ted Cruz (R-Tex.) warned Wheeler at the confirmation hearing that he would not vote for Wheeler if he supported such a policy, and he requested that Wheeler send him his views on the policy in writing. Democratic senators pressed Wheeler to state his support for the policy during the confirmation hearing, but Wheeler said the issue required further study, according to a June 18, 2013 post on the "Hillicon Valley" blog. Former FCC commissioner Michael Copps issued a statement in support of Wheeler on the website of the government accountability interest group Common Cause suggesting that Wheeler was in favor of such disclosures. "If confirmed, Tom will have the most critical role in government in responding to the many daunting challenges facing our nation's communications ecosystem," Copps wrote. "Consumers deserve a leader who will put the brakes on media monopolization, make competitive high-speed telecommunications a reality for every American, ensure the long-term freedom and openness of the Internet, and require sponsorship disclosure of political ads." Meanwhile, the *New York Times* Editorial Board wrote on May 8, 2013, a week after President Obama nominated Wheeler, that Wheeler had raised hundreds of thousands of dollars in campaign donations for Obama in 2008 and 2012, and that it was likely that he had solicited donations "from people whose companies he would regulate [as FCC chairman], creating potential conflicts of interest."

The Commerce Committee approved Wheeler by a voice vote on July 30, 2013. A vote by the full Senate on Wheeler's nomination is not expected until President Obama nominates a candidate for the Republican vacancy on the FCC, which he had not done as the *Bulletin* went to press.

Brett Johnson
Silha *Bulletin* Editor

British PM Calls for Nationwide Default Filters to Combat Internet Pornography

Opponents say plan sacrifices free speech and privacy, does not address root causes of sexual abuse.

Saying Internet pornography was "corroding childhood," British Prime Minister David Cameron announced in a speech on July 22, 2013 a multi-pronged initiative aimed at protecting children from viewing online pornography and stanching the online proliferation of images depicting simulated rape and child sexual abuse. Cameron announced that broadband Internet service providers (ISPs) in the United Kingdom would equip all new and existing accounts in private homes and in public Wi-Fi locations with filters automatically set to block pornographic images. He said customers must notify their ISPs if they wanted to turn the filters off, calling the decision "unavoidable."

INTERNET FILTERING

Cameron said his government had already reached agreements with British ISPs TalkTalk, Virgin, Sky, BT, O2, Nomad, and Arquiva, which together control 90% of public and private connections in the country, to put the automatic filters in place by the end of 2014. He also announced that "all of the operators [of British mobile phone services] have now agreed to put adult content filters onto phones automatically," and customers would have to contact their mobile company to opt out of the filters. Cameron also asked Ofcom, the British government agency that regulates telecommunication, "to judge how well the ISPs are doing [with filtering] and to report back regularly." The BBC reported on July 28, 2013 that the Chinese firm Huawei Technologies managed the filters of the ISP TalkTalk. The U.S. House Intelligence Committee reported on Oct. 8, 2012 that Huawei posed a threat to national security because it had attempted to extract information from U.S. companies regarding their loyalty to the Chinese government. The British government's Intelligence and Security Committee reported on June 6, 2013 that "the alleged links between Huawei and the Chinese State are concerning, as they generate suspicion as to whether Huawei's intentions are strictly commercial or are more political." Huawei regularly has denied having strong ties with the Chinese government.

Cameron's plan also would criminalize possession of depictions of simulated rape throughout the United Kingdom. The creation of so-called "rape porn," which falls into the category of "extreme pornography" under the Criminal Justice and Immigration Act 2008, is illegal in all of the United Kingdom, but possessing it is only illegal in Scotland. "These images normalize sexual violence against women and they're quite simply poisonous to the young people who see them," Cameron said in his speech. Holly Dustin, director of the End Violence Against Women Coalition, told the BBC on July 22, 2013 that her organization was "delighted" at the ban for "tackling a culture that glorifies abuse" of women and girls. However, the London *Sunday Times* reported on June 9, 2013 that a letter released by an unnamed Ministry of Justice official stated that there was "no evidence to show that the creation of staged rape images … causes harm to society at large."

Cameron also called on Internet search giants Google, Bing, and Yahoo! to create "a list of terms — a blacklist — which offer up no direct search returns" for images of child pornography. He did not offer any examples of possible terms. The British non-profit organization Internet Watch Foundation (IWF) maintains a blacklist of URLs of sites containing images of child pornography, which it sends to both ISPs and law enforcement in an effort to have the websites removed.

Cameron said in his speech that Internet search companies have a "moral duty" to block "sick" people from searching for illegal pornography. "You [search companies] are not separate from our society, you are part of our society, and you must play a responsible role in it," he said. Cameron also stated that he "simply d[id]n't accept the argument that some of these companies have used to say that these searches should be allowed because of freedom of speech." A spokesman for Google told the BBC on July 22, 2013 that the company already had "a zero tolerance attitude to child sexual abuse imagery. Whenever we discover it, we respond quickly to remove and report it." Microsoft, owner of Bing, announced on July 27, 2013 that it had created a system where searches for child pornography would be met with a pop-up window warning the user that the content is illegal and providing a link to counseling services. The BBC reported on July 27, 2013 that Yahoo! was devising a similar system.

Cameron announced the plan nearly two months after Mark Bridger was convicted of murdering five-year-old April Jones and Stuart Hazell was convicted of murdering 12-year-old Tia Sharp. Authorities found images of child pornography on the computers of both men, leading many in the British media to blame child pornography for provoking the murders. Cameron said in his speech that the parents of Jones and Sharp "want to feel that everyone involved is doing everything they can to play their full part in helping rid the Internet of child abuse images." Cameron's plan came nearly one month after Michael Moran, head of Interpol's Crimes Against Children unit, stated on June 17, 2013 that "no police force in the world" was properly combating the spread of child pornography online.

Cameron's government had been publicly considering the new proposals for nearly two years. Conservative MP Claire Perry chaired an independent inquiry into online child protection, which published its findings in April 2012. The inquiry concluded that "many children are easily accessing online pornography and that this exposure is having a negative impact on children's attitudes to sex, relationships and body image," and that default filters "would offer the best protection for children online." Perry told the *Guardian* on May 4, 2012 that "the Internet was no different to TV and radio and should be regulated accordingly." However, the inquiry concluded that "[n]o filtering system will ever deliver total protection and parents will still need to remain engaged and active in helping their families stay safe online," and that "government regulation of the internet should always be done with the lightest touch."

Internet privacy advocates and proponents of online free speech have raised several criticisms of Cameron's plan. Critics have contended that filtering technology would block valuable non-pornographic content, such as information on sexual health. Tim Worstall, a fellow at the Adam Smith Institute, a London-based libertarian think tank, wrote for *Forbes* magazine on July 21, 2013 that blocking search results for the term "child pornography" would block important information on the legal history of child pornography. The London *Independent* reported on Aug. 21, 2013 that advocates for LGBT (lesbian, gay, bisexual and transgender) causes wrote an open letter to Cameron arguing that the filters would be detrimental to LGBT youth seeking information on their sexual identity. Critics have also argued that the filters would be under-inclusive and would

not block non-pornographic lascivious content that could be considered demeaning toward women. For example, Cameron told the BBC's Jeremy Vine on July 22, 2013 that the filters he was proposing would not block written pornography or images of topless or nearly naked women, such as those commonly featured on "Page 3" of *The Sun*.

Such a concern about over-blocking was central to the U.S. Supreme Court's reasoning in its decision in *Reno v. ACLU*, 521 U.S. 844 (1997). The court held that provisions of the 1996 Communications Decency Act, 47 U. S. C. § 223, designed to punish producers of "patently offensive" pornographic content were unconstitutionally overbroad because they also threatened to punish producers of "large amounts of non-pornographic material with serious educational or other value." However, in *United States v. Am. Library Ass'n*, 539 U.S. 194 (2003), a divided Supreme Court upheld the constitutionality of the Child Internet Protection Act (CIPA), 47 U.S.C. § 254 (h)(1)(B), which made the installation of pornography filtering technology on public library computers mandatory for those libraries to receive federal subsidies. Six Justices held that CIPA did not violate library patrons' First Amendment rights, as patrons could ask librarians to turn the filters off if they wanted to view non-pornographic content that was blocked by the filters. In his concurring opinion, Justice Anthony Kennedy called this requirement a "minor burden on free speech." In dissent, Justice John Paul Stevens argued that CIPA was unconstitutional because filters "overblocked" content that was "completely innocuous for both adults and minors." Stevens also argued that the filters did not block other sexually explicit material, "provid[ing] parents with a false sense of security without really solving the problem that motivated its enactment." (For more information on *U.S. v. ALA*, see "Courts Rule in Internet Cases: *United States v. American Library Association*" in the Summer 2003 issue of the Silha *Bulletin*.)

Critics of the plan have argued that it conflates two separate issues: eradicating illegal pornography, such as rape porn and child porn, and preventing children from viewing legal pornography. In a July 22, 2013 column, *Guardian* columnist Suzanne Moore called Cameron's proposals "unworkable and sentimental," arguing that they "deliberately confuse" child pornography with other kinds of legal pornography. Laurie Penny, contributing editor for the British public affairs magazine *New Statesman*, wrote on June 13, 2013, "The worst thing about this debate is that it turns a real-world, complex problem into a simple moral choice: porn is either good or bad, right or wrong, and not one shade of grey can be permitted, let alone 50."

In a July 22, 2013 column, Steve Kovach, senior editor at *Business Insider*, called the requirement to ask the filters to be turned off, "a huge violation of privacy." Adam Taylor, a columnist for *Business Insider*, argued in a July 23, 2013 column that "Cameron's plan is to make it awkward to opt out of the filter," meaning that fewer adults will watch legal pornography for fear of, in the words of the BBC's Jeremy Vine from his July 22, 2013 interview with Cameron, "fessing up" to their desire to watch it. Privacy advocates also have expressed concern over ISPs keeping records of the customers who choose to opt out of the filters. *Guardian* columnist Moore asked in her July 22, 2013 column, "In the day of PRISM [the NSA data surveillance program] and maxi-surveillance, do we actually want more databases of those who access porn?" Loz Blain, columnist for the online technology magazine Gizmag, predicted in a July 23, 2013 column that "[s]omewhere, there will be a very useful list of people who are porn users, and one day it will leak," and that "the famous British gutter press will be delighted to reveal the names of famous people who have asked for the filter to be disabled."

Critics of the plan have argued that for all of its costs to privacy and free speech, the plan does not do enough to fight the root causes of sexual abuse. Laurie Penny of *New Statesman* wrote on June 13, 2013, "To say that dirty pictures are the problem in themselves, rather than a structure of violent misogyny and sexual control, is to confuse the medium with the message." Jim Gamble, former head of Britain's Child Exploitation and Online Protection center (CEOP) told the London *Independent* on July 22, 2013 that the plan was "a pop-up that paedophiles will laugh at," because most child porn is shared using untraceable peer-to-peer networks. *Business Insider* reported on July 22, 2013 that Britons could circumvent the filters easily using virtual private networks (VPNs), blocking their IP addresses with software such as Tor, or remotely accessing desktops in another country. Charles Arthur, technology editor for the *Guardian*, argued in a July 22, 2013 column that "the only way to stop someone really determined to access peer-to-peer systems or well-hidden sites is to cut off the Internet."

Proponents of Internet free speech disagreed with Cameron's argument in his speech that his plan was not "about companies or government censoring the internet, but [rather] about filters to protect children." In a July 22, 2013 interview with the London *Independent*, Padraig Reidy of the Index on Censorship (IOC), a British organization that promotes freedom of speech around the world, called Cameron's plan "default censorship." The Electronic Frontier Foundation (EFF) stated on its "Deep Links" blog on July 23, 2013 that "the lasting damage of [Cameron's] new initiative will serve to extend the precedent that the UK government and private actors can interfere with Internet communications without regulation or legislative oversight." The EFF argued that "[a] secret blacklist can have no transparency," and "an unregulated filtering system will have no oversight." Paul Bernal of *New Statesman* questioned in a July 22, 2013 article whether Cameron's call to filter pornography would lead to future filtering of other content, such as the depiction of violence or the glorification of terrorism. "It's a very slippery slope towards censoring pretty much anything you don't like, whether it be for political purposes or otherwise," Bernal wrote.

Cameron contended in his speech that Internet companies could not use the "technical obstacles" as an excuse for inaction. "You're the people who have worked out how to map almost every inch of the Earth from space; who have developed algorithms that make sense of vast quantities of information," he said. "Set your greatest brains to work on this." However, Georgina Voss, a technology researcher at the Royal College of Art in London, wrote in a July 24, 2013 post for the *Guardian*'s "Political Science" blog that Cameron's demands were antithetical to the values of those great brains. Voss took issue with Cameron's call in his speech for those great brains to "hold a hack-a-thon for child safety," contending that hack-a-thons are generally geared toward improving government transparency and Internet freedom. "[I]t would be wise for policymakers to exercise caution around considering [Internet] users as cheap and malleable forms of R&D to achieve some government-defined notion of 'good,'" Voss wrote.

Brett Johnson
Silha *Bulletin* Editor

Activists, U.S. Government Advocate Removal of User-Generated Content

In May 2013, interest groups and the U.S. State Department sought the removal of controversial user-generated content (UGC) from the Web in three separate incidents. On May 2, 2013, the social networking giant Facebook removed from its servers two videos depicting three individuals being beheaded. A few weeks later, Facebook came under fire from feminist organizations for pages created by users on the social network that advocated or made light of rape and domestic violence. On May 8, 2013, the U.S. State Department demanded that a University of Texas law student and gun enthusiast remove the instructions for making a plastic handgun using a 3D printer from his company's website, which it claimed violated the Arms Export Control Act, 22 U.S.C. § 2778, and other federal regulations. These incidents have stirred debate on how to deal with potentially harmful UGC, highlighting the struggle among individuals, activist groups, advertisers, private companies, and the government over who has the final say on whether such content — even if it is protected speech — should be removed from the Web.

ONLINE SPEECH

Facebook Removes Controversial Content, Vows to Update Its Terms of Use

In late April 2013, two videos of unknown origin, one depicting the beheading of a woman and the other showing the beheading of two men, spread throughout the personal pages of Facebook users. A caption with the first video said the female victim was beheaded for infidelity, and language heard on the video suggested it was filmed in Mexico, according to a May 1, 2013 BBC article. The two male victims in the second video stated before being beheaded that they were Mexican drug traffickers, the BBC reported. According to the May 1 BBC article, a university student in Belfast named Ryan L. asked Facebook to remove one of the videos after it appeared on his news feed, a display of the Facebook-related activity of a user's friends on the social network.

Facebook replied to the student that the video did not violate the social network's terms of service regarding graphic violence, which ban the depiction of "harm to someone or something, threats to the public's safety, or theft and vandalism," or "sharing any graphic content for sadistic pleasure." Facebook released a statement on April 30, 2013 justifying its decision. It said, "People are sharing this video on Facebook to condemn it. Just as TV news programs often show upsetting images of atrocities, people can share upsetting videos on Facebook to raise awareness of actions or causes. While this video is shocking, our approach is designed to preserve people's rights to describe, depict and comment on the world in which we live." The U.S.-based Family Online Safety Institute (FOSI), an interest group that serves on Facebook's Safety Advisory Board and promotes methods of making the Internet safe for children while also respecting free expression, criticized Facebook's decision. Two hours later, Facebook removed the videos, stating, "We will remove instances of these videos that are reported to us while we evaluate our policy and approach to this type of content," according to the May 1, 2013 BBC article.

Several other interest groups responded to Facebook's initial decision by arguing that such videos could cause psychological harm, particularly to children. Some contended that the networked nature of Facebook would lead to greater harm because such videos could spread quickly and involuntarily to users. Arthur Cassidy, director of the suicide prevention charity Yellow Ribbon, told the BBC that he worried "some people, in their innocence, might share this [video] with friends to say how abhorrent it is, and we are concerned about the profound and uncontrollable impact this can have on an entire community." Cassidy said that such videos can "cause flashbacks, nightmares and sleep disturbance," which over time "can transfer into many other negative effects in a child and adults as well such as anxiety-related disorders and panic attacks." Stephen Balkam, the CEO of FOSI, told *Huffington Post* for a May 2, 2013 article that the removal of the videos was justified because Facebook is not a news site. "You could make an argument [that such videos are in the public interest] on a mediated news site like the *Huffington Post*, like CNN or NBC.com, where you have professional editors and standards and you are accountable," Balkam told the *Huffington Post*. "But the public interest argument becomes far more tenuous for Facebook, and also for Tumblr and for YouTube."

The issue of violent and graphic content on Facebook may be bigger than the beheading videos. Following the BBC's May 1, 2013 article about Facebook's removal of the beheading videos, the British network reported on May 9, 2013 that it was contacted by readers who claimed that they had contacted Facebook with requests to remove videos depicting a murder, cruelty to animals, and the beating of a schoolgirl, among other activities that appeared to violate Facebook's community standards. The readers said that Facebook denied their requests, according to the article, which reported that Facebook "confirmed its policy had only been amended in regard to decapitations."

Another contentious debate over Facebook's speech codes that made headlines soon after the incident with the beheading videos involved user-created pages that glorified or made light of rape and domestic violence. Activist Soraya Chemaly, Jaclyn Friedman of the group Women, Action and the Media (WAM), and Laura Bates of the Everyday Sexism Project, published an open letter online on May 21, 2013 demanding that Facebook not tolerate "speech that trivializes or glorifies violence against girls and women." The women asked Facebook users to contact companies whose ads appeared on pages with such speech. In April 2013, Bates took a screenshot of a page titled "Drop kicking sluts in the teeth" and tweeted it to the cosmetics company Dove, whose ad appeared next to the page, according to a May 21, 2013 article in the *Guardian*. The open letter stated that pages had titles such as "Fly Kicking Sluts in the Uterus" and "Violently Raping Your Friend Just for Laughs," and images appeared on the network "of women beaten, bruised, tied up, drugged, and bleeding, with captions such as 'This bitch didn't know when to shut up' and 'Next time don't get pregnant.'" The activists persuaded Facebook's advertisers such as Nissan UK, *Jump* magazine, and Desire Books and 15 other companies to pull ads from the social network on May 28, 2013, according to WAM. Nationwide Building Society, a British mutual fund firm that

suspended advertising on Facebook following the open letter from the women's rights organizations, released a statement on May 29, 2013 saying "sites like Facebook should have stringent processes and guidelines in place to ensure that brands are able to protect themselves from appearing alongside inappropriate content."

Marne Levine, Facebook's vice-president for global public policy, responded to the activists' demands in a May 29, 2013 blog post on the social network, promising that Facebook officials would "update the training for the teams that review and evaluate reports of hateful speech or harmful content on Facebook." Levine wrote that Facebook would push for more accountability from "the creators of content that does not qualify as actionable hate speech but is cruel or insensitive by insisting that the authors stand behind the content they create." For example, this requirement would mean that "the creator of any content containing cruel and insensitive humor include his or her authentic identity for the content to remain on Facebook." Levine did not promise that Facebook would remove any of the pages. (The blog post is available at https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054).

On June 28, 2013, Facebook announced on its blog that it would "seek to restrict ads from appearing next to Pages and Groups that contain any violent, graphic or sexual content." The decision came after Rupert Murdoch's British Sky Broadcasting Group and British clothier Marks and Spencer pulled ads from Facebook after finding out that their advertisements were placed on a page titled "Cute and Gay Boys" that contained suggestive photos of teenage boys. The blog post continued, "In order to be thorough, this review process will be manual at first, but in the coming weeks we will build a more scalable, automated way to prevent and/or remove ads appearing next to controversial content. All of this will improve detection of what qualifies as questionable content, which means we'll do a better job making sure advertising messages appear next to brand-appropriate Pages and Groups." Amanda Dodge, blogger for the Internet marketing company CopyPress, criticized Facebook's new policy in a July 3, 2013 post for creating "a gray area where pages can be offensive, but not offensive enough to be taken down. These pages still exist and can promote their message, and because brands aren't compensated for having ads on their pages, there is no incentive for borderline offensive groups to clean up their acts. Removing the ads seems more like a crisis PR move to keep advertisers happy than Facebook paving the way towards a less sexist, less racist Internet."

Facebook's removal of the gory videos and its promise to review sexist pages more strictly sparked a debate on the role of social networks in facilitating speech and how social networks should manage their terms of use to fit that role. Richard Allan, Facebook's director of policy for Europe, the Middle East, and Africa, told the BBC on May 9, 2013, "While we freely admit that we do not always get it right, the trouble-free daily experience of the vast majority of Facebook users demonstrates that our systems are working well in all but the most exceptional cases and that they are improving over time." Allan said that "there are situations where it is important for people to be able to share content through Facebook even if this can at times be quite shocking." He cited users living through the Syrian civil war using Facebook to document atrocities from that conflict as an example of such shocking yet important content. Lynne Jordan, a British psychologist, told the BBC that social media sites' voluntary ethical codes "are there for safety and to preserve the right to choose what is viewed when users are considered of age or able to understand the implications. Social media sites are mostly not obliged to adhere to such codes which creates a problem, particularly if they issue their own vague inadequate guidelines."

> "Advocates for free expression must remain vigilant that the private players that provide so much public value online are meeting their responsibilities to users."
>
> **— Andrew McDiarmid, Senior Policy Analyst, Center for Democracy & Technology**

Joanna Chiu, a columnist for the Canadian feminist magazine *Herizon*, criticized the arbitrariness of Facebook's content policy in a May 29, 2013 article in the *International Business Times*. "Why were photos of women breastfeeding deleted but pages that promoted rape, violence against women and racism allowed to stay online for years?" Chiu asked. "[Facebook] still need[s] to be held accountable to their users and advertisers for the hate speech they allowed to proliferate on their platform while going around deleting photos of errant nipples." The May 2013 uproar over the sexist pages was not a first for Facebook. In 2011, Facebook removed several pages with names that were very similar to the pages that activists campaigned against in May 2013. Jane Osmond of the British advocacy group Women's Views on News, which seeks to "redress the gender imbalance in global news reporting," told the BBC in November 2011 that Facebook must do more than remove sexist pages to preserve its own image. "The public need to know that Facebook have revised their position," she said.

Andrew McDiarmid, senior policy analyst at the Center for Democracy & Technology in Washington, D.C., told the BBC that "systems for assessing content require constant refinement to ensure that free expression is protected," and that advocates for free expression "must remain vigilant that the private players that provide so much public value online are meeting their responsibilities to users." George Washington University law professor Jeffrey Rosen told NPR on April 3, 2013 that Internet giants such as Facebook "have more power over who can speak and what can be said all across the globe than any king or president or Supreme Court justice." Computer programmer and activist Aaron Swartz, who committed suicide in January 2013 before his federal hacking trial was to begin, argued in a July 2012 interview that *Wired* magazine posted on its website on April 29, 2013 that large firms controlling Internet communications, such as Facebook, were committing "corporate tyranny." Such firms "don't have a constitution to answer to," Swartz said in the interview, allowing them to regulate speech in much the same way malls can regulate speech. Swartz called this regulation "censorship."

Yet many First Amendment scholars argue that the term "censorship" cannot be used to describe private regulation of speech. The U.S. Supreme Court held in *Miami Herald v. Tornillo*, 418 U.S.

Online Speech, *continued on page 34*

Online Speech, *continued from page 33*
241 (1974), that a Florida statute requiring newspapers to publish responses from individuals to attacks in the paper amounted to an unconstitutional prior restraint. The decision was predicated on the idea that only government can censor, not private institutions. Reuters columnist Jack Shafer wrote on May 30, 2013, "Just because Facebook has given you free access to its 21st century universal printing-press doesn't mean it has an obligation to publish your message. If you don't like Facebook's rules, you can still create controversy and test boundaries at other social media sites." However, Jeremie Zimmermann, co-founder of La Quadrature du Net, a French organization that promotes access to a free and open Internet, argued that "private censorship" is not only a question of the relationship between Internet companies and their users, but rather it involves the role of government as well. He told the BBC for the May 9, 2013 article that vague policies on speech codes could "ensure that any government could pressure Facebook to consider their own criteria, whether for political, religious or other reasons." He argued that governments could put such pressure on private actors because a "dominant, centralized actor such as Facebook would be incentivized to spend as little money as possible determining which content would be … suitable or not." "As surely as we cannot trust giant centralized corporations to defend our fundamental freedoms, we cannot ask them to become the judges and enforcers of what information should be shared online," he argued.

Government officials in the United States and abroad regularly have asked private Internet companies to remove content that they deem harmful. In May 2008, Sen. Joe Lieberman (I-Conn.) sent a letter to Google CEO Eric Schmidt demanding that the company remove all "terrorist training" videos from its subsidiary YouTube. Google declined the request, saying it would remove only videos that violated its terms of use concerning hate speech and the depiction of violence. In September 2012, Google blocked the inflammatory YouTube video "Innocence of Muslims" from being viewed in Egypt, Indonesia, India, Jordan, Malaysia, Russia, Saudi Arabia, Singapore, and Turkey, following requests from those countries' governments. Google also temporarily removed the video from view in Libya "due to difficult circumstances" in that country, according to Google's 2013 Transparency Report, which documents the number and nature of requests from governments around the world for removal of content that Google controls.

The Obama administration initially contended that unrest over the video led to the Sept. 11, 2012 attack by Islamists on the U.S. consulate in Benghazi, Libya in which four people were killed, including U.S. Ambassador J. Christopher Stevens. Officials asked Google to review the video to determine whether it complied with its terms of use, and Google said that the video did comply, according to the Transparency Report. The administration later said the attack was a planned terrorist attack, according to multiple media reports.

Stephen Carter, a professor at Yale Law School, wrote in a widely distributed column in mid-September, 2012 titled "How Muslim Extremists can learn from Larry Flynt" that "[s]ome observers have pointed out, correctly, that even if the U.S. government can't censor the video, Google Inc., owner of YouTube, is a private corporation and can do as it likes. Given Google's size, and YouTube's ubiquity, I am wary of endorsing any call [by the government] for a crackdown." (Google's 2013 Transparency Report is available at http://www.google.com/transparencyreport/removals/government/).

Online Blueprints for 3D-Printed Handgun Spark First Amendment Debate

On May 3, 2013, *Forbes* magazine reported that Cody Wilson, a law student at the University of Texas and founder of the company Defense Distributed, had created a plastic handgun called the "Liberator" using a 3D printer. 3D printers work by a process known as "additive manufacturing," whereby the printers lay down layer upon layer of plastic as thin as 0.25mm to create an object. The printers follow a digital model created using a computer assisted design (CAD) file to make the object. On May 6, Wilson posted a video on YouTube showing the Liberator being successfully fired at a shooting range in Austin, Texas. Defense Distributed posted the CAD file for the Liberator on its website, and the file was downloaded more than 100,000 times, according to multiple news reports.

On May 8, 2013, the U.S. State Department sent a letter to Wilson demanding that he remove the CAD file from his company's website because the Department claimed the files violated the Arms Export Control Act (AECA), 22 U.S.C. § 2778, and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130. The letter specifically cited section 120.10 of ITAR, which regulates the export of "technical data," defined as "[i]nformation, other than software …, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles." Such information includes "blueprints, drawings, photographs, plans, instructions or documentation." The State Department argued that by posting the CAD file online, Wilson could potentially be exporting technical data for weapons designs, for which he would require an export license. Wilson complied with the State Department's request and removed the CAD file from his website. The website, defcad.com, currently contains the following message: "DEFCAD files have been removed from public access at the request of the US Department of Defense Trade Controls. Until further notice, the United States government claims control of the information." Although the CAD file is no longer available on defcad.com, the file is available on the Swedish torrent site known as The Pirate Bay.

Fox News reported on May 23, 2013 that it obtained a Department of Homeland Security (DHS) intelligence bulletin distributed to state and federal law enforcement agencies that warned of the dangers of 3D-printed guns. (As the *Bulletin* went to press, Fox News had not posted the intelligence bulletin to its website and it had not been found anywhere else online.) According to the Fox News report, the intelligence bulletin warned that 3D-printed guns might violate the 1998 Undetectable Firearms Act, Pub. L. 100-649, because plastic guns could pass undetected through magnetometers (traditional metal detectors), they could be made without serial numbers, and they could be obtained without a background check. The bulletin specifically referred to Defense Distributed and the CAD file for the Liberator as evidence of the emergence of the production of 3D-printed guns and the difficulty of regulating them. Although Wilson included instructions to place a 6 oz. steel cube inside the Liberator to comply with the Undetectable Firearms Act, the intelligence bulletin warned that "manufacturers may deliberately omit the unnecessary metal insert, leaving only a small nail and ammunition as the sole metal component," and that "[f]uture designs could further reduce or eliminate metal entirely." The bulletin admits that "online distribution of these

digital [CAD] files will be as difficult to control as any other illegally traded music, movie or software files."

Wilson's CAD file and the State Department's request for its removal have spurred a debate on whether Wilson had a First Amendment right to post the file and whether the government's request amounted to an unconstitutional prior restraint on Wilson's speech. Scholars and journalists have pointed out that the debate hinges on the connection between Wilson's publication of the blueprints and the likelihood that the blueprints could lead to a direct violation of law or causation of harm, now or in the future. The gun Wilson fired was made from a professional $8,000 3D printer, according to a June 7, 2013 article in the *San Antonio Express* by reporter René Guzman. Guzman quotes Ken Denmead, editorial director at *MAKE* magazine, which writes about "do-it-yourself" (DIY) projects, as saying a consumer-grade desktop 3D printer could not make Wilson's gun because the plastic from such a printer would not be dense enough to withstand firing.

The *Guardian* reported on May 9, 2013 that its reporters tested two Liberator handguns that they made with a professional printer similar to Wilson's. One gun broke apart after several shots, and another gun broke apart on the first shot. Guzman also wrote that many third-party 3D printing services such as Cubify forbid the printing of weapons, making it more unlikely that an individual could acquire the plastic gun in the near future. Two reporters for the London *Daily Mail*, Simon Murphy and Russell Myers, published an article on May 11, 2013 describing their experience bringing the Liberator through a metal detector and onto the Eurostar train between London and Paris. Photos on the *Daily Mail*'s website show Murphy and Myers holding the gun in plain sight while on the train. On Aug. 9, 2013, Fox News reported that a Canadian man named "Matthew" posted a video to YouTube showing a rifle that he created with a 3D printer. Matthew said the rifle fired 14 .22-caliber rounds before splitting in two. The rifle needed to be taken apart and reassembled to load each new round. Matthew's video is no longer on YouTube.

Whether or not guns such as the Liberator are illegal now or are made illegal through future legislation, the CAD files used to make them may have First Amendment protection. Ansel Halliburton, an IP lawyer for the Palo Alto, Calif. firm ComputerLaw Group, wrote in a May 15, 2013 article for technology news website Tech Crunch that under the Undetectable Firearms Act, plastic handguns are contraband, but "you can possess CAD files for an undetectable firearm without violating [the Act]." Halliburton called that distinction "an easy legislative patch," but argued that any new law banning blueprints like Wilson's "will run into free speech problems."

Some commentators have questioned whether banning the CAD file will actually succeed in preventing any potential harm, thereby bolstering Wilson's First Amendment right to publish the files. J.D. Tuccille, managing editor of *Reason* magazine, wrote in a May 8, 2013 post on *Reason*'s "24/7" blog that "the Internet is a world-wide network; you need only one jurisdiction friendly to free speech to defeat censorship efforts elsewhere. Internet censorship has never been successful, and it seems a faint hope for controlling the distribution of 3D printer designs." James Ball, columnist for the *Guardian*, wrote in a May 10, 2013 column that "the wider political danger [the State Department's ban] could represent is huge. This is a ban that's going to be virtually impossible to enforce: as almost any music company will testify, stopping online filesharing by banning particular sites or devices is roughly akin to stopping a tsunami with a bucket."

> "If our government takes the position that all material published online is treated with the scrutiny we used to reserve for international defense contractors, we have just placed severe limitations on persons Congress never sought to control when it passed these international trade statutes."
>
> **— Andy Sellars**
> **Staff Attorney,**
> **Digital Media Law Project**

Andy Sellars, a staff attorney at the Digital Media Law Project (DMLP) and the Corydon B. Dunham First Amendment Fellow at the Berkman Center for Internet and Society at Harvard University, wrote in a May 10, 2013 DMLP blog post that the order for the removal of the blueprints was "obviously and inherently done for the expressive content that they convey." Sellars also criticized the State Department's use of the ITAR in justifying the removal request. "If our government takes the position that all material published online is treated with the scrutiny we used to reserve for international defense contractors, we have just placed severe limitations on persons Congress never sought to control when it passed these international trade statutes," Sellars wrote.

Sellars argued that if Wilson were to challenge the State Department's request in court, the 1999 case *Bernstein v. U.S. Dep't of State*, 176 F.3d 1132 (9th Cir. 1999) might be dispositive. In *Bernstein*, a divided panel of the U.S. Court of Appeals for the Ninth Circuit held that computer encryption code was protected expression and the State Department's attempts to regulate encryption code via the ITAR amounted to an unconstitutional prior restraint. Judge William A. Fletcher wrote that the government's argument essentially boiled down to the claim "that even one drop of 'direct functionality' overwhelms any constitutional protections that expression might otherwise enjoy." He added that a distinction between expression and functionality "would prove too much in this era of rapidly evolving computer capabilities. The fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the government the unfettered power to impose prior restraints on speech in an effort to control its 'functional' aspects." Tech Crunch's Halliburton agreed with Sellars that "Defense Distributed will likely follow *Bernstein*'s path," and that "[t]he State Department's takedown demand probably qualifies as a prior restraint." However, he wrote that "the ability to download a file, press 'Print,' and have gun parts come out could also tip some judges toward calling gun CAD files functional things and allowing the government to regulate them."

Brett Johnson
Silha *Bulletin* Editor

Gawker Media, *Rolling Stone*, and Oakland Fox Affiliate Spark Ethics Debates

Audiences witnessed three major controversies in journalism ethics over the summer of 2013. U.S. alternative news website Gawker raised eyebrows when it solicited donations from readers to pay drug dealers for a video allegedly showing Toronto mayor Rob Ford smoking crack cocaine. *Rolling Stone* angered many by publishing its Aug. 1, 2013 issue with a controversial image of suspected Boston Marathon bomber Dzhokhar Tsarnaev on the cover. Oakland, Calif. Fox affiliate KTVU-TV was criticized for mistakenly airing phony and racist names of the pilots involved in the crash of Asiana Airlines flight 214 in San Francisco.

ETHICS

Gawker Media Pushes the Envelope on "Crowdfunding" in Alleged Rob Ford Crack Scandal

On May 16, 2013, the news website Gawker announced that members of its staff had watched a video purportedly showing Toronto mayor Rob Ford smoking crack cocaine. The *Toronto Star* also announced that two of its reporters had seen the video. Gawker did not name the source of the video, saying only that it came from people connected with drug dealers in Toronto. Gawker reported that the source wanted $200,000 to release the video to Gawker. To raise the money, Gawker created a campaign called "Crackstarter," a play on words of the website Kickstarter, to solicit donations from readers. Kickstarter is a website that allows individuals and organizations to raise money from the public to fund artistic projects. Gawker created Crackstarter using the crowdfunding website Indiegogo, which works the same way as Kickstarter.

John Cook, editor of Gawker, wrote a May 17, 2013 blog post justifying the plan to pay the drug deals. "The owners of this video fear for their safety, and want enough money to pay for a chance to get out of Toronto and set up in a new town," Cook wrote. "Their fear is not entirely unwarranted. Rob Ford is a powerful if buffoonish man, and he was wrapped up in a drug scene that purportedly involved many other prominent Toronto figures." Cook wrote on May 17, 2012 that if the video's owners disappeared or sold the video elsewhere, Gawker would "donate every penny … to a Canadian non-profit that helps people suffering from addiction and its consequences." On June 4, 2013, Cook wrote that the owner of the video told him through an intermediary that the video was "gone" and that he wanted Gawker to "leave [him] alone," saying he was afraid of being identified. The CBC reported on July 18, 2013 that Gawker had chosen four Toronto charities to which it would donate the $184,782.61 that it raised in its campaign.

On May 16, 2013, *Toronto Star* reporters Robyn Doolittle and Kevin Donovan reported they too had viewed the video. The video "appears to show Ford in a room, sitting in a chair, wearing a white shirt, top buttons open, inhaling from what appears to be a glass crack pipe," the reporters wrote. The reporters said they "had no way to verify the authenticity of the video," which was "shot during the past winter." However, they said that they had "studied numerous city-hall-related videos of Ford and, to the best of [their] abilities, they separately concluded the man in the video was Ford." The reporters quoted Ford's lawyer Dennis Morris as asking them, "How can you indicate what the person is actually doing or smoking?" The reporters wrote that the *Star* could have bought the video but chose not to do so, and, like Gawker, that the people selling the video wanted to leave Toronto.

Both Gawker's and the *Star*'s coverage of the alleged Ford scandal raised several ethical questions. Should Gawker have been willing to pay $200,000 to alleged drug dealers for the video? Should it have solicited the funds from readers? Should Gawker or the *Star* have published the allegations against Ford without having video evidence to show readers? Reactions from journalists, media analysts, and readers have been mixed.

Hugo Rodrigues, president of the Canadian Association of Journalists, told the Canadian Journalism Project on May 23, 2013, "Canadian journalism isn't a culture that pays for information. It's just not part of our fibre." Russell Smith, columnist for the Toronto-based *The Globe & Mail*, wrote on May 21, 2013 that Gawker's willingness to pay drug dealers for the video was no different from the *News of the World* phone hacking scandal in the United Kingdom. (For more information on the phone hacking scandal, see "Not Just a 'Rogue Reporter': 'Phone Hacking' Scandal Spreads Far and Wide" in the Summer 2011 issue of the Silha *Bulletin*, and "Murdoch-owned British Paper Embroiled in Phone Scandal" in the Fall 2009 issue.) Jeff John Roberts, columnist for the online news site PaidContent.org, wrote on May 17, 2013 that "turning [checkbook journalism] over to the public could have unforeseen consequences. Until now, publicly funded journalism has been largely been contained to organizations like Pro Publica that launch investigations into things like patient safety and vote buying. Is the world ready for a publicly funded version of TMZ where everyone can pool money to see celebrity's private lives?"

Christopher Zara, columnist for the *International Business Times*, argued in a May 22, 2013 column that it was "a mathematical certainty" that the video, if it exists, would be released whether or not Gawker paid for it. "But," Zara wrote, "at least if Gawker fails, we can expect to see fewer copycat 'Crackstarters,' which would mean fewer news outlets asking their readers to bankroll their virality [ability to go viral], which would mean fewer people paying to watch incriminating videos, which would mean a better world." Tom McCarthy, columnist for the *Guardian*, criticized Gawker in a May 24, 2013 column for hypocritically endorsing crowdfunding for the Rob Ford video after one of Gawker's writers criticized filmmaker Zach Braff for soliciting money on Kickstarter for his latest film in April 2013.

Jane Kirtley, Silha Professor of Media Ethics and Law at the University of Minnesota and director of the Silha Center, said in a June 9, 2013 interview on the Canadian radio program "The Roy Green Show" that she found Gawker's actions "really difficult to defend." "There was a time when it was simply unthinkable to report on unsubstantiated charges," Kirtley said. "Rule number one is that you have to be absolutely sure of your facts." Kirtley also said that "the last thing [Gawker] ought to be doing is crowdsourcing the money." Kirtley called Gawker's "plan B" of donating the crowdsourced funds to charity "a lame excuse" for not being able to obtain the video.

Others have argued that the ends justified the means in this case because of Ford's reputation as a controversial public figure. In a May 21, 2013 column, *Toronto Star* columnist Rosie DiManno said "Ethics shmethics," and called for her employer to buy the video "[b]ecause somebody will. And if that somebody happens to be an ally of the mayor or just a Ford junkie with deep pockets, the purported evidence of Toronto's chief magistrate sucking on a crack pipe will disappear — locked in a vault, burned, erased. Then, all deniability would be plausible." Robyn Doolittle defended her organization's decision to run the story

without the video in an interview with the CBC for a June 3, 2013 story. "It's interesting to me that people believe there is some mass conspiracy between two organizations and three separate people," Doolittle said. "It's fair that people are questioning the things that they're reading. The people who don't believe it, maybe won't believe it even when they're confronted with the video." Gerard Adderley, a resident of Toronto, told the *Huffington Post* on May 24, 2013 that he supported the story coming to light and Gawker's attempt to buy the video through crowdfunding. "[W]hat I think makes a fantastic story is that ultimately if this video comes to light it will not have been a news organization, per se, that paid for it, it will be the people," Adderley said. "A lot of people feel this is tantamount to bullying, and my reply to that is: Actually, no, it's not. This is the school yard coming together to put the bully in his place." The editorial board of the Queen's University *Journal* wrote on May 28, 2013 that although "the media's coverage may seem gratuitous, the alternative was staying silent about the misconduct of an elected official — a more unethical option."

Meanwhile, Chris MacDonald, director of the Jim Pattison Ethical Leadership Education & Research Program at Toronto's Ted Rogers School of Management, wrote in a May 22, 2013 column for *Canadian Business* that the ethics of the actions of Gawker and the *Star* are not black-and-white. "Too often the question gets posed as 'Is this ethical?' when what would be more useful is to ask 'Just how bad is this?'" MacDonald wrote. "In the end, avoiding the all-or-nothing judgment is pretty important in a case like this, because it's very unlikely that many of us (in Toronto, at least) will keep our hands clean. The option most of us will choose is to let Gawker or someone else get their hands dirty — let them do the crowdsourcing, buy the tape, and so on — and then cackle with glee at the results in the privacy of our own homes." Robyn Urback, columnist for the Canadian *National Post*, wrote on May 22, 2013 that "the idea that two investigative reporters would risk their careers to fabricate a story in collaboration with international media is a little too far-fetched for all but the most ardent inhabitants of Ford Nation." However, Urback argued that the main ethical issue of the story was its sensationalist nature, writing that "viewing the video would provide nothing more than a thrill for the army of opponents dedicated to chasing the mayor from City Hall. Nothing else."

On Aug. 19, 2013, *Huffington Post Canada* reported that the Ontario Press Council will hold a public hearing on Sept. 9, 2013 to determine whether the *Toronto Star* "engaged in irresponsible, unethical investigative reporting" in covering the Rob Ford story. The Ontario Press Council is a non-governmental body made up of 15 members, including both journalists and non-journalists, that addresses complaints from the public on the "proper ethical standards" of Ontarian journalism, according to the Council's website. The Council "exists because media organizations recognize that a democratic society has a legitimate and fundamental interest in the quality of the information it receives," according to the Council's constitution, published on its website. The Council's website states that the Council receives around 100 complaints from the public per year. The Council received 41 complaints regarding the story, according to the Aug. 19 *Huffington Post Canada* article. The article also stated that *The Globe & Mail* would be the subject of a public hearing on the same day to determine whether the newspaper also "engaged in irresponsible, unethical investigative reporting" in a story it published about Rob Ford's brother, Toronto City Councilman Doug Ford, being an alleged drug dealer. Each newspaper is required to publish the final decision of the Council regarding the ethics of the respective stories.

> "There is a legitimate journalistic story to be told here, but *Rolling Stone* cheapened it with that particular photograph on the cover."
>
> **— Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law**

Rolling Stone *Cover Featuring Glam Shot of Alleged Boston Bomber Stirs Ethical Debate*

On July 18, 2013, *Rolling Stone* angered many and prompted a debate among media ethicists when it released the cover of its Aug. 1, 2013 issue, which featured a photograph portraying alleged Boston Marathon bomber Dzhokhar Tsarnaev in a flattering pose. The photo promoted a feature piece about Tsarnaev that reporter Janet Reitman wrote for that issue. The photograph was a so-called "selfie," or self-portrait, that Tsarnaev took using his cell phone. Tsarnaev's facial features are soft, he is shown smiling slightly, and he is wearing a designer T-shirt.

Rolling Stone released a statement from its editors on its website saying that the story "falls within the traditions of journalism and *Rolling Stone*'s long-standing commitment to serious and thoughtful coverage of the most important political and cultural issues of our day. The fact that Dzhokhar Tsarnaev is young, and in the same age group as many of our readers, makes it all the more important for us to examine the complexities of this issue and gain a more complete understanding of how a tragedy like this happens."

The cover elicited angry reactions from politicians and entertainers in both traditional and social media. Drug store chains CVS and Walgreens announced on July 18, 2013 that they would not sell the August issue. Many criticized *Rolling Stone* for portraying Tsarnaev in a glamorous, rock star light, with some even going so far as to accuse the magazine of deliberately making Tsarnaev look like Jim Morrison or Bob Dylan. Boston mayor Tom Menino said the magazine cover "reward[ed] a terrorist with celebrity treatment." On July 18, 2013, *Boston Globe* columnist Ty Burr took issue with the fact that *Rolling Stone* used a self-portrait, a choice he called "irresponsible." Burr wrote that Tsarnaev "is an enigma," and *Rolling Stone*'s choice of using a selfie gave too much deference to Tsarnaev's interpretation of "the self Tsarnaev saw himself as, rather than the complex person he was." *Rolling Stone* editor Christian Hoard fanned the flames of the controversy on July 19, 2013 when he tweeted in response to the criticism, "I guess we should have drawn a dick on Dzhokhar's face or something." Hoard later apologized for the tweet.

On July 18, 2013, Massachusetts State Police photographer Sean Murphy responded to the *Rolling Stone* cover by releasing hundreds photos to *Boston Magazine* that depicted Tsarnaev after his capture. One of the photos, which the magazine released to other news media, showed Tsarnaev raising a bloody right hand in a sign of surrender while the bright red light of a rifle's laser scope appeared on his forehead. Murphy told *Boston Magazine* that he disclosed the photos because *Rolling Stone* was "glamorizing the face of terror." Murphy was placed on restricted duty hours after releasing the photos and the Massachusetts State Police Department said it would review his actions, according to *Boston Magazine*. *The Boston Globe* reported on July 23, 2013 that State Police officials said Murphy likely would not be fired for the leak.

Some journalists and media ethicists contended that the use of that particular

Ethics, *continued on page 38*

Ethics, *continued on page 39*
photograph was a legitimate editorial decision, and that the photograph was meant to mirror the theme of the article: that Tsarnaev appeared to be an average teenager who no one would have expected to commit terrorism. *Rolling Stone* contributing editor Matt Taibbi wrote in a July 20, 2013 column that the uproar over the cover lay in the "gap between the popular image of the magazine and the reality of its reporting." He described *Rolling Stone* as "more than ever a hard news outlet in a business where long-form reporting is becoming more scarce," despite the fact that many view the magazine as being in the entertainment and pop culture genre. The *New York Times* editorial board wrote on July 18, 2013 that "singling out one magazine issue for shunning is over the top, especially since the photo has already appeared in a lot of prominent places … without outcry." The editorial board noted that the *Times* had published the same photograph on its front page on May 5, 2013. The editorial board also argued that *Rolling Stone*'s decision was not unprecedented. "*Time* magazine, for example, had quite a few covers featuring Adolf Hitler during the war years. Less than a month after the Sept. 11, 2001, attacks, *Time* featured a less-than-demonic photo of Osama bin Laden. Charles Manson appeared on *Rolling Stone*'s cover 40-some years ago for a jailhouse interview that was as chilling as it was revealing. We could go on."

However, *Rolling Stone* also received criticism for deliberately using the photo to create a buzz. *The Boston Globe*'s Burr accused the magazine of "marketing." Director of the Silha Center Jane Kirtley told "The Roy Green Show" on July 20, 2013 that *Rolling Stone* was trying to stir publicity with the photo and "cloak it as a journalistic exercise." She argued that "there is a legitimate journalistic story to be told here, … but [*Rolling Stone*] cheapened it with that particular photograph on the cover." She called the magazine's editorial choice "tone deaf." However, Kirtley said that using a mug shot of Tsarnaev would not necessarily have been a better option, because doing so often makes the accused appear guilty before having been tried. She cited *Time* magazine's use of O.J. Simpson's mug shot — which the magazine digitally altered to make Simpson look more sinister — in June 1994 as an example of an image that made an alleged criminal appear guilty.

Oakland Fox Affiliate Falls Victim to Racist Hoax, Apologizes

On July 6, 2013, Asiana Airlines flight 214 crash-landed at San Francisco International Airport, killing three passengers and injuring dozens of others. During its noon newscast on July 12, 2013, Oakland's Fox affiliate KTVU reported on what it believed were the names of four members of the Korean airline's flight crew. The names, read in a serious tone by anchor Tori Campbell, depicted the reactions of the made-up crew during the landing in a racist manner: "Sum Ting Wong, Wi Tu Lo, Ho Lee Fuk, and Bang Ding Ow." Recordings of the newscast spread quickly through social media, angering many for the offensive nature of the names and leading others to question how the names could have been aired.

> "We need to have experienced people around us who understand the kind of snark that would produce this kind of prank. More than that, we should promote the kind of thinking in newsrooms that questions everything, even when it comes from a usually reliable source."
>
> **— Al Tompkins, Media Consultant**

KTVU tweeted several hours after the noon newscast that it was "[o]ffering our sincerest apologies after falling for a hoax." On its website, KTVU said that it took "full responsibility" for the mistake. KTVU anchor Frank Somerville gave an on-air apology on July 12, 2013, explaining to viewers what led to the mistake. "First, we never read the names out loud, phonetically sounding them out," Somerville reported. "Then, during our phone call to the NTSB where the person confirmed the spellings of the names, we never asked that person to give us their position with the agency. We heard this person verify the information without questioning who they were and then rushed the names on our noon newscast." KTVU did not say from where it received the names. The NTSB issued a statement on July 12, 2013 that a "summer intern" had been the person who "erroneously confirmed the names."

The newscast sparked a threatened defamation claim by Asiana Airlines that failed to materialize. On July 15, 2013, CNN reported that Asiana would pursue a defamation lawsuit against KTVU for the "mocking" nature of the newscast, which "resulted in damaging the company's image." However, AP reported two days later that Asiana Airlines would not continue the lawsuit against KTVU. Many journalists and American media law experts questioned Asiana's plan to sue without have a clear cause of action under U.S. law. The *Los Angeles Times* reported on July 15, 2013 that the airline's "decision to sue may [have] come from the strength of defamation laws in South Korea, where companies in the past decade or so have been eager to file suit to protect their image." R. Joseph Harte, executive director of Columbia Law School's Center for Korean Legal Studies, told the *Times* that Koreans generally "are very much more sensitive to losing face and they take it much more seriously."

Following the newscast, the Asian American Journalists Association (AAJA) issued a statement saying that it was "embarrassed for the anchor of the noon broadcast, who was as much a victim as KTVU's viewers and KTVU's hard-working staff, including the journalists who produced stellar work covering the crash." However, the AAJA stated, "With such a vaunted reputation among local news stations, we expected much more from KTVU. We fail to understand how those obviously phony names could escape detection before appearing on the broadcast and were spoken by the news anchor. We urge KTVU to conduct a thorough review to prevent similar lapses." Lee Rosenthal, KTVU's news director, told the AAJA on July 12, 2013 that his station's apology "doesn't make things right." He acknowledged lapses in the reporting process, but assured that "none of this was premeditated nor was there any malicious intent in any way."

Al Tompkins, a consultant for news media, wrote on July 15, 2013 on the Poynter Institute's website that KTVU's mistake should lead newsrooms to improve fact-checking efforts and increase diversity among their editors. Tompkins wrote that "this case shows the value of having 'smart-asses' among us. We need to have experienced people around us who understand the kind of snark that would produce this kind of prank. More than that, we should promote the kind of thinking in newsrooms that questions everything, even when it comes from a usually reliable source."

Brett Johnson
Silha *Bulletin* Editor

James C. Goodale to Give 28th Annual Silha Lecture

SILHA CENTER EVENTS

James C. Goodale, vice chairman and general counsel of *The New York Times* during the Pentagon Papers litigation in 1971, will present the Silha Center's 28th Annual Lecture, "The Lessons of the Pentagon Papers: Has Obama Learned Them?" on Oct. 16, 2013. Goodale is the author of a new book, *Fighting for the Press: the Inside Story of the Pentagon Papers and Other Battles.* His lecture will address questions such as: How far can the U.S. government go in its pursuit of people who disclose classified information, such as Edward Snowden or Bradley Manning? Should "whistleblowers" be prosecuted for espionage? Can journalists who publish classified material be forced to reveal their confidential sources? How can the public's right to know be balanced against the government's claims of national security?

The Pentagon Papers consisted of thousands of pages from a secret U.S. Department of Defense study of the history of U.S. involvement in Vietnam. In 1971, former U.S. military analyst Daniel Ellsberg turned over the Pentagon Papers to reporters and editors of *The New York Times* and the *Washington Post*. In a March 19, 2013 article, Goodale told the *Columbia Journalism Review*'s Susan Armitage he wrote *Fighting for the Press* at this time because he "was really curious as the 40th anniversary of the Pentagon Papers came about, to take a look at the claims the government made of breaches of national security in composite form … and reach a conclusion." That conclusion, Goodale told Armitage, is that "not one claim has — after 40-plus years — ever been proved to damage national security." Characterizing President Barack Obama's approach to classified information and press freedom as "antediluvian, conservative, backwards," and "[w]orse than Nixon," Goodale said that many journalists do not believe that the president has an aversion to press freedom. "No one seems to care," Goodale said. "[Obama] thinks that anyone who leaks is a spy! I mean, it's cuckoo."

Goodale's book has received critical acclaim. Kofi Annan, former Secretary General of the United Nations, described Goodale's book as "[a]n engaging work which underlines the importance of fighting for a free press. Without press freedom, informed public debate is curtailed and democratic accountability diminished." R. Alan Clanton, editor of *Thursday Review*, an online magazine, wrote, "[T]his book is not only well-written, it is elegantly straightforward … never once did my eyes glaze over from lawyerly mumbo jumbo or linguistic prevarication. In fact, I could barely put the book down." Clanton's review is available online at http://www.thursdayreview.com/PentagonPapers.html. Chris Spannos, a reviewer with the alternative online news site *NYTimes eXaminer*, wrote that Goodale's book "offers a strong and contagious dose of courage — which is needed to carry forward today's fight for a free press." James D. Zirin, who reviewed the book for the *New York Law Journal*, called it a "legal thriller-diller" that "packs a real whallop." Zirin wrote, "Fighting for the Press is a clarion call to journalists, lawyers, and the public that our basic freedoms will not be destroyed with a stroke of a pen, but may be seriously eroded by a cumulation of instance, where there is insensitivity to the importance of the values enshrined in the First Amendment, and the exceptions eventually swallow the rule." Since Goodale's book has been published, he has participated in over 50 television, print, Internet and radio interviews.

As a young attorney, Goodale was a member of the U.S. Army Reserve and an intelligence analyst, a career that shaped his views on classified documents and later influenced his work on the Pentagon Papers case. In addition to the Pentagon Papers case (*New York Times Co. v. United States*, 403 U.S. 713 (1971)), Goodale served as general counsel for *The New York Times* in all its U.S. Supreme Court cases, including *Branzburg v. Hayes*, 408 U.S. 665 (1972), *New York Times v. Sullivan*, 376 U.S. 254 (1964), and *New York Times et al. v. Tasini*, 533 U.S. 483 (2001). In 1972, he established the Communications Law Seminar for the Practising Law Institute, enabling media attorneys to learn more about First Amendment law. In addition to his latest book, he is the author of two other books, *The New York Times v. The U.S.* and *All About Cable*, as well as approximately 200 articles that have appeared in a variety of publications ranging from academic journals to newspapers and magazines. His work has earned him the title "father of the reporter's privilege."

A member of the law firm Debevoise & Plimpton LLP since 1980, Goodale also has taught First Amendment and communications law at the law schools of Yale University, New York University and Fordham University. From 1995 to 2010 he produced and hosted the New York metropolitan area public television program "Digital Age," about the effect of digital technology on media, politics, and terrorism. From 1989 to 1994 he served as chairman of the board for the Committee to Protect Journalists, which has been instrumental in the release of imprisoned journalists around the world.

Goodale will conclude the lecture with time to take audience members' questions. Copies of his book will be available for purchase, and a book signing will follow the lecture. This event is free and open to the public. No reservations or tickets are required. The lecture will begin at 7:30 p.m. in Cowles Auditorium on the West Bank Campus of the University of Minnesota in Minneapolis. Parking is available in the 19th and 21st Avenue ramps. Additional information about directions and parking can be found at www.umn.edu/pts.

The Silha Center is based at the School of Journalism and Mass Communication at the University of Minnesota. Silha Center activities, including the annual Lecture, are made possible by a generous endowment from the late Otto Silha and his wife, Helen. For further information, please contact the Silha Center at 612-625-3421 or silha@umn.edu, or visit www.silha.umn.edu.

Elaine Hargrove
Silha Center Staff

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

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

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

TWENTY-EIGHTH ANNUAL SILHA LECTURE

The Lessons of the Pentagon Papers: Has Obama Learned Them?

James C. Goodale

Photo by Laurie Gaboardi, the *Litchfield County Times*

Everyone has heard of the "Pentagon Papers" case, but few are aware of the strategies and tactics, the negotiations and compromises, that took place behind closed doors. The Pentagon Papers case is full of larger-than-life characters from law, politics, journalism and the military who shaped the outcome of one of the most important First Amendment cases in U.S. history.

NSA contractor Edward Snowden's unauthorized leaks of classified information about mass surveillance have reignited the debate over national security versus the public's right to know. Do the government's claims stand up to scrutiny today? Have we learned the lessons of the Pentagon Papers?

Former *New York Times* General Counsel James C. Goodale is the author of a new book, *Fighting for the Press: The Inside Story of the Pentagon Papers and Other Battles*. Copies of his book will be available for purchase at a book signing following the lecture.

October 16, 2013 • 7:30 p.m. - 9:00 p.m.

Cowles Auditorium, University of Minnesota West Bank

A book signing will follow the lecture.