THE SILHA Bulletin

A PUBLICATION OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW | SUMMER 2015

"Right to Be Forgotten" Continues to Develop in the Year Following European High Court Decision

More than a year after the Court of Justice of the European Union's (CJEU) ruled that European citizens retain the right to have Internet search results deleted that link to "inaccurate, inadequate, irrelevant or excessive" information about themselves under the European Union's Data Protection Directive, Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317 (May 13, 2014), available at http://curia.europa.eu/juris/liste.jsf?num=C-131/12, Google continues to grapple with EU member countries over how far the reach of the "right to be forgotten" should extend. At the time of the decision in May 2014, many legal observers suggested that this right to be forgotten could pose serious challenges for online search engines, Internet publishers, and news media organizations (For more on the CJEU's decision, see "European Union Court Holds that Citizens Have the 'Right to Be Forgotten' from Internet Searches" in the Summer 2014 issue of the Silha *Bulletin*). Political and legal debates over the erasure of information found online continued in the United States as well as abroad.

Google Continues to Face Challenges in Europe over the Right to Be Forgotten

According to a July 25, 2014 story by *The Verge*, Google began to comply with the CJEU's order shortly after the May 2014 ruling, removing thousands of links from its search results from European versions of its site in the first few months following the decision. Despite Google's efforts, the Article 29 Working Party, the data protection advisory board for the European Commission, published non-binding guidelines in November 2014 on how search engines should implement the right to be forgotten. The report seemed to suggest that Google was not properly adhering to the European court's ruling.

In the guidelines, the EU advisory board reported that in order for search engines to fully comply with the CJEU's ruling, they must delete links from all their website domains accessible worldwide, not just the EU-related domains, because European users can find simple ways to access non-European sites, such as ".com" websites. Additionally, Article 29 wrote in the report that search engines should not provide disclaimers to users that information may have been deleted nor should search engines inform webmasters that links to their sites have been deleted because there was "no legal basis for such routine communication under EU data protection law." Google had been publishing disclaimers on its own website and informing other webmasters of deleted links. Article 29's full report is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

However, Google pushed back in February 2015 when it published the findings of a panel it had convened, which consisted of industry experts assembled to advise the tech giant on how to implement the CJEU's ruling. The panel's report advised Google that deleting links from only its European domains sufficiently complied with the EU court's rulings. "We believe that delistings applied to the European versions of search will, as a general rule, protect the rights of data subject[s] adequately in the current state of affairs and technology," the panel wrote. "The [panel] supports effective measures to protect the rights of data subjects. Given concerns of proportionality and effectiveness, it concludes that removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling at this stage." Google's report on the implementation of the right to be forgotten is available at https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view.

Although the report indicated there was general consensus among the advisory group, panel member Jimmy Wales, co-founder of Wikipedia, noted his strong opposition to the right to be forgotten. "This report is a good faith effort under the limiting circumstance of the confused and self[-]contradictory European Law to make recommendations to Google on compliance with the law. I am happy that the report explicitly notes 'the Ruling does not establish a general Right to be Forgotten,'" Wales wrote in his comments for the report. "I completely oppose the legal situation in which a commercial company is forced to become the judge of our most fundamental rights of expression and privacy, without allowing any appropriate procedure for appeal by publishers whose works are being suppressed. The European Parliament needs to immediately amend the law to provide for appropriate judicial oversight, and with strengthened protections for freedom of expression."

On Feb. 19, 2015, *The Guardian* reported that a Google official also acknowledged during a London debate in February 2015 that the tech company understood why users might want information removed from searches. "Google has been working

Forgotten, *continued on page 3*

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

COLLEGE OF LIBERAL ARTS
UNIVERSITY OF MINNESOTA

Inside This Issue

Summer 2015: Volume 20, No. 3

The Fall 2014 Silha Bulletin *story "Tenth Circuit Dismisses Claims that News Program Violated Insurance Broker's Civil Rights, Allows Defamation Claims to Proceed" contained factual inaccuracies that were brought to the attention of the Silha* Bulletin *staff. In the original version of the story, the* Bulletin *inaccurately reported that the Tenth Circuit Court of Appeals noted that Tyrone Clark admitted to using scare tactics during training presentations. Clark never admitted to using scare tactics. The three-judge panel acknowledged that Clark could not deny the accuracy of the individual statements that were attributed to him in the presentation, but the panel did not find that Clark ever affirmatively admitted to using scare tactics to sell annuities. The* Bulletin *apologizes for any confusion or misinformation that this mistake may have caused for readers.*

Silha Center Staff

Forgotten, *continued from page 1*

hard to strike the right balance," Google European Director of Communication Peter Barron said. "We certainly accept that there is an issue to be addressed. For us, the whole process has been an exercise in learning and listening and, as [Google CEO] Larry Page has said, to try to see things from a more European perspective." Barron also claimed that Google rejected nearly 60 percent of all requests to delete search links, according to *The Guardian*.

On May 14, 2015, *The Guardian* reported that a letter signed by 80 academics with expertise in technology and data privacy law criticized Google for its lack of transparency on how it was processing deletion requests. Google started publishing transparency reports in October 2014 about users' requests to delete links, but the academics wrote that the limited information Google released was inadequate. Specifically, the scholars called on Google to release detailed data about the types of requests it had received with personally identifiable information redacted.

COVER STORY

"Beyond anecdote, we know very little about what kind and quantity of information is being delisted from search results, what sources are being delisted and on what scale, what kinds of requests fail and in what proportion, and what are Google's guidelines in striking the balance between individual privacy and freedom of expression interests," they wrote. "The [CJEU's] ruling effectively enlisted Google into partnership with European states in striking a balance between individual privacy and public discourse interests. The public deserves to know how the governing jurisprudence is developing. We hope that Google, and all search engines subject to the ruling, will open up." The scholars' letter is available at https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

A Google spokesman said that the company would take the scholars' request for more information under consideration. "We launched a section of our transparency report on these removals within six months of the ruling because it was important to help the public understand the impact of the ruling," the spokesman told *The Guardian* on May 14. "Our transparency report is always evolving and it's helpful to have feedback like this so we know what information the public would find useful. We will consider these ideas, weighing them against the various constraints within which we have to work — operationally and from a data protection standpoint."

Google also continued to face criticism over its handling of the right to be forgotten in June 2015 as France's data protection regulator, the Commission Nationale de l'Informatique et des Liberté ("CNIL"), called on Google to apply the right to be forgotten to all of its global domains. For France, the cause seemed especially pertinent. According to a June 12, 2015 *New York Times* story, French citizens have submitted more than 55,000 requests to Google since 2014. The search engine deleted approximately half of the links in question, but only on the EU-applicable version of Google. In other words, although the search engine deleted the links from country-specific sites — such as Google.de in Germany, or Google.fr in France — it did not remove the same results from Google.com.

Engadget reported on June 12 that CNIL contended that despite Google's current efforts, the delisting was ineffective unless it also involved removing links from "all extensions of the search engine." CNIL threatened to fine the U.S.-based company the Euro equivalent of nearly $340,000 if the French agency's requests were not met. "For Google, the answer is worldwide," said Isabelle Falque-Pierrotin, head of CNIL, in 2014, according to the *Times*' June 12 story. "If people have the right to be delisted from search results, then that should happen worldwide."

The French data protection agency also stated in its press release that it made its order public "to draw the attention of search engine providers and [I]nternet content publishers to the scope of the right to object and to obtain the erasure of personal data." CNIL's June 2015 press release indicated that it would begin the process to impose sanctions on Google if it refused to comply with the order. The French agency's announcement is available at http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/.

> "I completely oppose the legal situation in which a commercial company is forced to become the judge of our most fundamental rights of expression and privacy, without allowing any appropriate procedure for appeal by publishers whose works are being suppressed."
>
> **— Jimmy Wales, Co-Founder of Wikipedia**

Google disagreed with the assertion that search engine results should be deleted across all of its Internet domains. In a July 29, 2015 post on the company's *Europe Blog*, Google's Global Privacy Counsel Peter Fleischer insisted that the company would not follow CNIL's directive, writing, "This is a troubling development that risks serious chilling effects on the web. While the right to be forgotten may now be the law in Europe, it is not the law globally. … As a matter of principle, therefore, we respectfully disagree with the CNIL's assertion of global authority on this issue and we have asked the CNIL to withdraw its Formal Notice." The search engine contended that nearly 97 percent of French Google searches occurred on European versions of the site, rather than on the U.S.-based version of Google.com, indicating that its current implementation of the right to be forgotten was nearly entirely effective. The company further argued that heeding CNIL's request would pave the way for other countries to dictate worldwide censorship on the web. "If the CNIL's proposed approach were to be embraced as the standard for Internet regulation, we would find ourselves in a race to the bottom," Fleischer wrote. "In the end, the Internet would only be as free as the world's least free place."

On July 14, 2015, *The Guardian* reported that less than five percent of the approximately 220,000 requests to delete links that Google had received from users concerned "criminals, politicians, and high-profile public figures." Between May 2014 and March 2015, Google complied with 46 percent of users' requests, according to *The Guardian*. Nearly all of the successful requests were related to "private or personal information." Less than 1 percent of successful requests for deletion were related to reasons involving "serious crime,"

Forgotten, *continued on page 4*

Forgotten, *continued from page 3*

"public figure[s]," "political," or "child protection." *The Guardian* discovered the previously undisclosed data about the requests after it examined source code of Google's online transparency report. However, Google officials told *The Guardian* that the data found in the source code was part of a test on how to best categorize requests, which made it unreliable for publication.

Although the data seemed benign on its face, *The Guardian*'s Julia Powles argued in a July 14 commentary that it undercut many of the arguments made by those who oppose the right to be forgotten. "It is repeatedly claimed that dangerous criminals and shady public figures are using European law to request that Google removes information about them, abusing rights designed to allow individuals some say over personal information that is inaccurate, irrelevant or outdated, and holds no public interest. Internet companies and the media fuel narratives by drawing attention to complex cases involving crime, fraud and politics," Powles wrote. "But new data revealed today by the *Guardian* categorically rebuts assertions that only unsavoury types benefit from rights concerning how we are represented on web searches."

Powles, who signed the May 2015 open letter to Google from the 80 academics, also criticized Google for not being more transparent with data about requests for deletion, suggesting that the company had too much power in overseeing the right to be forgotten. "The fact that this data has only come to light now, and not of Google's own initiative highlights the challenges of having a private multination company such as Google implementing private data rights," Powles wrote. "A widely shared discomfort with last year's European Court of Justice ruling is that it makes Google 'judge, jury and executioner' of our rights."

The Verge reported on Aug. 20, 2015 that Google's troubles continued when the United Kingdom's Information Commissioner's Office (ICO) ordered the company to remove nine links that it had refused to delete after the company deemed the links newsworthy. However, the matter was complicated by the fact that the ICO had ordered Google to remove links from its search results that connected to more recent news stories reporting that Google had removed links to older stories. The ICO wanted Google to remove links from its search engine results to the later stories that identified a specific individual tied to a ten-year-old crime. Google was given 35 days to remove the links to the recent news stories, but the ICO's order, dated Aug. 18, 2015, noted that the tech company had the option to appeal the decision.

"Google was right, in its original decision, to accept that search results relating to the complainant's historic conviction were no longer relevant and were having a negative impact on privacy. It is wrong of them to now refuse to remove newer links that reveal the same details and have the same negative impact," UK Deputy Information Commissioner David Smith said in an August 20 press release. "Let's be clear. We understand that links being removed as a result of this court ruling is something that newspapers want to write about. And we understand that people need to be able to find these stories through search engines like Google. But that does not need to be revealed when searching on the original complainant's name." A Google spokesman said that company would not comment on the ICO's order, according to an Aug. 21, 2015 Bloomberg BNA report. The ICO's order and press release are available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/08/ico-orders-removal-of-google-search-results/.

Despite numerous setbacks and criticisms since the CJEU's May 2014 decision, it does not appear that Google will simply acquiesce to EU officials' demands that the right to be forgotten extend beyond European borders. "While the right to be forgotten may now be the law in Europe, it is not the law globally. Moreover, there are innumerable examples around the world where content that is declared illegal under the laws of one country, would be deemed legal in others: Thailand criminalizes some speech that is critical of its King, Turkey criminalizes some speech that is critical of Ataturk, and Russia outlaws some speech that is deemed to be 'gay propaganda,'" Google Global Privacy Counsel Peter Fleischer wrote in the July 30 post on the company's *Europe Blog*. "We believe that no one country should have the authority to control what content someone in a second country can access."

> "If people have the right to be delisted from search results, then that should happen worldwide."
>
> **— Isabelle Falque-Pierrotin, Head of Commission Nationale de l'Informatique et des Liberté (CNIL), France's data protection regulator**

Right to Erase Personal Information Considered Outside of Europe

Several other countries outside Europe have also been addressing the ability of users to ask various search engines to delete links to their personal information online. On July 14, 2015, Bloomberg BNA reported that Russian President Vladimir Putin signed legislation into law that would essentially grant Russian citizens a right to be forgotten. According to the report, the new Russian law will allow individuals to ask search engines to delete links to any personal information online that is inaccurate or unlawfully published. However, the law does not permit individuals to request that search engines remove links related to webpages about individuals' criminal offenses. The law also does not require any search engines that are operated by municipal and federal authorities to comply with users' requests.

The new Russian law also permits users to sue a search engine if it does not delete links in a timely manner. The new law will go into effect on Jan. 1, 2016. Although Russia has not yet passed a law that would punish search engines for failing to comply with users' requests, Bloomberg BNA reported that the Russian Parliament is considering a bill that would allow the government to fine non-compliant search engines the equivalent of nearly $2,000. Additionally, the bill would permit fines up of approximately $50,000 for search engines who fail to delete links upon receiving a court order to do so.

After the Russian Parliament approved the right to be forgotten legislation, Russia's largest search engine, Yandex, criticized the proposal. "We believe that control over dissemination of information should not restrict free access to public data. It should not upset the balance of personal and public interests," Yandex officials told Reuters in a July 3, 2015 story. "Yandex and other Internet companies have criticized this legislation from the moment we heard about [it]. Unfortunately, many important changes, from our point of view, have not been implemented."

Elsewhere, Hong Kong-based Hogan Lovells attorneys Mark Parson, Eugene Low, and Dominic Edmonson wrote in an Aug. 21, 2015 commentary for Bloomberg BNA that an August 2014 enforcement notice issued by Hong Kong's Privacy Commissioner of Personal Data raised questions of whether individuals residing within the country had a right to be forgotten. The enforcement notice involved David Webb, who ran a website that published information about corporate and economic governance issues in Hong Kong. Webb's website would often publish links to public documents about various corporate individuals, one of which linked to public information about a matrimonial case heard in open court that Hong Kong's Judiciary published online between 2000 and 2002. Several years later, the Judiciary redacted several names in the document. The people named in the edited documents filed a complaint with the Hong Kong Privacy Commissioner's office requesting that Webb also remove the links from his website.

Webb refused to remove the links, resulting in the Privacy Commissioner issuing an enforcement notice that required Webb to delete the information under Data Protection Principle 3 of Hong Kong's Personal Data Privacy Ordinance (PDPO). The principle requires data processors to "use personal data only for the purposes for which it has been collected, or any directly related purpose."

Webb appealed the enforcement notice to Hong Kong's Administrative Appeals Board, which held a hearing on the appeal on July 13, 2015. During the hearing, Webb argued that being required to delete data would create significant precedence problems for access to information. "The information of 'haves' will be in a position of power against the 'have-nots,'" Webb said during the hearing, according to the *South China Morning Post* in a July 13, 2015 story. "We will be creating Orwellian memory holes in society, and even worse, entire media archive may become inaccessible to the public." The board was still considering the appeal in late August 2015.

Parson, Low, and Edmonson noted that the outcome of Webb's case had important implications for privacy in Hong Kong. "The Hong Kong enforcement action against Mr. Webb takes a different line of argument [from the case addressed by the Court of Justice for the European Union] — that the purpose of placing personal data into the public domain may, over time, be discharged at least when the primary publisher of the personal data, in this case the Judiciary, ceases to make information public," the attorneys wrote. "[T]he forthcoming decision in Mr. Webb's appeal will necessarily explore … the clashing of policy interests that arise when the interest in having a free flow of news and information poses challenges for privacy interests. Hong Kong's understanding of rights of privacy has expanded considerably in recent years. These issues are increasingly relevant in Hong Kong as elsewhere, and the decision in Mr. Webb's case will be an important one to watch."

Canadian courts also addressed issues related to the right to be forgotten in 2015. On June 11, 2015, the Court of Appeal for British Columbia dismissed an appeal by Google, which petitioned the appellate court to overturn an injunction preventing search results related to a trademark infringement claim from being accessed worldwide. *Equustek Solutions Inc. v. Google Inc.*, 2015 BCCA 265 (Can.). The case initially arose when Canadian tech company Equustek Solutions won a trademark infringement case against another tech company. In 2012, Equustek Solutions asked Google to remove search engine results that linked to the other tech company's website. Google agreed to remove the links from its Canadian domain but not from search engine results in its other worldwide domains. Equustek then asked for an injunction prohibiting Google from displaying the links in question across all of its domains, which the lower court granted. Google appealed the injunction arguing that the lower court did not have jurisdiction to create such limitations on its search results and that the order had an impermissible extraterritorial reach.

The Court of Appeal disagreed with Google, ruling that the lower court did have jurisdiction to grant an injunction because Google conducted business within the Canadian territory. The appellate court also noted that Canadian courts should consider how such injunctions could limit freedom of expression in other areas of the world, but that for the case at hand, there was likely to be limited impact on expression. The Court of Appeal explained that the links in question were related to information that violated the intellectual property rights of Equustek Solution rather than lawful activity. The appellate court found that the lower court adhered to the proper tests in order to grant the injunction. As a result, the court dismissed Google's appeal.

According to a June 11, 2015 story in *The Globe and Mail*, at least one legal observer expressed his concern over the Court of Appeal's ruling. "I think it's troubling that we see courts and now Canadian courts joining a trend of issuing orders involving the Internet that, by design, have an impact far beyond their jurisdiction," University of Ottawa Law Professor Michael Geist said. "You can see the amount of interest this case generated. … I think there is a view that this represents an important case and sets a pretty important precedent in terms of the scope of these jurisdictions."

However, Borden Ladner Gervais attorney Roberto Ghignone observed in a July 13 post on *The Law of Privacy in Canada Blog* that Canadian courts were being cautious in ordering Google to remove links outside of Canada. In July, a British Columbia court denied a plaintiff's request for Google to delete information from search results across all of its domains that he claimed linked to defamatory information, ruling that he had not met all parts of the test to obtain an injunction. *Niemala v. Malamas*, 2015 BCSC 1024 (Can.). "The importance of search engines in navigating the [I]nternet means that litigants in a variety of cases, including defamation and breach of privacy actions, will increasingly seek remedies against search providers," Ghigone wrote. "The Court's current approach is to consider whether the particular facts of each case warrant its intervention. In future cases, however, Canadian Courts will likely be required to explicitly consider whether there is a right to be forgotten in Canada."

United States Remains Skeptical of the Right to Be Forgotten

Many American scholars and legal observers treated the EU's right to be forgotten with skepticism in the year after the CJEU's May 2014 decision. In an Aug. 5, 2015 interview with *The New York Times*, Center for Democracy and Technology scholar Emma Llansó said that she believed the concept underlying the right to be forgotten was in direct conflict with information access. "When we're talking about a broadly[-]scoped right to be forgotten that's about altering the historical record of making information that was lawfully public no longer accessible to people, I don't see a way to square that with a fundamental right to access to information," Llansó said. In the same story, Harvard Law School Professor Jonathan L. Zittrain said that European efforts to delete Google search results worldwide were "extremely worrisome."

In the United States, news organizations and courts have rebuffed several efforts to allow individuals to demand that

Forgotten, *continued on page 6*

Forgotten, *continued from page 5*

others delete information posted online. For example, *The Washington Post* reported on Oct. 31, 2014, that European pianist Dejan Lazic asked the news organization to delete a critical online review of one of his performances. The *Post* refused to remove the offending article from its website, and then subsequently wrote a new story about Lazic's request containing a link to the original, critical review.

Elsewhere, in late January 2015, a three-judge panel of the U.S. Court of Appeals for the Second Circuit declined to hold a news organization liable for defamation after it refused to remove a story from its website. *Martin v. Hearst Corp.*, 773 F.3d 546 (2d Cir. 2015). A Connecticut woman, who had an arrest record expunged under the state's Criminal Records Erasure Statute, Conn. Gen. Stat. § 54-142a, asked a newspaper to also delete a story about the arrest posted online. When the newspaper refused, the woman sued the news organization for defamation, among other claims. She alleged that any remaining accounts of her arrest were libelous because the erasure statute deemed that the arrest never took place. The appellate court ruled that although the statute allowed individuals to have some official records held by the government deleted, "the statute does not render historically accurate news accounts of an arrest tortious merely because the defendant is later deemed as a matter of legal fiction never to have been arrested." As a result, the panel affirmed a district court's summary judgment in favor of the media defendants.

However, some efforts toward a right to be forgotten in America are taking shape. In June 2015, Google announced that it would begin to allow users to ask that the company remove search result links to revenge porn, which is the distribution of sexually explicit images without the subjects' consent. "This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, that may surface in our search results," Google Search Senior Vice President Amit Singhal wrote in a post on the tech company's *Public Policy Blog*.

In a June 25, 2015 op-ed for *The Guardian*, Professors Woodrow Hartzog and Evan Selinger argued that Google's decision to delete links to revenge porn could be a first step toward an American version of the right to be forgotten. "Google's recent decision to delist 'revenge porn' from its search results is a big deal, and not just for victims," the professors wrote in *The Guardian*. "Beyond opposing harmful conduct that disproportionately targets women, Google has essentially demonstrated how something akin to the European Union's right to be forgotten can, and should, work in the US." The professors also argued that public pressure to encourage Google to voluntarily establish forms so that users could request search result links to be deleted would alleviate any First Amendment concerns related to a government-established right to be forgotten in the United States.

> "Google's refusal to consider [right to be forgotten] requests in the United States is both unfair and deceptive, violating Section 5 of the Federal Trade Commission Act. We urge the Commission to investigate and act."
>
> **— John M. Simpson, Director, Consumer Watchdog Privacy Project**

In July 2015, *The Washington Post* reported that consumer advocacy group Consumer Watchdog filed a complaint with the Federal Trade Commission (FTC) claiming that Google was engaging in unfair and deceptive practices because the company did not permit American Internet users to request that links be deleted from search results. "Google's refusal to consider [right to be forgotten] requests in the United States is both unfair and deceptive, violating Section 5 of the Federal Trade Commission Act," Consumer Watchdog Privacy Project Director John M. Simpson wrote in the complaint. "We urge the Commission to investigate and act."

Specifically, Simpson cited Google's decision to allow users to request the deletion of links to revenge porn. "Google just announced it would honor requests to remove links from its search results to so-called 'revenge porn,'" Simpson wrote. "As clearly demonstrated by its willingness to remove links to certain information when requested in the United States, Google could easily offer the Right To Be Forgotten … request option to Americans. It unfairly and deceptively opts not to do so." As of late August 2015, the FTC had not officially responded to Consumer Watchdog's complaint. The full complaint is available at http://www.consumerwatchdog.org/resources/ltrftcrtbf070715.pdf.

Legislatively, California's "eraser law," Cal. Bus. & Prof. Code § 22581 (West 2015), which would allow minors to remove content that they posted online, went into effect in 2015, but there has been little news of how the law is actually impacting websites, according to an Aug. 4, 2015 *Washington Post* story. The *Post* reported that New Jersey and Illinois have also considered legislation that would require websites to allow minors to delete posts, but neither state has enacted its respective bills. At the Congressional level, Sen. Edward Markey (D-Mass.) and Rep. Joe Barton (R-TX) introduced similar legislation in June 2015 that would allow minors and their parents to request that websites delete the minors' personal information found online. Neither bill has received much consideration.

Despite the tepid development of the right to be forgotten in the United States, American-based privacy advocates continued to remain optimistic about the concept, especially in the wake of France's attempts to require Google to recognize the right to be forgotten across all of its domains. "A global implementation of the fundamental right to privacy on the Internet would be a spectacular achievement," Electronic Privacy Information Center Executive Director Marc Rotenberg, responding to France's efforts, told *The New York Times* in an Aug. 5, 2015 story. "For users, it would be a fantastic development."

Casey Carmody
Silha *Bulletin* Editor

Dillon White
Silha Research Assistant

U.S. Supreme Court Accepts Review of *Robins v. Spokeo, Inc.*

On April 27, 2015, the United States Supreme Court granted *certiorari* in *Spokeo Inc. v. Robins*, a case that could have broad implications for class action lawsuits targeting Internet companies under a number of consumer protection statutes. In *Spokeo*, the Court will decide whether a statutory violation alone, rather than an actual injury, is enough to establish Article III standing for class action litigation.

DATA PRIVACY

Article III of the U.S. Constitution permits the judiciary to hear only "cases" and "controversies," which the Supreme Court has interpreted to mean that a plaintiff must sustain a concrete, non-hypothetical injury-in-fact in order to bring a case or have standing in federal court. The *Spokeo* case asks whether the violation of a plaintiff's statutory rights can suffice to establish such an injury-in-fact entitling the plaintiff to bring the case in federal court absent any allegation of additional harm.

The case arises from a dispute between Spokeo Inc., the operator of a "people search engine" that generates search results about individuals gleaned from publicly available information, and Thomas Robins, one of the individuals who appeared in those results. Robins, the named plaintiff in the class action lawsuit, alleges that Spokeo willfully violated the Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681 *et seq.*, by publishing factually inaccurate information about his age, wealth, marital status, and education as part of Spokeo's online search engine results. The FCRA requires that consumer reporting agencies (CRAs) follow "reasonable procedures to assure maximum possible accuracy of" an individual's information in a consumer report and provides a statutory damages provision for willful violations.

In its brief requesting *certiorari*, Spokeo argued that Robins did not have the right to bring the case because a statutory violation alone without additional proof of an actual harm is not enough to confer Article III standing. Spokeo maintained that Robins only alleges speculative anxiety and concern about what might happen. Robins argued that the alleged statutory violations themselves are a sufficient basis to bring the case.

In 2011, Judge Otis Wright II of the U.S. District Court in Los Angeles dismissed the lawsuit for lack of standing due to no proof of a concrete harm. Robins appealed to the U.S. Court of Appeals for the Ninth Circuit. On Feb. 4, 2014, the Ninth Circuit held that the FCRA is written so that a violation of its procedures is in itself sufficient to establish standing. *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014). "The statutory cause of action does not require a showing of actual harm when a plaintiff sues for willful violations. A plaintiff can suffer a violation of the statutory right without suffering actual damages," wrote Circuit Judge Diarmuid O'Scannlain. The Ninth Circuit's holding joined the Sixth, Tenth and D.C. Circuits in finding that plaintiffs did not need to demonstrate actual harm under the FCRA. However, the Second and Fourth Circuits have found to the contrary.

> "The fear of large civil damages awards, and the mere cost of waging a defense against numerous specious claims, inhibits the development of content by media companies, and thus indirectly chills speech."
>
> **— *Amicus* brief of Time Inc. and other media organizations**

Another key aspect of the case is that the allegedly inaccurate information Spokeo returned on Robins was not necessarily negative on its face, according to Robins' attorney Jay Edelson. The search engine falsely reported that Robins was wealthy, had a graduate degree and was older than his actual age, Edelson said at the Perrin Class Action Litigation Conference held in Chicago on May 6, 2015. But Edelson added that the problems with inaccurate information must be put into context, as it might be detrimental depending on the types of jobs Robins might be seeking. "I don't think standing means that you have to be damaged," Edelson said. "You have to have an interest in a case that is different from your ordinary interest as a civilian." Edelson added that the case could turn on a "minor point" in the complaint: the fact that Spokeo failed to include a toll-free number on its website for people to call and request corrections, which is required under the statute.

On Oct. 6, 2014, the Supreme Court asked the Solicitor General to file a brief on whether the Court should grant *certiorari*. The Solicitor General filed an *amicus* brief on March 13, 2015 urging the Court to deny *certiorari* and leave in place the Ninth Circuit's holding. The Solicitor General's brief, which was coauthored by the Consumer Financial Protection Bureau, argued that the dissemination of inaccurate information in violation of a plaintiff's statutory right is a cognizable injury giving rise to Article III standing, even absent an allegation of any actual harm. The Supreme Court granted *certiorari* despite the Solicitor General's recommendation.

According to attorneys and industry observers, the outcome of the case could be significant for privacy class actions. As a May 1, 2015 post on Davis Wright Tremaine LLP's Privacy and Security noted, Robins would need to show that Spokeo actually harmed his job prospects if the Supreme Court reverses the Ninth Circuit's decision. Each of the class co-plaintiffs in the case would also need to allege and show a concrete-and-particularized injury as well. The Electronic Privacy Information Center (EPIC) contended in its *amicus* brief that "if individuals were required to prove harm in each circumstance, it would become virtually impossible to enforce privacy safeguards in the United States."

However, many observers are concerned that privacy class actions will become more frequent and deter companies from conducting business if the Supreme Court ultimately upholds the Ninth Circuit's ruling. Tech companies such as eBay, Facebook, Google, and Yahoo submitted *amicus* briefs arguing that if the Supreme Court allows the proposed class to go forward without a requirement to show actual harm, virtually every major tech company that provides direct services to consumers could face class action lawsuits comprised of plaintiffs who have not suffered any harm but demand statutory damages for technical violations of federal laws. The U.S. Chamber of Commerce also submitted an *amicus* brief arguing that allowing standing to be based merely on a technical statutory violation that affected a large swath of potential plaintiffs would render the traditional class-certification requirements of commonality and predominance meaningless. Such a decision would invite class action abuse, according to the Chamber of Commerce. The U.S. Chamber of Commerce and other organizations' *amicus* briefs can be found at http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/.

Media organizations also fear that increases in class action lawsuits will have chilling effects on newsgathering

Spokeo, *continued on page 8*

Two Years After Snowden Revelations, National Security Surveillance Issues Still Loom

The files that former National Security Agency (NSA) contractor Edward Snowden provided to Glenn Greenwald and Laura Poitras continued to provide more information in late 2014 and the first half of 2015 about the NSA's surveillance activities.

NATIONAL SECURITY

Two years ago in June 2013, Greenwald and *The Guardian* published the first of what would be several news stories by various media organizations about the NSA's efforts to collect communications worldwide. (For more on Snowden's earlier disclosures, see "Snowden Leaks Reveal Extensive National Security Agency Monitoring of Telephone and Internet Communication" in the Summer 2013 issue of the Silha *Bulletin*, "Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms" in the Fall 2013 issue, "NSA Surveillance Practices Prompt Reforms and Legal Challenges Throughout All Government Branches" in the Winter/Spring 2014 issue, "Fallout from NSA Surveillance Continues One Year After Snowden Revelations" in the Summer 2014 issue, and "Government Surveillance Critics Target Broad Authority of Executive Order 12333" and "29th Annual Silha Lecture Examines the Right to Access Government Information in the Wake of National Security and Privacy Concerns," in the Fall 2014 issue.)

The Intercept's examination of files in the Snowden archive revealed NSA efforts to infiltrate cellular communications throughout the world. Others used the Snowden files to report on AT&T's willingness to cooperate with the NSA. WikiLeaks also published new documents revealing the NSA's efforts to spy on the heads of state for two foreign allies of the United States. However, U.S. lawmakers made several meaningful reforms to the intelligence agency's ability to collect the communications of American citizens.

Snowden Documents Reveal National Security Agency's Efforts to Hack Cellphone Networks Worldwide

On Dec. 4, 2014, *The Intercept* reported that the NSA has been spying on several hundred tech organizations and companies in countries across the globe to exploit security weaknesses in cellphone network technology for surveillance purposes. The investigative journalism website uncovered the program in the archive of documents that Edward Snowden originally leaked in June 2013. *The Intercept*'s story also suggested that the documents about the program to exploit cellphone technology, codenamed AURORAGOLD, showed that the NSA intentionally created security flaws in communications networks to permit easier surveillance. However, at least one security expert argued that *The Intercept*'s claims of the NSA introducing flaws to cellular networks were merely speculative. The report came amid tensions between cellphone tech companies and law enforcement officials over data encryption and stronger protections for cellular communication networks. (For more information on controversies over stronger encryption tools for mobile phones, see "Law Enforcement, Tech Companies Clash on Built-In Privacy Features" in the Fall 2014 issue of the Silha *Bulletin.*)

According to *The Intercept*, two specialist surveillance units within the NSA oversaw the AURORAGOLD program. The first unit, the Wireless Portfolio Management Office, directed the "NSA's strategy for exploiting wireless communications." The second unit, the Target Technology Trends Center, monitored new innovations for communication technologies in order to prevent the NSA from being surprised by improvements that could limit surveillance efforts. The NSA had not previously publicly disclosed the existence of either unit.

Under the AURORAGOLD program, the NSA monitored the e-mails of employees of several cellular communication companies resulting in the collection of technical information about nearly 70 percent of all the world's cellular networks. The NSA also maintained a comprehensive list of "selectors," a search term used to identify information, such as an e-mail address or phone number, in order to monitor the internal communications of the targeted companies. According to *The Intercept*, the NSA sought information related to various selectors between 363 and 1,354 times from November 2011 to April 2012. Upon collecting information, the AURORAGOLD surveillance units forwarded the data to other NSA teams that would attempt to infiltrate the communication networks.

Although the documents in the Snowden archive did not reveal the names of all the specific mobile operator companies that the NSA targeted, *The Intercept* noted that at least one target was the London-based GSM Association (GSMA). The GSMA is a trade association that works with 800 mobile operators and 250 mobile device, software, and Internet companies worldwide. According to the organization's website, members of the GSMA include companies such as Sprint, T-Mobile, AT&T, Verizon, Cisco Systems, Facebook, Intel, Samsung, and Sony, among others. The GSMA has created "working groups" with several member companies to foster discussions among wireless network providers and tech companies about new cellular technologies and policies. *The Intercept* reported that the Snowden documents indicated the NSA specifically targeted these GSMA working groups for surveillance.

Spokeo, *continued from page 7*

and free speech. As an *amicus* brief submitted by Time Inc. and seven other media organizations explained, the increasingly technologically-based media landscape puts media organizations at the mercy of many privacy-related federal statutes. "The fear of large civil damages awards, and the mere cost of waging a defense against numerous specious claims, inhibits the development of content by media companies, and thus indirectly chills speech," the brief argued. "This is especially true in the case of statutes such as the Video Privacy Protection Act, where the delivery of content itself (digital video) may trigger a claim." The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video rental records in a newspaper. The Act is not often invoked, but stands as one of the strongest protections of consumer privacy against a specific form of data collection. Generally, it prevents disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material" and has had increased focus since the rise of digital video streaming services such as Netflix and Hulu.

Many attorneys and organizations anxiously await the Court's decision. As Segal McCambridge Singer & Mahoney trial attorney Brian Eldridge stated at the Perrin Class Action Litigation Conference on May 6, "[*Spokeo*] has the potential to be a tremendous sea change for privacy class actions and class action litigation in general."

Sarah Wiley
Silha Research Assistant

The Intercept also reported on the NSA's efforts to obtain "IR.21s," technical documents that cellphone network operators share among themselves to allow customers to connect to cellular networks in foreign countries. Some IR.21s contain information about a company's encryption process used to secure customers' communications as they travel across different cellular networks. With knowledge of the technical aspects found in the IR.21 documents, the NSA was able to exploit security weaknesses and bypass encryption to eavesdrop on cellular communications. Additionally, the NSA used the IR.21s to stay ahead of new encryption processes and techniques of cellular communication providers.

The Intercept also highlighted one NSA document that questioned whether the agency could "introduce vulnerabilities where they do not yet exist" once vulnerabilities were found in a cellular network. Mikko Hypponen, a security expert with online security and privacy company F-Secure, told *The Intercept* that any NSA efforts to introduce vulnerabilities to cellular networks created a significant security risk. "If there are vulnerabilities on those systems known to the NSA that are not being patched on purpose, it's quite likely they are being misused by completely other kinds of attackers," said Hypponen. "When they start to introduce new vulnerabilities, it affects everybody who uses that technology; it makes all of us less secure."

Cellphone security expert and cryptographer Karsten Nohl shared Hyponnen's concerns over the AURORAGOLD program. "Collecting an inventory [like this] on world networks has big ramifications," Nohl told *The Intercept*. "Even if you love the NSA and you say you have nothing to hide, you should be against a policy that introduces security vulnerabilities, because once NSA introduces a weakness, a vulnerability, it's not only the NSA that can exploit it."

However, in a Dec. 9, 2015 blog post on *Schneier on Security*, data security expert Bruce Schneier was skeptical about *The Intercept*'s claims that the NSA was creating new security vulnerabilities for cellular networks. "*The Intercept* points to the [archived Snowden documents] as an example of the NSA deliberately introducing flaws into global communications standards, but I don't really see the evidence here. Yes, the NSA is spying on industry organizations like the GSM Association in an effort to learn about new GSM standards as early as possible, but I don't see evidence of it influencing those standards," Schneier wrote in his post. "The one relevant sentence is in a presentation about the 'SIGINT [signals intelligence] Planning Cycle': 'How do we introduce vulnerabilities where they do not yet exist?' That's pretty damning in general, but it feels more aspirational than a statement of practical intent."

Nonetheless, Schneier did argue that *The Intercept*'s report was troubling news. "This is not a typical NSA surveillance operation where agents identify the bad guys and spy on them," Schneier wrote. "This is an operation where the NSA spies on people designing and building a general communications infrastructure, looking for weaknesses and vulnerabilities that will allow it to spy on the bad guys at some later date."

> "This is not a typical NSA surveillance operation where agents identify the bad guys and spy on them. This is an operation where the NSA spies on people designing and building a general communications infrastructure, looking for weaknesses and vulnerabilities that will allow it to spy on the bad guys at some later date."
>
> **— Bruce Schneier, Data security expert**

Schneier went on to note, "As I keep saying, we no longer live in a world where technology allows us to separate communications we want to protect from communications we want to exploit. Assume that anything we learn about what the NSA does today is a preview of what cybercriminals are going to do in six months to two years. That the NSA chooses to exploit the vulnerabilities it finds, rather than fix them, puts us all at risk."

The NSA declined to specifically comment on *The Intercept*'s report about the AURORAGOLD program. In a December 4 e-mailed statement to *CNET*, NSA spokeswoman Vanee Vines wrote, "NSA collects only those communications that it is authorized by law to collect in response to valid foreign intelligence and counterintelligence requirements — regardless of the technical means used by foreign targets, or the means by which those targets attempt to hide their communications. Terrorists, weapons proliferators, and other foreign targets often rely on the same means of communication as ordinary people. In order to anticipate and understand evolving threats to our citizens and our allies, NSA works to identify and report on the communications of valid foreign targets." Additionally, Vines declined to comment to *The Intercept* on whether AURORAGOLD was still an active program.

American and British Spy Agencies Reportedly Sought Crucial Encryption Information for Cellular Phones Worldwide

On Feb. 19, 2015, *The Intercept* reported that documents leaked by Edward Snowden revealed that the NSA and the British Government Communications Headquarters (GCHQ) had hacked into the internal computer databases of the world's largest manufacturer of subscriber identity module (SIM) cards, which contain small computer chips that allow mobile phones to securely connect to cellular networks. After hacking the computer networks, the spy agencies allegedly attempted to acquire encryption keys for the computer chips that would allow the NSA and GCHQ to decrypt mobile communications secretly without ever needing to seek approval from any legal authority. *The Intercept* reported that data security experts and privacy advocates had noted that the NSA and GCHQ's actions were "tantamount to a thief obtaining the master ring of a building superintendent who holds the keys to every apartment."

According to *The Intercept*, a set of NSA and GCHQ operatives, called the Mobile Handset Exploitation Team (MHET), secretly accessed the e-mail and Facebook accounts of employees at several major technology companies in order to gain more information about SIM card encryption keys. One of the companies that the team targeted was Netherlands-based Gemalto, the world's largest producer of SIM cards whose clients include Verizon, AT&T, T-Mobile, and Sprint, among several other wireless carriers around the world. In a Feb. 20, 2015 story, *The Guardian* reported that Gemalto manufactures nearly 2 billion SIM cards each year for approximately 450 different mobile phone companies across 85 countries. Essentially, nearly every cellular phone provider has used Gemalto-produced SIM cards at some point, according to *The Guardian*.

The Intercept reported that although not originally designed for encryption purposes, SIM cards play an important role in authenticating users' phones and encrypting messages on cellular commu-

Surveillance, *continued on page 10*

Surveillance, *continued from page 9*

nication networks. The card contains a small computer chip that is inserted into a mobile phone. The chip often stores data such as a phone's contacts list, text messages, and phone number. Each chip also contains a unique encryption key that is burned directly onto the chip. Once in the phone, the SIM card uses the individualized key to create an encrypted connection between the cellular phone and the cellular service provider's wireless network. However, cellular phone providers typically outsource the production of SIM cards to other companies. As a result, the SIM card manufacturer must provide a file containing every encryption key to the cellular phone provider in order for the connections between phones and wireless networks to work.

The GCHQ and NSA sought specifically to intercept the files containing encryption keys when Gemalto transferred them to cellular service providers because access to the keys meant the agencies could easily decrypt cellular communications. *The Intercept* reported that the GCHQ identified important Gemalto employees who might have access to the company's primary internal computer system and SIM card encryption keys. The British spy agency then created automated processes to collect file transfers and e-mails that were sent between the targeted Gemalto employees and cellular service providers, despite the fact that large amounts of personal communications would be collected. The leaked top-secret documents indicated that the GCHQ's automated process had collected millions of encryption keys during a three-month period in 2010 alone. Another document also revealed that the NSA had the ability to process between 12 and 22 million encryption keys per second in 2009. The agency believed it would eventually be able to process 50 million keys per second for use against surveillance targets.

If the agencies had obtained encryption keys, the NSA and GCHQ would have fewer barriers to overcome in order to spy on individuals' communications, according to *The Intercept*. The intelligence agencies could conduct passive bulk collections of encrypted communication data sent from wireless devices to wireless networks. Once collected, the NSA and GCHQ only needed to match the encrypted data from devices with the encryption keys in order to decrypt the communications. Additionally, *The Guardian* reported on February 20 that access to encryption keys would enable the NSA and GCHQ to examine mobile communications without the knowledge or approval of any other government entities or wireless communication companies.

"Key theft enables the bulk, low-risk surveillance of encrypted communications," ACLU Principal Technologist Christopher Soghoian told *The Intercept* in the February 19 story. "Agencies can collect all the communications and then look through them later. With the keys, they can decrypt whatever they want, whenever they want. It's like a time machine, enabling the surveillance of communications that occurred before someone was even a target."

Gemalto was not the only target of the NSA and GCHQ. *The Intercept* reported that the GCHQ had used the NSA's XKeyscore program, which Glenn Greenwald wrote in 2013 "allows analysts to search with no prior authorization through vast databases containing emails, online chats, and the browsing histories of millions of individuals," to access private e-mails of employees at several other SIM card manufacturers, wireless network operators, and tech companies like Google and Yahoo. As a result, the encryption processes of many other types of SIM cards that were not produced by Gemalto might be compromised. *The Intercept* noted that the revelations suggest that the only way to secure mobile communications from NSA and GCHQ surveillance would be through encryption software that goes beyond SIM card encryption.

> "Key theft enables the bulk, low-risk surveillance of encrypted communications. Agencies can collect all the communications and then look through them later. With the keys, they can decrypt whatever they want, whenever they want."
>
> **— Christopher Soghoian, Principal Technologist, American Civil Liberties Union**

Data security experts and digital privacy advocates expressed significant concern over the revelations that the NSA and GCHQ had possibly obtained SIM card encryption codes. Electronic Frontier Foundation staff attorney Mark Rumold told *The Guardian* on February 19 that U.S. and British intelligence agencies had likely broken Dutch law if they had stolen encryption keys from Gemalto. He also noted that the problem was not limited to only the United States and the United Kingdom. "They have the functional equivalent of our house keys," Rumold said. "That has serious implication for privacy not just here in the US [*sic*] but internationally."

Data security expert Bruce Schneier told British tech-news website *The Register* on February 19 that *The Intercept*'s report was surprising. "Wow. This is huge — it's one of the most significant findings of the Snowden files so far," he said. "We always knew that they would occasionally steal SIM keys. But *all* [*sic*] of them? The odds that they just attacked this one firm are extraordinarily low and we know the NSA does like to steal keys where it can."

Johns Hopkins University Information Security Institute cryptologist Matthew Green told *The Guardian* on the same day that the news of the intelligence agencies' attempts to intercept encryption keys was troubling for several reasons. "It's a big breach. The problem is that the attacks could still be ongoing," Green said. He also noted that the number of encryption keys that might have been compromised meant that any SIM card replacement process was going to be difficult. "Suppliers are going to have to tighten up their practices before anyone can think about fixing this, and that's going to be a nightmare," he said.

The Intercept also reported that GCHQ would not provide specific comments about any operations to secretly obtain SIM card encryption keys other than stating in an e-mail that the agency completes its operations within "a strict legal and policy framework." The NSA declined to provide any comment.

Survey Reports Suggest American Citizens, Journalists Suspicious of Government Spying

Two years after Edward Snowden's disclosure of classified documents about secret U.S. government spying, several studies have shown that surveillance issues continue to concern Americans. Surveys conducted by the Pew Research Center have found that many Americans are suspicious of government spying and have undertaken efforts to try to keep their communications private. A survey of journalists has also indicated that they are concerned about being specifically targeted for government spying.

In November 2014, the Pew Research Center published a report of its findings from a national survey detailing that a significant percentage of Americans were aware of and still had concerns over

government surveillance more than a year after Snowden's initial disclosures. According to the report, approximately 87 percent of adults had either heard "a lot" or about "a little" on "the government collecting information about telephone calls, emails, and other online communications as part of efforts to monitor terrorist activity." Only five percent of adults said that they had heard nothing at all about various government surveillance programs. Americans who had heard "a lot" about government surveillance programs also tended to believe that various communication tools, such as e-mails, text messages, cell phone calls, and social media websites, were not secure channels to share private information.

Additionally, 80 percent of adults "agreed" or "strongly agreed" that Americans should be concerned about widespread government surveillance of phone calls and Internet communications as compared to 18 percent of adults who either "disagreed" or "strongly disagreed." The survey also found that only 36 percent of Americans "agreed" or "strongly agreed" that it is beneficial for a society when people believe the government is watching online activity. The Pew Research Center's full November 2014 report is available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

In March 2015, the Pew Research Center released a separate report highlighting various privacy strategies that Americans had used after the Snowden document leaks. According to the report, 34 percent of adults who had heard of government surveillance programs had taken at least one step to shield information from the U.S. government, including changing privacy settings on social media, communicating more often in person rather than online or over the phone, and avoiding specific terminology while communicating online. Approximately 25 percent of the surveyed adults told the Pew Research Center that they had changed how they used various online platforms either "somewhat" or "a great deal" in response to the information found in Snowden's disclosure of classified documents. The most prominent changes in technology use involved changing behaviors related to e-mail, search engines, social media websites, and cellular phones.

However, the March 2015 report also indicated that a large portion of Americans had not adopted basic security processes to make their Internet activities more private. One significant reason was that 54 percent of adults believed that it would be "somewhat" or "very" difficult to find the tools needed to secure online communications. Many Americans also had not adopted basic tools that create more privacy online, such as e-mail encryption, using search engines that do not track user's histories, or privacy-enhancing web browser plug-ins. The full March 2015 report is available at http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

The Pew Research Center published an additional report in February 2015 detailing investigative journalists' perceptions of government surveillance. Of the journalists surveyed for the report, 64 percent said they believed that the U.S. government had probably collected information about their phone calls, e-mails, or online interactions. Investigative journalists who cover national security issues were even more likely to indicate that they believed their communications had been targeted for surveillance. Approximately 70 percent of investigative journalists said that they thought the government had likely collected information about their work.

These suspicions have altered the way that many journalists conduct their investigations. About half of the surveyed journalists said they have somewhat changed the way they store and share sensitive documents. Twenty-nine percent of journalists also noted that they had changed how they communicated with other reporters, editors, and producers, while 38 percent of reporters had altered their processes for communicating with sources. Only 14 percent of journalists said that their suspicions about surveillance had prevented them from pursuing a story or leaving the profession altogether. The Pew Research Center's February report is available at http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

Taken as a whole, the reports suggest that the Snowden disclosures have brought U.S. government surveillance into the central consciousness of both journalists and American citizens. Many Americans have taken steps to shield their online communications from the government, but many could still make greater efforts to employ basic data security tools. Investigative journalists are also particularly suspicious of U.S. government spying but remain undeterred in their pursuit of informed reporting.

USA Freedom Act Reforms Key Aspects of U.S. Surveillance

On June 2, 2015, *The Washington Post* reported that President Barack Obama signed the USA Freedom Act into law, which placed significant limitations on U.S. national security surveillance tools created in the wake of the terrorist attacks on Sept. 11, 2001. The law prescribes new regulations for the bulk collection of Americans' phone records and requires the Foreign Intelligence Surveillance Act (FISA) Court to declassify many significant decisions. USA Freedom Act of 2015, Pub. L. No. 114-23 (2015). The law received bi-partisan support but faced significant opposition from several Republican leaders in the U.S. Senate. The reforms came nearly two years after Edward Snowden disclosed documents revealing several of the NSA's secret surveillance programs.

Specifically, the USA Freedom Act halted the bulk collection of Americans' telephony metadata records under Section 215 of the USA PATRIOT Act, 115 Stat. 272 (2001). All metadata records will remain in the hands of telecommunication companies, which often retain the information for varying lengths of time. Government authorities could still access metadata records so long as an investigation is relevant to national security and they first obtain an order from the FISA court, according to a June 2 story by *Wired*. The USA Freedom Act directed the FISA court to appoint an *amicus curiae* panel to provide the court with guidance on issues related to the protection of individuals' privacy and civil liberties. The law also ordered the Director of National Intelligence to declassify any FISA court decision "that includes a significant construction or interpretation of any provision of law." The new law also extended the expiration date of several provisions of the PATRIOT Act, including Section 215, to 2019.

The New York Times reported on April 28, 2015 that Reps. Jim Sensenbrenner (R-Wisc.), Bob Goodlatte (R-Va.), John Conyers (D-Mich.), and Jerry Nadler (D-N.Y.) had introduced the bill in the House of Representatives. The House Judiciary Committee approved the bill on April 30 with a 25-2 vote before the entire House voted overwhelmingly in favor of it with a bipartisan 338-88 vote on May 13, according to a *Times* story on the same day as the full House vote.

However, the *Times* reported that an identical bill introduced in the U.S. Senate faced a much more significant challenge due to opposition from Senate Majority Leader Mitch McConnell (R-Ky.) and other Republican Senators who insisted that any changes to the PATRIOT Act could damage national security. Other Republican senators, including Sen. Rand Paul (R-Ky.), argued that the bill needed to include more restrictions in order to create stronger privacy protections for U.S. citizens. Senate Democrats were nearly unanimous in their support for the bill. The U.S. Court of Appeals for the Second Circuit further complicated the debate after it ruled that

Surveillance, *continued on page 12*

Surveillance, *continued from page 11*

Section 215 did not authorize the bulk collection of telephony metadata. *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. May 7, 2015).

The debate over the USA Freedom Act among Senate Republicans led to procedural posturing by both Sens. McConnell and Paul, which delayed a vote on the bill and resulted in the temporary expiration of sections of the PATRIOT Act on June 1. The Senate then approved the bill on a 67-32 vote on June 2, with 23 Republicans joining 43 Democrats and one Independent, Sen. Angus King (I-Maine), according to *The Washington Post*'s June 2 story. *The Guardian* reported that other senators, including Paul and Bernie Sanders (I-Vt.), voted against the bill because they believed the bill did not go far enough in restricting surveillance. Obama signed the bill into law the same day as the Senate's approval.

Privacy advocates praised the passage of the USA Freedom Act. In a June 2 post on the Electronic Frontier Foundation's (EFF) *Deeplinks* blog, EFF Executive Director Cindy Cohn and Activism Director Rainey Reitman wrote, "Technology users everywhere should celebrate, knowing that the NSA will be a little more hampered in its surveillance overreach, and both the NSA and the FISA court will be more transparent and accountable than it was before the USA Freedom Act."

However, Cohn and Reitman also noted that the new law could have been better. "It's no secret that we wanted more. In the wake of the damning evidence of surveillance abuses disclosed by Edward Snowden, Congress had an opportunity to champion comprehensive surveillance reform and undertake a thorough investigation," they wrote. "Congress could have tried to completely end mass surveillance and taken numerous other steps to rein in the NSA and FBI." Cohn and Reitman also noted that the EFF withdrew their support from the bill in "an effort to spur Congress to strengthen some of its privacy protections."

Meanwhile, national security proponents expressed concern that the USA Freedom Act would prove to be problematic for U.S. surveillance efforts. Former NSA General Counsel Stewart Baker told *The Washington Post* on June 2 that the new law was sending a troubling message. "It is going to make the National Security Agency risk-averse in ways that the CIA has occasionally been risk-averse," Baker said. "They followed the rules. They believed they were following the rules, and they got punished nonetheless."

WikiLeaks Publishes Documents Detailing U.S. Spying on Foreign Leaders

On June 23, 2015, WikiLeaks published documents on its website containing evidence of U.S. spying on several French presidents. According to a June 24 story by *The Guardian*, the documents showed that the NSA had recorded phone conversations of former presidents Jacques Chirac and Nicolas Sarkozy as well as current French President François Hollande. The documents also suggested that the NSA had targeted other French officials, including cabinet ministers and an ambassador to the United States. The Associated Press (AP) reported the same day that the recorded conversations included discussions about a United Nations appointment, the Middle East peace process, and frustration over U.S. officials' reluctance to sign an international pact limiting espionage, among other topics. WikiLeaks spokesman Kristinn Hrafnsson told the AP that the documents were authentic but declined to explain how the organization obtained the information.

The reports detailing the NSA's surveillance of French leaders prompted Hollande to call the revelations "unacceptable" and to hold emergency meetings with intelligence officials to discuss the documents, according to a June 24 *New York Times* story. *The Washington Post* reported that U.S. President Barack Obama had a phone conversation with Hollande to reassure the French president that no further espionage had taken place since an earlier 2013 commitment to halt spying on foreign leaders. U.S. Ambassador Jane Hartley was also called to the French Foreign Ministry to explain the contents of the documents.

French officials condemned the NSA's actions. "If the fact of the revelations today does not constitute a real surprise for anyone, that in no way lessens the emotion and the anger. They are legitimate," French Prime Minister Manuel Valls said, according to *The Washington Post*. "France will not tolerate any action threatening its security and fundamental interests." However, French government spokesman Stephane Le Foll said that the revelation of spying would not disrupt diplomatic relations between the two countries.

On July 31, 2015, *The Washington Post* reported that WikiLeaks published additional documents indicating that the NSA had also spied on the phone calls of prominent Japanese government and business officials. According to Wikileaks, the NSA had targeted 35 phone numbers for surveillance since 2006, including the phone numbers for the office of Prime Minister Shinzo Abe, the Japanese finance and trade ministries, and Mitsubishi's natural gas division, among others. The documents indicated that the NSA spied on Japanese officials' conversations about talking points for U.S.-Japan trade negotiations over agricultural issues as well as climate-change talks. WikiLeaks also said that NSA designated one of the top-secret documents to be distributed among the United States' "Five Eyes" intelligence alliance, which includes Australia, Britain, Canada, and New Zealand.

Japanese officials did not comment at length about the revelations of U.S. spying. Japanese Foreign Ministry press secretary Yasuhisa Kawamura told the AP on July 31 that American and Japanese government officials had been in contact about the news of NSA spying. He declined to elaborate on the specifics of the conversations, but said, "Japan will continue to employ all the necessary measures to protect [its] information."

The AP later reported on August 4 that Vice President Joe Biden had made a phone call to Prime Minister Abe to tell the Japanese official that the U.S. remained committed to President Obama's 2013 promise to cease spying on allied leaders. The Japanese prime minister's office told the AP that Abe had said that he expected the United States to investigate the claims made in the documents. He also told Biden that if the allegations were true, trust between the two countries could be damaged.

The United States has faced similar embarrassment in the past over the disclosure of the NSA's spying on foreign leaders. In 2013, documents disclosed by Edward Snowden showed that United States' efforts to conduct espionage on German Chancellor Angela Merkel, which prompted investigations by a German federal prosecutor. Government officials in Brazil and India also complained in 2013 after Snowden's disclosure of classified documents contained files that showed the NSA had spied on telephone conversations of key government leaders. (For more information on the NSA's surveillance of other foreign leaders, see International Outrage Continues over Snowden Leaks in "Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms" in the Fall 2013 issue of the Silha *Bulletin*.)

Snowden Documents Reveal Telecom's Willingness to Assist NSA

On Aug. 15, 2015, *The New York Times* and ProPublica reported that documents leaked by Edward Snowden in 2013 revealed that telecommunications company AT&T has had a close relationship with the NSA for several decades. The partnership, which the intelligence agency described as "highly collaborative," has resulted in

AT&T providing the NSA access to the metadata for billions of phone calls and e-mails sent domestically as well as Internet communications worldwide. Privacy advocates have pointed to the reports as further evidence that many telecommunications companies are willing participants in the surveillance of American citizens.

According to the *Times* and ProPublica, the partnership between the NSA and AT&T, codenamed "Fairview," began in 1985. During the course of several decades, AT&T willingly turned over communications flowing across its network to the NSA. Shortly after the terrorist attacks on Sept. 11, 2011, AT&T began to turn over e-mails and phone calls to the NSA under warrantless surveillance programs beginning in October 2001. Documents indicated that in September 2003, AT&T became the first telecommunications company to initiate a new data collection program that the NSA described as a "'live' presence on the global net." The new program allowed AT&T to send the NSA approximately 400 billion Internet metadata records in its first months of operation.

AT&T also began providing the NSA with nearly 1.1 billion domestic cellphone calling records in 2011. This revelation countered NSA's previous claims that it had collected only domestic landline phone records when Snowden revealed that the intelligence agency was collecting American citizens' phone records. AT&T also provided the NSA access to the contents of e-mails sent between foreign individuals that traveled across its American Internet cables. However, the documents from Snowden indicated that the NSA did not typically receive Internet data en masse from AT&T. Rather, the telecom company sifted through communications before providing messages to the NSA that the agency might have been able to collect legally.

The documents revealed that other telecommunication companies, such as Verizon, have also provided communications to the NSA, but the agency's relationship with AT&T appeared to be unique. The *Times* and ProPublica reported that the NSA's budget for the partnership with AT&T was twice that of the next-largest program. NSA documents instructed agency officials to be polite during visits to AT&T facilities because "[t]his is a partnership, not a contractual relationship." Another document complimented AT&T for its "extreme willingness to help" with NSA surveillance efforts.

Although the NSA's documents never specifically used the name of AT&T, the *Times* and ProPublica reported that they were able to determine that the telecom company was the partner in the Fairview program through a "constellation of evidence." ProPublica reported that information contained in the documents noted that the Fairview program partner needed to repair an underwater cable in the Pacific Ocean that was damaged during the Japanese earthquake of 2011, which was the same cable that belonged to AT&T according to Federal Communications Commission (FCC) filings. Another document contained technical jargon that was specific to AT&T, as confirmed by former employees of the company. ProPublica also noted that an internal NSA newsletter described the successful efforts of Fairview engineers spying on Internet communications at the United Nations headquarters in New York City. A spokesman for the United Nations later confirmed to reporters that AT&T managed the organizations' fiber optic network at its headquarters. Additionally, documents that detailed the locations of Fairview's submarine telecommunications cables' landing points in the United States corresponded with AT&T's descriptions of its landing points as documented in FCC filings. Several former intelligence officials also confirmed the *Times*' and ProPublica's suspicions that the Fairview program involved AT&T.

After the *Times* and ProPublica's report was published, privacy advocates criticized AT&T and the NSA for hiding their close working relationship. According to an Aug. 15, 2015 post on the organization's *Deeplinks* blog by Mark Rumold, Electronic Frontier Foundation (EFF) Executive Director Cindy Cohn said, "It's long past time that the NSA and AT&T came clean with the American people. It's also time that the public U.S. courts decide whether these modern general searches are consistent with the Fourth Amendment's guarantee against unreasonable search and seizure."

Rumold noted in the blog post that the report from the *Times* and ProPublica was crucial to one of the EFF's ongoing lawsuits against the NSA. The organization's case, *Jewel v. NSA*, was filed on behalf of several AT&T customers and challenged the constitutionality of NSA programs that collected the telephone and Internet communications of American citizens. *Jewel et al. v. NSA et al.*, No. 08-cv-4373-JSW (N.D. Cal. filed Sept. 18, 2008). However, in February 2015, a judge for the U.S. District Court for the Northern District of California dismissed the plaintiffs' challenges to the constitutionality of an NSA program because it could result in the disclosure of classified information, which could potentially harm national security. The federal district court also ruled that the plaintiffs lacked standing to challenge the NSA's bulk collection of Internet communications because they could not prove that surveillance had actually taken place. The EFF appealed the federal district court's decision, which was still under consideration by the United States Court of Appeals for the Ninth Circuit when the *Times* and ProPublica published their story. *Jewel et al. v. NSA et al.*, No. 08-cv-4373-JSW, 2015 U.S. Dist. LEXIS 16200 (N.D. Cal. Feb. 10, 2015), appeal docketed, No. 15-16133 (9th Cir. June 4, 2015).

"These reports are just the latest in a long line of evidence demonstrating AT&T's deep involvement in the NSA's surveillance programs," Rumold wrote in the *Deeplinks* post. "Although the cat has been out of the bag for years now, the government still pretends that AT&T's participation in its programs is a classified 'state secret,' and has used that claim to repeatedly attempt to convince the courts to dismiss *Jewel*, EFF's lead case against the Internet surveillance. *Jewel* is now on appeal to the Court of Appeals for the Ninth Circuit, and these reports show once again the futility of the government's efforts to delay consideration of the NSA's activities."

According to the *Times* and ProPublica, the documents outlining the Fairview program did not indicate whether the NSA and AT&T partnership was still ongoing. Spokespeople for the NSA and AT&T declined to provide much comment to the news organizations about the relationship. "We don't comment on matters of national security," an AT&T spokesman told the news organizations.

Casey Carmody
Silha *Bulletin* Editor

Major Data Breaches for Government, Private Companies Create Problems in 2015

DATA PRIVACY

On June 4, 2015, the Office of Personnel Management (OPM), the independent government agency tasked with managing Federal civil service, announced that it had been a victim of a data breach impacting the personnel data for nearly 4.2 million current and former federal employees. In a June 4 press release, OPM revealed it discovered the breach during its "aggressive effort to update its cybersecurity posture" in April 2015. The agency then partnered with the U.S. Department of Homeland Security's Computer Emergency Readiness Team (CERT) and the Federal Bureau of Investigation (FBI) to determine the extent of the intrusion. The results exposed an even larger breach.

OPM later disclosed in a July 9 press release, that a "separate but related" breach compromised the information of 21.5 million federal employees, contractors, employment applicants, and family members. Stolen information included "identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history … fingerprints … [and] usernames and passwords." William R. Dougan, the National President of the National Federation of Federal Employees, called the breach "staggering" in a July 9 press release, noting that "not only do federal employees have to worry about their own personal information … but they must also [now] worry about their spouse[s] and children having their information compromised."

Congressional leaders, including some whose information was compromised in the hack, called for the resignation of OPM leadership immediately following the announcement of the first breach. "Since at least 2007, OPM leadership has been on notice about the vulnerabilities to its network and cybersecurity policies and practices," said House Oversight Chairman Jason Chaffetz, (R-Utah) in a July 9 statement. "[OPM] Director [Katherine] Archuleta and [Chief Information Officer Donna] Seymour consciously ignored the warnings and failed to correct these weaknesses … Such incompetence is inexcusable." OPM Director Katherine Archuleta resigned the following day, according to *The New York Times* on July 10, 2015.

ABC News reported on June 15, 2015, that authorities suspected Chinese hackers accessed the OPM system through KeyPoint Government Solutions, one of the primary background check providers for federal employees. However, the government has not publicly blamed the Chinese for the attack, at least in part because of a reluctance to reveal evidence, according to *The Washington Post* on July 21. Exact details were still unknown, but authorities believed the hackers stole electronic credentials from KeyPoint to "somehow use them to … unlock OPM's systems" and that they accessed records for more than a year. On August 14, Reuters reported that the seventh class action suit was filed against OPM and KeyPoint, most of which claimed violations of the Privacy Act and Administrative Procedures Act. The Judicial Panel on Multidistrict Litigation (JPML) was expected to consolidate the suits. Though the final venue is uncertain, experts believed the cases will boil down to constitutional standing, per the 2013 Supreme Court decision in *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013), which held that a reasonable likelihood that communications would be intercepted is not sufficient to show injury and thus standing. (For more on Clapper, see "U.S. Supreme Court Rejects Challenge to Federal Surveillance Law" in the Winter/Spring 2013 issue of the Silha *Bulletin*.)

The case was expected to be complicated. On June 15, 2015, the head of the Department of Homeland Security's cyber response team Ann Barron-DiCamillo told ABC News that the scope of the breach had become increasingly muddled, due to the erasure of the hackers' digital trail. Since the breach, "information that would [have] point[ed] to how many people inside and outside of government [had] been affected … [had been] simply lost," Barron-DiCamillo told ABC News. Although many government computer systems save the records of accessed files for two months, the time that passed between the breach and OPM's discovery caused much of the data to disappear.

OPM's handling of the two breaches called into question the government's ability to defend against cybersecurity attacks, and Congressional leaders urged other agencies to re-examine their own systems. "Every other agency should have its head examined if it's not taking steps to protect its data," House Intelligence Committee member Adam Schiff (D-Calif.) told *The New York Times* on July 10, 2015. "Because if there's a problem at one agency, there's likely a problem at other agencies." Other government officials acknowledged the cybersecurity weaknesses in the federal bureaucracy, and though Josh Earnest, President Obama's spokesperson, stated in a July 10 press briefing that the White House was rushing to conduct a rapid reassessment of cybersecurity measures, such as seeking to implement more advanced authentication systems and increased monitoring, the *Times* reported that the cost of eventually executing such a fix was unknown.

However, experts believed the problem to be more endemic than cost. *The Washington Post* reported on July 19 that the federal government is experiencing a cybersecurity skills gap, losing much of the nation's top talent to the private sector as a result of lackluster recruiting efforts, resulting in a "serious shortage of cyber talent" and a "dim future." The Government Accountability Office (GAO) agreed. In a 2015 report on high-risk areas for the nation's agencies and programs, the GAO stated, "Although steps have been taken to close critical skills gaps in the cybersecurity area, it remains an ongoing problem, and additional efforts are needed to address this issue government-wide." According to *The Washington Post*'s July 9 story, U.S. Chief Information Officer Tony Scott echoed the concern to the National Council on Federal Labor-Management Relations in mid-July, saying, "It's the hardest recruiting that there is on the planet today … We're going to have to take extraordinary moves to try to develop a broader set of talent and skill base in that area."

Data Breach Problems Continued to Grow Throughout 2015

The OPM breaches were only two among many during a tumultuous seven months for cybersecurity. In its *Data Breach Report* published on Aug. 18, 2015, the Identity Theft Resource Center reported 505 data breaches between January and August 2015. Leading the targets was the healthcare industry, whose principal breach came in January 2015 from health insurance company Anthem, Inc. (Anthem). On Jan. 29, 2015, Anthem announced in a press release that "cyber attackers executed a sophisticated attack to gain unauthorized access to [its] IT system and obtained personal information." However, the *Los Angeles Times* reported on March 6 that the breach was not as sophisticated as Anthem suggested. The insurance company neglected to "encrypt the huge volume of personal information it held." Hackers used simple phishing techniques — sending emails encouraging individuals to reveal network IDs or passwords — to access the credentials of approximately five employees. At its core, the Anthem breach, like many others,

seemed to be as much a people problem as it was a system problem. Cybersecurity expert Steve Ragan noted in a February 9 post on CSO that "technical controls will only go so far. Once the humans are exploited, those controls are next to useless. Behavioral controls and monitoring can help flag a compromised human element, but it isn't an exact science … Self-awareness among the staff is a serious bonus to any information security program."

That self-awareness seems sparse in the cybersecurity world. On Aug. 17, 2015, the Internal Revenue Service (IRS) revealed that more than 334,000 user accounts were hacked through its "Get Transcript" application, a program for consumers to retrieve information about their tax returns — along with an additional 170,000 "suspected failed attempts to access the application." A week prior, on Aug. 7, 2015, an anonymous source in the Defense Department told NBC News that Russian hackers illegally accessed the e-mail system of the Pentagon's Joint Chiefs of Staff. Although the identity of the hackers was unknown, the source reported that the incident was "clearly the work of a state actor." On July 7, 2015, CVS and Walmart Canada announced that a breach at a Canadian IT vendor may have leaked millions of credit card numbers from its online photo processing site. "This year, there's no sign of let-up," wrote cybersecurity journalist Zach Whittaker in an August 14 article on *ZDNet*. "The chances are [that] your data was leaked this year."

Several of these leaks have already resulted in tangible harm. On Aug. 12, 2015, the Federal Trade Commission accused two data-brokerage firms, Sequoia One LLC and Gen X Marketing Group, of illegally selling the financial information of more than 500,000 people to several companies, including Ideal Financial Solutions. Ideal Financial Solutions then allegedly stole more than $7 million from consumers' bank accounts as part of a payday loan scheme. In an Aug. 12, 2015 article, *The Washington Post* reported that data-selling cases like this one highlighted the dangers that cybersecurity threats pose to the consumer – not only in accessing sensitive information, but also in making that information accessible to others.

Ashley Madison Hack Demonstrates New Era of Cyber Insecurity

Perhaps no breach in 2015 exemplified that more than the hack of Ashley Madison. On Aug. 18, 2015, hackers of AshleyMadison.com, a site aimed at facilitating affairs among married persons, released nearly 10 gigabytes of data about Ashley Madison subscribers, including e-mail addresses, profiles, and partial credit card numbers, among other types of personal data. Journalists and news organizations faced many ethical challenges in reporting the data breach and subsequent disclosure of the hacked data.

Following the leak, hosts of the "Fitzy and Wippa Show," an Australian radio program, invited listeners who suspected their spouses of cheating to call the program. The hosts then searched for the spouse's information in the leaked data. One woman phoned because her husband's mood had shifted since the announcement of the leak. When the hosts told the woman that her husband's details suggested he was active on the Ashley Madison website, the woman panicked and hung up the phone. "I don't know if we should have done that," said one of the hosts afterwards. "That hasn't left me with a good feeling."

Thousands of listeners agreed, taking to social media to ridicule the show for its questionable ethics in handling the situation. As the *Columbia Journalism Review* (CJR) argued on Aug. 21, 2015, those listeners are not alone, as the Ashley Madison hack sparked a national discussion on journalistic ethics, and more specifically, on whether a personal-to-private boundary exists in reporting. Within hours of the leak, several major news outlets released controversial stories. *The Times-Picayune* in New Orleans reported on August 20 that an executive director of the GOP appeared in the leak, although he claimed the account was for research. *Gawker* revealed on August 19 that the credit card information of Josh Duggar, a star of a reality show that focused on a large religious family, was in the leak. The Associated Press (AP) reported on Aug. 20 that an investigation into Internet Protocol (IP) addresses suggested a number of White House employees logged on to the site from their work computers. Despite the information's possible inaccuracy — the site does not verify e-mail addresses, so many public accounts, including, for instance, former British Prime Minister Tony Blair's public e-mail address, appeared in the data dump — its availability raised serious concerns among journalists and lawyers.

"I don't know if we even know the right questions to ask," said vice-chair of ethics at the Society of Professional Journalists (SPJ) Monica Guzman told *CJR* on August 21. "This is unprecedented in journalism, the frequency with which information that previously would not have been disclosed is being revealed." However, one such question ethicists asked was whether the media should be able to contact the victims of a hack that illegally releases private information. Several outlets, including the AP and the *Los Angeles Times*, sifted through the leaked data and contacted users on the list, under the presumption that the use of government e-mail addresses justified the investigation.

"I absolutely think it's worth investigating," said Jane Kirtley, director of the Silha Center and professor of media ethics and law at the University of Minnesota, in an August 24 radio interview on "AirTalk" on KPCC radio. "My own view is that anybody that has a .gov or other government e-mail account has to assume that what they're doing is official business under the law, and I think that for most people, the idea that government employees are using government resources to post on a site like this could be a matter of public interest and concern. My biggest concern … is that some of these Ashley Madison profiles may have been hacked or phished, and they may not actually represent the person that has that e-mail address."

This potential for publishing inaccurate information also raised a larger debate over the ethics of publishing. As *CJR* noted, the argument for many journalists is simple: once the data is public, then as long as journalists apply the standards of newsworthiness, public interest, and minimizing harm, then "why not treat it like any other information?" Guzman disagreed, saying, "Public is not the same as published. If you're a journalist, you are assuming responsibility for what you publish. … We're looking at these hacks like forces of nature. These are crimes, not tornados."

But some experts contended that this argument actually supports the investigation of leaked names in order verify accuracy. "[I]f what these news organizations are saying is, 'We're going to follow up on these and contact these folks and see if in fact they're the ones [on the site],' I think that's an absolutely legitimate line of inquiry," said Kirtley.

Underlying the journalistic concerns is the blurred distinction between public and private, especially on the Web. As cybersecurity hacks continue to become an everyday occurrence, the leaks of sensitive information once securely stored online may raise more concerns about privacy rights in the digital age. "I'm not sure anyone is really reckoning with how big [breaches like this] could be, yet," said *The Awl*'s John Herrman in an August 18 post. "If the data becomes as public and available as seems likely right now, we're talking about tens of millions of people who will be publicly confronted with choices they thought they made in private. The result won't just be getting caught, it will be getting caught in an incredibly visible way that could conceivably follow victims around the [I]nternet for years."

Dillon White
Silha Research Assistant

Minnesota Court of Appeals Declares Criminal Defamation Statute Unconstitutional

On May 26, 2015, the Minnesota Court of Appeals ruled that the state's criminal defamation law was unconstitutionally overbroad. *Minnesota v. Turner*, No. A14-1408 (Minn. Ct. App. May 26, 2015). A three-judge panel found that the statute violated the First Amendment's protections of speech because it had the potential to criminalize true statements. Free speech advocates have noted that the victory is not surprising given the broad protections the First Amendment provides for expression. However, some Minnesota state legislators have suggested that they will work toward enacting new criminal laws to regulate the types of online behavior that were at issue in the case.

DEFAMATION

The case arose in 2013 after Timothy Turner published several posts on Craigslist, an online classified ads service, posing as his ex-girlfriend and her daughter. The posts contained sexually explicit language as well as the phone numbers of both women. The women began receiving phone calls and text messages soliciting sex, as well as messages with nude photos from several men, which prompted the women to contact law enforcement authorities. When authorities confronted him with the allegations, Turner admitted that he had created the Craigslist posts because he was angry with the two women. Isanti county prosecutors then charged Turner with two counts of violating the state criminal defamation statute. Minn. Stat. § 609.765, subd. 2.

During pre-trial proceedings in 2014, Turner sought to have the charges dismissed, arguing that the state's criminal defamation statute was unconstitutionally overbroad and vague. Turner also alleged that the prosecution violated his rights to free speech under the Minnesota Constitution and the First Amendment of the U.S. Constitution. The district trial court denied Turner's motion, finding that the statute was neither unconstitutionally vague or overbroad. Turner pleaded not guilty to both charges of criminal defamation. The district court later found Turner guilty on the two counts after a stipulated-facts trial. After the verdict, Turner appealed his conviction to the Minnesota Court of Appeals.

The unanimous three-judge panel's opinion, written by Judge Denise Reilly, overturned Turner's conviction, finding that the criminal defamation statute violated First Amendment protections of expression because its language was overbroad. The panel noted that Minnesota had established a negligence standard of liability for civil defamation cases involving private individuals. The liability standard required proof that a "defendant knew or in the exercise of reasonable care should have known that the defamatory statement was false." *Jadwin v. Minneapolis Star & Tribune Co.*, 367 N.W.2d 476 (Minn. 1985). Additionally, Reilly wrote that a plaintiff must prove that a statement was false in order to prevail in a civil defamation claim in Minnesota, according to prior case law. *Stuempges v. Parke, Davis & Company*, 297 N.W.2d 252 (Minn. 1980).

> "Although [Turner's] conduct was reprehensible and defamatory, we cannot uphold his conviction under an unconstitutional statute."
>
> **— Judge Denise Reilly, Minnesota Court of Appeals**

The panel found that the state's statute did not create similar levels of protection against charges of criminal defamation. The statute allowed truth to serve as a defense only if the statement was also "communicated with good motives and for justifiable ends." The panel held that this qualified defense conflicted with the state's definition of civil defamation. Additionally, the court concluded that the statute criminalized truthful statements, which receive First Amendment protections, as well as unprotected false statements.

Turner, as well as an *amicus* brief submitted by the Electronic Frontier Foundation (EFF), also challenged the criminal defamation statue on the basis that the law did not contain an "actual malice" standard for false statements about public concerns as established in *New York Times v. Sullivan*, 376 U.S. 254 (1964). Actual malice requires a libel plaintiff to prove that defendants made defamatory statements with knowledge of their falsity or with reckless disregard of the truth. The statute barred prosecution only if a statement about individuals participating in public matters was true or was a "fair and true report or a fair summary of any judicial, legislative or other public or official proceedings." The appellate panel agreed with Turner's argument, finding that the statute did not require a showing of actual malice to prove criminal liability. As a result, the statute was unconstitutionally overbroad because it had the potential to chill political speech.

Additionally, attorneys for the state argued that the court of appeals could narrowly construe the statute in order to "save it from constitutional challenge." The state argued that the appellate court could remove the "with good motives and for justifiable ends" qualifications to make the law comply with the First Amendment. However, the panel disagreed with the state's argument, noting that the court would need to re-write the statute by removing language and adding an actual malice standard. Such an action would require the court to act in "the legislative domain," which the panel refused to do. The court concluded stating that "although [Turner's] conduct was reprehensible and defamatory, we cannot uphold his conviction under an unconstitutional statute."

After the court of appeals issued the ruling, First Amendment attorney Mark Anfinson told the Minneapolis *Star Tribune* on May 26 that the court's decision was not surprising as the criminal defamation statute had been a "sitting duck constitutionally for decades." He acknowledged that although the court's decision might prevent prosecutors from pursuing individuals "who are clearly guilty of serious behavior," the panel's decision properly protected free speech under the First Amendment.

In the same story, Assistant Isanti County Prosecutor Deanna Natoli, who pursued the prosecution of Turner, expressed disappointment over the appellate court's decision to strike down the statute. "Right now it leaves victims without a remedy," Natoli told the *Star Tribune*. According to a May 26 story by the Associated Press (AP), Natoli said that she had considered charging Turner with disorderly conduct but did not believe that it would have reflected his "deplorable" behavior well enough. The prosecutor said she believed that the First Amendment did not protect Turner's actions, but she was unaware of any other state laws that would criminalize Turner's conduct. State prosecutors also refrained from appealing the intermediate court's decision to overturn the criminal defamation statute to the Minnesota Supreme Court.

Turner*, *continued on page 17

Supreme Court Throws Out Convictions for Violent Facebook Postings, Citing Intent

On June 1, 2015, the U.S. Supreme Court ruled that an individual's intent must be considered when determining whether speech constitutes a "true threat." The case, *Elonis v. United States*, 135 S. Ct. 2001 (2015), presented the question of whether convictions for violating 18 U.S.C. § 875(c), which prohibits transmitting in interstate communications that contain a threat to injure others, require a jury to find that the defendant subjectively intended his statements to be understood as threats, or if it was enough to show that a "reasonable person" would regard the statement as threatening.

ONLINE SPEECH

True threats occupy one of the few categories of expression not safeguarded by the First Amendment. The U.S. Supreme Court first held that "true threats" of committing an act of violence were not protected by the First Amendment in *Watts v. United States*, 394 U.S. 705 (1969). However, what exactly constitutes such a threat and what prosecutors must prove in order to obtain a conviction under the statute has not been especially clear.

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

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

> "Elonis's [*sic*] conviction was premised solely on how his posts would be viewed by a reasonable person, a standard feature of civil liability in tort law inconsistent with the conventional criminal conduct requirement of awareness of some wrongdoing."
>
> **— Chief Justice John Roberts, U.S. Supreme Court**

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

The Third Circuit rejected Elonis' argument and upheld the conviction on Sept. 19,

Elonis, *continued on page 18*

Turner, *continued from page 16*

Minnesota Rep. Debra Hilstrom (DFL-Brooklyn Center) told the AP on May 26 that the type of behavior that Turner engaged in is becoming more common. "Technology gets out ahead of statutes all the time. This is a new way that people are doing things that are a harm to the victims," Hilstrom said. "It's not safe and it's wrong. … We need to give prosecutors the tools they need." During the 2015 Minnesota legislative session, Hilstrom introduced a bill that would have made impersonating someone online for the purpose of harassment a felony offense. The bill did not pass, but Hilstrom told the AP she intended to introduce it again during a future legislative session.

The appellate decision also prompted Minnesota State Rep. John Lesch (DFL-St. Paul) to begin crafting a "revenge porn" statute, according to a St. Paul *Pioneer Press* story on June 2. Revenge porn is the online distribution of nude images or videos of individuals without their consent. "Revenge porn is a specific type of crime that needs its own law," Lesch said. "It can't crawl under the parameters of a catch-all like criminal defamation or disorderly conduct." Several other states have also passed revenge porn laws despite concerns that such statutes could criminalize First Amendment protected speech. (For more information on other states passing revenge porn statutes, see "California Legislators Address Data Protection and New Technology on Several Fronts" in the Fall 2013 issue of the Silha *Bulletin*. For more information on how Google is attempting to limit online access to revenge porn images, see United States Remains Skeptical of the Right to Be Forgotten in "'The Right to Be Forgotten' Continues to Develop in the Year Following European High Court Decision" on page 1 of this issue.)

In a June 9 interview on Minnesota Public Radio, Lesch explained that he was assembling a working group of defense attorneys, domestic abuse prevention activists, and free-speech advocates to help draft the law. "I think that [a revenge porn] law is complicated enough that it needs to be vetted by a group of folks who know what they are talking about … because the wording is critical," Lesch said. The *Pioneer Press*' June 2 story reported that Lesch intended to have a draft of the bill criminalizing revenge porn completed by the fall of 2015.

Casey Carmody
Silha *Bulletin* Editor

Elonis, *continued from page 17*

2013, reasoning that limiting the definition of true threats to only those statements where the speaker subjectively intended to make a threat would fail to protect individuals from "the fear of violence" and the "disruption that fear engenders," because it would protect speech that a reasonable speaker would understand to be threatening. The U.S. Supreme Court granted *certiorari* in the case on June 16, 2014. Oral arguments were heard in December 2014. (For more information regarding oral arguments and history of the case see "Supreme Court Considers Whether Facebook Posts Constitute 'True Threats'" in the Fall 2014 issue of the Silha *Bulletin*.)

The U.S. Supreme Court's review of the decision settled a split between the subjective intent standard that the Ninth Circuit adopted in *United States v. Cassel*, 408 F.3d 633 (9th Cir. 2005), and the objective listener standard utilized by the majority of the other circuits. The majority of circuits rejected the subjective intent requirement, holding that statements that are reasonably construed as threats by the listener are not given First Amendment protection and can be punished. However, the Ninth Circuit, as well as the highest state courts in Massachusetts, Rhode Island, and Vermont, required proof of the speaker's subjective intent to threaten before the government can punish a speaker. The U.S. Supreme Court ruled that the defendant's subjective intent must be taken into account.

Prior to the Supreme Court's decision, many legal commentators argued that the decision might be an important case for the First Amendment, rap music lyrics, and the rules for threatening and abusive language on social media. The Reporters Committee for Freedom of the Press, the Student Press Law Center, and the American Civil Liberties Union submitted *amicus* briefs arguing that Elonis' statements should be protected under the First Amendment and warned that if a defendant's intent was not taken into account it could chill speech out of fear of criminal prosecution. However, rather than addressing the First Amendment arguments, the Court's opinion focused only on statutory interpretation and principles of criminal law. "Elonis's [*sic*] conviction was premised solely on how his posts would be viewed by a reasonable person, a standard feature of civil liability in tort law inconsistent with the conventional criminal conduct requirement of awareness of some wrongdoing," Chief Justice John Roberts wrote for the 8-1 majority. Chief Justice Roberts went on to add that "given [the Court's] disposition, it is not necessary to consider any First Amendment issues."

Chief Justice Roberts wrote that prosecutors must do more than prove that reasonable people would view statements as threats. He explained that a conviction "is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat. "However, the majority opinion offered little in the way of specifics about exactly what government prosecutors must prove in order to obtain a successful conviction.

In a separate opinion that concurred in part and dissented in part, Justice Samuel Alito criticized the majority opinion for not establishing a clear rule of what level of intent would suffice for a conviction and how prosecutors could prove such intent. "[T]he Court holds that the jury instructions in this case were defective because they required only negligence in conveying a threat. But the Court refuses to explain what type of intent was necessary," Justice Alito wrote. "Did the jury need to find that Elonis had the purpose of conveying a true threat? Was it enough if he knew that his words conveyed such a threat? Would recklessness suffice? The Court declines to say. Attorneys and judges are left to guess." Justice Alito also argued that the government at least must prove that the defendant acted recklessly with his statements, or that the defendant had conscious disregard for the risk that a statement could be taken as a threat. In the majority's opinion, Chief Justice Roberts declined to say whether a "recklessness standard" would suffice, noting that neither Elonis nor the government had argued the point.

In his own dissenting opinion, Justice Clarence Thomas agreed with Justice Alito that the majority's opinion failed to give lower courts clear guidance, writing that the Court's "job is to decide questions, not create them." Thomas went on to write that "given the majority's ostensible concern for protecting innocent actors, one would have expected it to announce a clear rule — any clear rule. Its failure to do so reveals the fractured foundation upon which today's decision rests. Failure to decide [a specific intent requirement] throws everyone from appellate judges to everyday Facebook users into a state of uncertainty."

Several free speech advocates agreed with the Court's decision. In a June 1, 2015 interview with *The Washington Post*, American Civil Liberties Union Legal Director Steven R. Shapiro said, "[the law] for centuries required the government to prove criminal intent before putting someone in jail. That principle is especially important when a prosecution is based on a defendant's words. The Internet does not change this long-standing rule." *Washington Post* writer Brian Fung also noted that the Court's decision could bolster online speech. "Most people probably agree that there should be as few restrictions on speech as possible on the Internet, the better to promote innovation and expression," Fung wrote.

> "The Internet is the crime scene of the 21st century. The laws governing social media require swift interpretation to keep pace with the ever-advancing criminal activity in this space."
>
> **— Mai Fernandez, Executive Director, National Center for Victims of Crime**

However, several victims' rights groups were disappointed at the stricter standard and warned that the ruling would make it harder to convict those who make threats. "The Internet is the crime scene of the 21st century. The laws governing social media require swift interpretation to keep pace with the ever-advancing criminal activity in this space," said Mai Fernandez, executive director of the National Center for Victims of Crime, in a June 1 press release.

"This decision fails to recognize that victims of stalking experience fear regardless of the offender's intent. If what constitutes a threat is not clearly defined, our concern is that this ruling provides enormous space for stalkers and abusers to act. Offenders can simply claim they never intended harm and as a result will not be held accountable," added Director of the Stalking Resource Center Michelle M. Garcia in the same press release.

Some legal commentators also argued that *Elonis* might have created an opportunity for Congressional intervention. "*Elonis* is more important for what it leaves open than what it resolves. The Court didn't supply an answer to what minimum [intent] would apply generally to federal criminal statutes under the background principles for interpretation of criminal statutes" wrote Jonathan Keim, counsel for the Judicial Crisis Network, in a June 3 *National Review* article. "This leaves the door wide open for Congress to pick up where the Court left off."

Sarah Wiley
Silha Research Assistant

Obama Administration's Handling of Freedom of Information Act Requests Under Fire

During the first half of 2015, several reports raised questions over President Barack Obama's administration's efforts to be transparent, despite the fact that the President had often called for greater government transparency. Specifically, observers criticized the administration's handling of Freedom of Information Act (FOIA) requests, which allow citizens to ask the government to publicly release agency records. 5 U.S.C. § 552. Although the law is intended to apply to all federal agencies, observers have alleged that members of the Obama administration have taken steps to limit disclosure of records or avoid it altogether. These reports have also prompted at least one Congressional committee to hold hearings on the effectiveness of FOIA and whether reforms are needed.

FOIA

In 2007, the administration of President George W. Bush announced that the White House Office of Administration (OA) would no longer respond to Freedom of Information Act (FOIA) requests. For more than thirty years, the OA, the agency responsible for overseeing the White House's records archiving system, was subject to FOIA like any other government agency. However, by 2007, as *Mother Jones* reported on May 15, 2009, millions of e-mails were missing from the system, including some that may have shed light on a number of political scandals. Not wanting to disclose documents that may have explained the lost e-mails, the Bush administration claimed the OA was an advisory office, rather than a federal agency, and was not subject to FOIA. After a lengthy legal battle, the administration's decision was upheld in *Citizens for Responsibility and Ethics in Washington v. U.S. Dep't of Justice*, 658 F.Supp.2d 217 (D.D.C. 2009). However, when President Obama took office on Jan. 21, 2009, he stated in his inaugural address that "transparency and the rule of law [would] be the touchstones of [his] presidency." Many transparency advocates hoped Obama would reverse the Bush administration's practice of exempting the OA from FOIA.

On March 17, 2015, the Obama administration appeared to change course on its promise for greater executive office transparency. In a Federal Register notice, 80 Fed. Reg. 13757, the government issued a final rule — meaning there will be no opportunity for public comment — declaring the OA formally exempt from FOIA requests. The notice called the action an implementation of "well-settled legal interpretations," stating that the OA is an "entity whose sole function is to advise and assist the President of the United States [and] is not an agency … and thus is not subject to the Freedom of Information Act."

The announcement came during the annual Sunshine Week, a week dedicated to increasing open government, and only one day after Freedom of Information Day on March 16. Critics like Anne Weissmann, the interim executive director and senior counsel for the Citizens for Responsibility and Ethics in Washington's (CREW), called the notice a "mockery" of Obama's commitment to transparency in a statement following the announcement. Obama officials were quick to point out that the decision was not a radical one.

> "The government ought to be accountable to the people, and transparency yields accountability. Unfortunately, federal agencies continue to find creative ways to avoid the level of transparency that FOIA was designed to foster."
>
> **— Sen. Chuck Grassley, (R-Iowa)**

"This federal register notice does not change any aspect of the Administration's FOIA policy," said an unnamed White House official in an e-mail to *The Hill* on March 16, 2015. "It simply removes outdated regulations that no longer apply to the Office of Administration and haven't applied since the Bush administration."

However, the notice signaled yet another black mark in a series of recent revelations about FOIA practices in the Obama administration. In a *National Review* story on June 9, 2015, editor Eliana Johnson detailed the government's involvement in a practice known as "sensitive review." According to *National Review*, Treasury Department Deputy Executive Secretary Wally Adeyemo wrote a memo in December of 2009 declaring that any "sensitive information" requested under FOIA would be subject to review not only by career FOIA officials, as is customary practice, but also by a committee of political appointees from legislative affairs, public affairs, and the general counsel's office." This practice delayed the production of documents well beyond the designated FOIA requirement — 20 days for government response, plus an additional 10 days in special circumstances — often introducing political considerations into a process that was designed to create transparency in spite of such motivations, according to *National Review*. Evidence uncovered by the *National Review* also suggested that the Internal Revenue Service (IRS), the Department of Homeland Security, and a handful of other agencies all implemented a similar version of sensitive review. The government denied such involvement.

"These actions run counter not just to the spirit and the letter of the Obama administration's pledge to unprecedented transparency, but also to the spirit of the Freedom of Information Act itself," Johnson wrote.

Adding to the controversy were the findings from a federal data analysis published by the Associated Press (AP) on March 17, 2015, which revealed that in 2014, the Obama administration set a record for "censor[ing] government files" or completely denying access to them under FOIA. The report also uncovered longer release times, as compared to 2013, when the government did provide documents, as well as a record number of times that files deemed especially "noteworthy" were not turned over quickly. Perhaps most notable, the report found that nearly one in three cases in which the government redacted or withheld information were improper under the law when challenged.

"This disappointing track record is hardly the mark of an administration that was supposed to be the most transparent in history," said Sen. John Cornyn (R-Texas) in a statement, who co-sponsored a bill with Sen. Patrick Leahy (D-Vt.) to improve FOIA that died in the House in 2014.

Hearing Examines Whether FOIA is Effective

In light of these revelations, the House Oversight and Government Reform Committee met in the first week of June 2015 to discuss whether FOIA needed reform. Requesters, including journalists and watchdog groups, testified on the barriers they experienced in FOIA requests. Reporter

Administration, *continued on page 20*

D.C. Circuit Clarifies Key Fee Waiver Provisions of FOIA

On Aug. 25, 2015 the U.S. Court of Appeals for the District of Columbia Circuit clarified who could be eligible for particular types of fee waivers under the Freedom of Information Act (FOIA). *Cause of Action v. Federal Trade Commission*, No. 13-5335 (D.C. Cir. Aug. 25, 2015). FOIA allows federal agencies to charge reasonable fees for "document search, duplication, and review, when records are requested for commercial use." However, FOIA permits requesters to ask the agency to waive fees in several different circumstances, including when the disclosure of the records "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" or when the requester is "a representative of the news media." In its decision, the D.C. Circuit Court of Appeals rejected a lower court's interpretation of both the public interest and news media waiver provisions that prevented a non-profit organization from being eligible to have fees waived under FOIA.

FOIA

In 2011, the newly-established Cause of Action (Action), a non-profit organization that "advocates for economic freedom and opportunity by educating the public about the threat posed by improvident federal regulations, spending, and cronyism," submitted a FOIA request to the Federal Trade Commission (FTC) seeking all records related to the agency's guides on product endorsement use in advertising. The organization later agreed to narrow its request to records about any changes to the guides in reference to social media publishers, but also asked the FTC to grant the group a public-interest fee waiver because of its non-profit status. The FTC denied Action's requests because the agency said that FOIA only allows for a public-interest fee waiver if the disclosure of records was "likely to contribute significantly to public understanding of the operation or activities of the government." Action then asked for a fee waiver, claiming it was a news media representative that intended to disseminate information found in the records. Again, the FTC denied the request, stating that the organization did not specify how the information would be disseminated. However, in accordance with FOIA, the FTC did not charge Action a fee for the first 100 pages of the requested records, but stated that the remaining pages would be withheld until the organization submitted payment.

Action submitted an administrative appeal of the FTC's decision to deny a fee waiver, which the agency refused to overturn. Action also made a second request for all of the agency's records related to cases when the FTC granted public-interest fee waivers as well as records about the processes for how those decisions were made. With the second request, Action applied for both public interest and news media representative fee waivers. Again, the FTC provided 100 pages free of charge but refused to grant a waiver for the remaining pages. The agency also rejected an administrative appeal of the decision from Action, again stating that the group failed to provide details about how information would be disseminated and did not sufficiently explain how it was a news media representative.

Action then submitted a final FOIA request. The third request renewed the two earlier requests as well as asked for all records related to the processes of how the FTC made the decisions not to grant Action's previous fee waiver requests. The group also asked for a fee waiver simply by asserting that it was a non-profit group. The FTC narrowed the organization's request to only the records regarding the decision-making process about fee waivers, which totaled 95 pages with 16 pages withheld due to FOIA exemptions. The FTC did not consider whether Action qualified for a public interest or news media fee waiver because the disclosed records totaled less than the complimentary 100 pages required by FOIA. Action filed an administrative appeal, and through subsequent correspondence with the FTC, described how the organization intended to "analyze the responsive records, use its editorial skills to create distinct works, and share the resulting analysis with the public through a variety of channels," including through newsletters, a website, a Facebook page, tweets through a Twitter account, and published reports. Action also highlighted several online articles it had published as evidence that it should qualify for a public interest or news media few waiver. However, the FTC denied Action's administrative appeal, arguing that the questions over fee waivers were moot

Administration, *continued from page 19*

Jason Leopold of *Vice News* described how the Pentagon's Office of Net Assessment (ONA) offered to fulfill his request only if he promised to never file another one, according to a June 2, 2015 story by *The Washington Post*. The Reporters Committee for Freedom of the Press (RCFP) reported in a June 5 news update that in a separate instance, former CBS journalist Sharyl Attkisson testified about filing a FOIA request with the Defense Department in 2003 and did not receive a response until 2013. The RCFP also noted that Rep. Elijah Cummings (D-Md.) blamed some of the inefficiency on a shortage of personnel and resources, noting that despite a 20% increase in FOIA requests from 2009 to 2014, the number of FOIA officers decreased by almost 200 people in the same time period.

The House committee also sought advice on ways to improve FOIA, including whether the proposed FOIA Improvement Act of 2015 (S. 337) would fix some of the law's problems. According to an AP story on May 6, 2015, the proposed bill would "codify the presumption of disclosure," make the Office of Government Services (OGIS) more "independent to help it achieve its stated purpose," establish a "modern FOIA portal to intake and track requests," and restrict the use of Exemption 5 withholdings. Exemption 5 withholdings protect privileged information from third-party access, and they are often invoked to protect inter- or intra-agency letters or memoranda. The bill is co-sponsored by Sens. Cornyn and Leahy, and, according to a press release issued by Sen. Leahy's office on Feb. 2, 2015, it is nearly identical to a bill that failed in the House in 2014.

"The government ought to be accountable to the people, and transparency yields accountability," said Sen. Chuck Grassley (R-Iowa), chairman of the Judiciary Committee and an original co-sponsor of the bill, in the February 2 press release. "Unfortunately, federal agencies continue to find creative ways to avoid the level of transparency that FOIA was designed to foster. This bill takes an important step to ensure that agencies won't be able to hide behind an exemption solely to protect their public image. Instead, it requires agencies to disclose information unless they reasonably foresee that disclosure would harm an interest that an exemption protects. Agencies also need flexibility to process and respond to their FOIA requests, rather than a one-size-fits-all approach. This bill strikes the right balance."

Dillon White
Silha Research Assistant

because the disclosed records for the third request totaled less than 100 pages and no fee was ever charged.

On May 25, 2012, Action filed a lawsuit in the United States District Court for the District of Columbia challenging the FTC's decision to withhold certain records as well as the denial of fee waivers. The district court granted summary judgment in favor of the agency regarding both the withholding of specific records as well as the FTC's decision to deny fee waivers in relation to Action's first two FOIA requests. The district court also agreed with the FTC that any issue over fee waivers related to Action's third requests was also moot. *Cause of Action v. Federal Trade Commission*, 961 F. Supp.2d 142 (D.D.C. 2013). Action did not appeal the summary judgment order related to the withheld documents, but asked the U.S. Court of Appeals of the D.C. Circuit to review the district court's decision to grant summary judgment in favor of the FTC on the issues related to fee waivers.

Writing for a unanimous three-judge panel, Chief Judge Merrick Garland first ruled that the FTC and district court were incorrect to declare the fee waiver issue moot in relation to Action's third request. He wrote that in addition to records about the FTC's processes to deny fee waivers to the group, Action's third request had asked for the same records it sought during the initial two requests. The FTC acknowledged during oral arguments that ignoring the renewed requests was a mistake. As a result, the appellate court found that the FTC should have provided additional records from the initial requests as part of the third request, which would have totaled more than the free 100 pages that the FTC provided. The judge noted that the fact that the fee waiver issue should not have been rendered moot was a key component of the case, because Action provided significant evidence as to why it should qualify for a public interest or news media fee waiver under FOIA during its correspondence with the agency about the third request. Thus, the court of appeals remanded the case to the district court because the lower court did not consider any of the evidence for a fee waiver that Action provided in relation to the third request due to the mootness decision.

Chief Judge Garland also went on to clarify how the lower court's decision on remand should interpret FOIA's provisions granting fee waivers for the production of records in the name of the public interest or for news media organizations. The judge acknowledged many aspects of the district court's initial, improper analysis on Action's fee waiver applications for the group's FOIA requests could be attributed to the D.C. Circuit Court of Appeals, "which has provided relatively little guidance regarding the complexities of those two provisions." However, the appellate court noted that several mistakes in the lower court's analysis should also be attributed to the FTC's "erroneous interpretations of FOIA contained in its own regulations."

On the public-interest waiver provision, Chief Judge Garland quoted FOIA's text, noting that it required three criteria to be satisfied in order to have fees waived: (1) the records must shed light on "the operations or activities of the government;" (2) be "likely to contribute significantly to public understanding" of such operations or activities; and (3) not be "primarily in the commercial interest of the requester." The court of appeals found that the FTC's regulations, which the district court applied in the case, erroneously required that a requester show that information contained in the records sought would increase the understanding of the public "at large." Chief Judge Garland wrote that FOIA did not require a standard of reaching such a wide audience. Rather, the appellate court wrote that "the relevant inquiry … is whether the requester will disseminate the disclosed records to a reasonably broad audience of persons interested in the subject," quoting the U.S. Court of Appeals for the Second Circuit's opinion in *Carney v. U.S. Dep't of Justice*, 19 F.3d 807 (2d Cir. 1994).

Chief Judge Garland also held that FOIA did not require requesters to "identify several methods of disseminating the information" contained in disclosed agency records in order to qualify for the public-interest fee waiver. In other words, FOIA did not require a minimum number of possible outlets of dissemination so long as the requester identified some way to get the information to the public. The judge acknowledged that Action's initial two FOIA requests did not provide substantial evidence on how it would disseminate information or whom it might reach. "But whether Action cleared that bar with the substantial additional evidence it submitted with its third request — evidence regarding its newsletter, periodicals, website, social media presence, planned reports, and press releases to media contacts — must be addressed on remand," he wrote.

Additionally, the court of appeals disagreed with the lower court's decision that a FOIA request for records related to a fee waiver process should automatically be treated as a "commercial" interest. The appellate court wrote that a request about the waiver process had the potential to be informative for the public even though the records requester would be the primary beneficiary of the information. "Of course, if a requester's only interest in a particular request is to further its own litigation, it may be difficult to show that disclosure of the information is likely to contribute significantly to public understanding," Chief Judge Garland wrote. "But in that situation, the fee-waiver application runs aground on a different element of the public-interest test."

As for the news media waiver provision, Chief Judge Garland noted that the last time the D.C. Circuit Court of Appeals had substantially addressed this specific provision was in the 1989 case *National Security Archive v. Dep't of Defense*, 880 F.2d 1381 (D.C. Cir. 1989), which likely led to many of the failures in the district court's analysis. He wrote that FOIA created five criteria that a requester must meet in order to be considered a representative of the news media for fee waiver purposes. According to the appellate court, a requester must: (1) gather information of potential interest (2) to a segment of the public; (3) use its editorial skills to turn the raw materials into a distinct work; and (4) distribute that work (5) to an audience. The judge also noted that the records could not be "sought for commercial use."

Chief Judge Garland acknowledged that the district court's analysis that Action met the first two prongs of the news media representative was accurate. However, he criticized the district court's analysis because it examined the nature of Action's FOIA requests in order to determine whether the organization should qualify for a news media fee waiver. "Such a case-by case approach is correct for the public-interest waiver test, which requires that the 'disclosure of the [requested] information' be in the public interest," Chief Judge Garland wrote. "But the news-media waiver, by contrast, focuses on the nature of the requester [*sic*], not its request. The provision requires that the request be 'made by' a representative of the news media. … A newspaper reporter, for example, is a representative of the news media regardless of how much interest there is in the story for which he or she is requesting information." If Action met all five prongs of the news media representative test, "it does not matter whether any of the individual requests does so," the appellate court ruled.

Chief Judge Garland then turned to the district court's decision that Action did not qualify for a fee waiver as a news media representative because it failed to meet the final three prongs of the test. With respect to the third prong, he wrote that the district court did not consider that Action could create original works that would consist of commentary for news organizations, such as a press release detailing information found in the records or editorial comments about the records in an interview with

D.C. Circuit, *continued on page 22*

D.C. Circuit, *continued from page 21*

the press. "A substantive press release or editorial comment can be a distinct work based on the underlying material, just as a newspaper article about the same documents would be — and its composition can involve 'a significant degree of editorial discretion,'" Chief Judge Garland wrote, quoting *National Security Archive v. Dep't of Defense.* The appellate court also found that the district court erred when deciding that Action did not qualify as a news media representative because the organization did not seek to supplement the content of their editorial products with information gathered from sources beyond what was found in the requested records. FOIA did not create such a requirement, the court of appeals held.

As for the fourth and fifth prongs of the test, Chief Judge Garland wrote that the district court did not conduct a proper analysis. He again noted that the lower court focused primarily on the nature of the requests rather than who the requester was, which was not the proper analysis for the news media fee waiver provision of FOIA. The court also held that despite semantic debates between the parties in the case and *amici* about what qualified as dissemination of information, "posting content to a public website can qualify as a means of distributing it — notwithstanding that readers have to affirmatively access the content, rather than have it delivered to their doorsteps or beamed in their homes unbidden."

The judge then wrote that the district court was incorrect to deny Action news media status based on the group's failure to provide estimates of audience size and the fact that the organization had not published a newsletter prior to the first FOIA request. "There is no doubt that the requirement that a requester distribute its work to 'an audience' contemplates that the work is distributed to more than a single person. But beyond requiring that a person or entity have readers (or listeners or viewers), [FOIA] does not specify what size the audience must be," Chief Judge Garland wrote. "Nor is it disqualifying that Action's newsletter did not exist at the time it made its first FOIA request. It is true that the statute uses present-tense verbs — 'gathers,' 'uses,' and 'distributes' — that characterize a present state of being, not just a set of aspirations. … But this does not mean that a new news-media venture cannot qualify as a 'representative of the news media' until it has a track record. Although a bare statement of intent is not enough to qualify, firm plans can be."

Chief Judge Garland ruled that courts must make fact-based determinations as to whether an organization claiming to be a news media representative has provided sufficient evidence, whether it be current examples or documentation of future plans, to qualify for the FOIA waiver. "For a requester that serves (or plans to serve) the public through multiple outlets — here, newsletters, press releases, press contacts, a website, and planned reports — those must be considered in combination," he wrote. "An entity with an extensive record will ordinarily qualify with only a thin recital of its plans (or perhaps none at all). Conversely, an entity with little or no historical record of distributing its work … may make up for that absence by concretely setting out its plans to do so."

> "Posting content to a public website can qualify as a means of distributing it — notwithstanding that readers have to affirmatively access the content, rather than have it delivered to their doorsteps or beamed in their homes unbidden."
>
> **— Chief Judge Merrick Garland, U.S. Court of Appeals for the District of Columbia Circuit**

Finally, the appellate court criticized the lower court for relying on the FTC's outdated language defining news media organizations in the agency's guidelines for FOIA compliance. The FTC's guidelines defined a news media representative as "any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public." Chief Judge Garland wrote that the district court was wrong to focus so heavily on the FTC's interpretation that an organization must be "organized especially around dissemination" in order to qualify for news media waivers. The judge explained that FOIA's language did not create such a limited interpretation of what could be considered a news media organization.

The court of appeals also disagreed with the lower court's assessment "that a public interest advocacy organization cannot satisfy the statute's distribution criterion because it is 'more like a middleman for dissemination to the media than a representative of the media itself.'" Rather, Chief Judge Garland wrote, "assuming that these other criteria are satisfied, there is no indication that Congress meant to distinguish between those who reach their ultimate audiences directly and those who partner with others to do so, as some recognized journalistic enterprises do." The appellate court then remanded the case for further proceedings, noting that the fee waiver request issues were not moot and instructing the district court to make an appropriate decision in line with the clarifications in Chief Judge Garland's opinion.

After the decision was published on August 25, Action released a statement on its website praising the appellate court's ruling. "Today's decision is the most significant court ruling for the news media in over a quarter-century and represents a major victory in the fight to make the federal government more transparent," Action Executive Director Dan Epstein said in the press release. "As a result of this ruling, the ability of federal agencies to deny fee waivers in order to stifle the release of information has been significantly limited. We, together with our partners from the Reporters Committee [for Freedom of the Press, who submitted an *amicus* brief], are hopeful that this decision spurs a new era of greater public access to information."

Holland & Knight attorneys Adrianna C. Rodriguez and Charles D. Tobin also recognized the importance of the appellate court's decision for FOIA fee waivers. "The Court of Appeals' decision in *Cause of Action v. Federal Trade Commission* — the first ruling in more than two decades to address the issue — will make it more difficult for agencies to deny fee waivers to the news media and other organizations serving the public interest," the attorneys wrote. "The [] decision makes it more difficult for agencies to deny waivers to new organizations that are just beginning to establish a following, as well as the growing group of newsgatherers that maintain a web presence as their primary — or in some cases, exclusive — outlet."

Casey Carmody
Silha *Bulletin* Editor

Updates to State Laws Create Challenges, New Benefits for News Organizations

During the summer of 2015, several states made or attempted to make significant changes to laws that affect how reporters and news media organizations do their work. In Washington, the state Supreme Court struck down a law limiting frivolous law suits against the press.

STATE LAW UPDATES

In Texas, the state legislature created new protections for journalists who report on whistleblower allegations. Meanwhile, the Wisconsin state legislature halted proposed changes to the state's open records laws after significant backlash from news organizations and open government advocates.

Washington Supreme Court Strikes Down Anti-SLAPP Law

On May 28, 2015, the Washington Supreme Court struck down the state's anti-Strategic Lawsuit Against Public Participation (anti-SLAPP) law in its entirety, ruling in *Davis, et al. v. Cox, et al.*, 183 Wash. 2d 269 (Wash. 2015), that the law violated the Washington Constitution's guarantees of the right to a civil jury trial. The Washington law, RCW 4.24.525 (RCW) — and anti-SLAPP laws in general — provided protection against frivolous libel lawsuits aimed at suppressing speech. RCW curbed the possibility of harassing litigation by affording defendants an easy process for requesting a lawsuit's dismissal at a judge's discretion. However, the state Supreme Court determined that requiring judges to rule on factual issues during the pretrial stage could prevent a legitimate claim from reaching a jury. Under Section 21 of the Washington Constitution, the right to a jury trial "shall remain inviolate."

"RCW 4.24.525(4)(b) creates a truncated adjudication of the merits of a plaintiff's claim," wrote the state Supreme Court. "Such a procedure invades the jury's essential role of deciding debatable questions of fact."

Central to the court's decision was the stipulation in provision 4(b) that a libel case be thrown out unless the plaintiff could show by "clear and convincing evidence a probability of prevailing on the claim." Having determined that this provision was unconstitutional, the state court then considered whether this provision could be separated from the remainder of RCW, or whether the law could not function without it. Finding that the law would not work without the unconstitutional provision, the Supreme Court struck down RCW in its entirety. The decision marked the first time a state's anti-SLAPP law has been deemed unconstitutional, according to a May 28, 2015, statement from the Reporters Committee for Freedom of the Press (RCFP), which also submitted an *amicus* brief in the case, urging the court to uphold the anti-SLAPP statute in order to allow courts the ability to effectively dispose of SLAPPs. The RCFP's brief for *Cox* as *amicus curiae* is available at https://www.rcfp.org/sites/default/files/2014-12-05-davis-v-cox.pdf (2015). However, according to *The Washington Post* on May 28, 2015, the decision, although a significant blow for free speech advocates, may not be devastating secondary precedent for other states. Although 28 states, the District of Columbia, and Guam have enacted some type of anti-SLAPP statute, many of them allow courts to decide whether a plaintiff must lose as a matter of law, but do not call on judges to weigh evidence, nor do they require a plaintiff to rebut an anti-SLAPP motion by meeting the clear and convincing evidence standard.

> "It therefore appears that, for now at least, media defendants and others [in Washington state] have lost an important protection against baseless lawsuits targeting their First Amendment activities."
>
> **— Attorney Bruce Johnston, Davis Wright Tremaine, LLP**

"Because the basis [of this decision] is the state constitution, the Washington Supreme Court's opinion is the last word, pending any future fix," said Bruce Johnson, an attorney with Davis Wright Tremaine LLP, which represented the defendants in the case, in the firm's blog on May 28, 2015. "It therefore appears that, for now at least, media defendants and others [in Washington state] have lost an important protection against baseless lawsuits targeting their First Amendment activities."

Texas Passes Whistleblower Protection Law for Reporters

On May 28, 2015, Texas Gov. Greg Abbott signed Senate Bill 627 (SB 627) into law, allowing journalists a privilege to accurately report on accusations of wrongdoing that have not yet been investigated by the government. Though the media had been using this defense against libel under common law in Texas for the past 25 years, SB 627 officially codified the privilege. According to a June 3, 2015, statement from the Freedom of Information Foundation (FOIF) of Texas, the bill protects the free flow of information for all Texas citizens.

SB 627 followed a complicated legal battle. Since 1990, media law practitioners have relied on *McIlvain v. Jacobs*, 794 S.W.2d 14 (Tex. 1990), to assert a media defendant's right to accurately report on third-party allegations, even if the allegations themselves are false. However, in 2013, the Texas Supreme Court issued its opinion, followed by a revised opinion in 2014, in *Neely v. Wilson*, 418 S.W.3d 52 (Tex. 2014), which called that practice into question. In that case, a doctor sued a media outlet that aired a story suggesting that the doctor was disciplined for operating on patients while under the influence of drugs. The doctor had been placed on probation following the Texas Medical Board's investigation showing that he had prescribed himself medication and was unable "to practice medicine with reasonable skill and safety to patients." In its opinion, the Court ruled that genuine issues of material fact existed as to whether the accusations were true. In its revised opinion issued on Jan. 30, 2014, the Court clarified that although it had not created a third-party reporting privilege in *McIlvain* in 1990, it did not explicitly reject one in *Neely*, because the facts did not require a determination of whether such a rule should apply. This left many media practitioners confused as to the state of the law, including the Texas Association of Broadcasters, which called the *Neely* decision "disastrous" in the organization's blog on March 3, 2015, noting that the ruling "called into question nearly 25 years of case law." With the passage of SB 627, the accurate reporting defense against libel is now solidified.

"By passing SB 627, the Legislature has ensured the ability of the media to report on critical information that can lead to government investigations and legislative reform," said co-chair of the FOIF's legislative committee Laura Prather in a June 3, 2015, statement on the organization's blog.

State Laws, *continued on page 24*

State Laws, *continued from page 23*

Wisconsin Politicians Face Backlash after Proposing to Change Open Records Law

On July 2, 2015, Republicans on the Joint Finance Committee in Wisconsin amended the state's 2015-2017 budget bill to create dramatic changes to the state's open records law. According to the *Wisconsin State Journal* on July 3, 2015, the proposal, which would have blocked the public from "reviewing nearly all records created by lawmakers, state and local officials or their aides, including electronic communications and drafting files of legislation," passed the Legislature's budget committee on a party-line vote and was sent to the state's full Assembly and Senate.

Following a flood of criticism, including a July 3 letter from the Society of Professional Journalists (SPJ) urging the legislature not to "eliminate any opportunity" for open government, as well as widespread condemnation from members of both parties, Wisconsin Gov. Scott Walker and other Republican legislators agreed to remove the provision from the budget. In a joint July 4, 2015 press release, Walker and other Republican leaders reaffirmed their commitment to an "open and accountable government," and said that although the "intended policy goal of [the] changes was to provide a reasonable solution to protect constituents' privacy and to encourage a deliberative process between elected officials and their staff in developing policy," they nevertheless agreed to remove the provision "in its entirety." The statement added that the state legislature would "form a Legislative Council Committee to more appropriately study [the issue] and allow for public discussion and input."

However, the maelstrom over the proposal also created a new controversy over who initially proposed the changes. According to a July 3 report from the Wisconsin Center for Investigative Journalism (WCIJ), similarities existed in the language used in both the open records changes and records-request denials from the governor's office, prompting the WCIJ to raise questions over whether now-presidential candidate Scott Walker was involved in the proposal. Adding to the skepticism was the unwillingness of Republican lawmakers to release the name of the person or persons responsible for proposing the changes to the law. According to the *Wisconsin State Journal*, lawmakers who voted for the initial proposal — including Joint Finance Committee co-chairpersons Reps. John Nygran (R-Marinette) and Alberta Darling (R-River Hills) — failed to elaborate on where the initial idea developed. The speculation over whether Gov. Walker had a hand in the proposal —including a July 29, 2015, article from the *Journal Sentinel*, which reported that Gov. Walker's office "pushed to add language … that would have shielded briefings, discussions about policy drafts and other 'deliberative' documents" — caused considerable concern among media organizations and lawmakers alike.

"This [proposal] was specifically and deliberately intended to inhibit transparency," said Bill Lueders, president of the Wisconsin Freedom of Information Council, to the *Wisconsin State Journal* on July 5, 2015. "I think there ought to be some political consequences for this."

> "We are excited about any crack of the window that allows us to give transparency to the public, and make the court process clearer to Minnesota."
>
> **— Mike Caputa, WCCO-TV News Director**

Following the controversy, more than 200 government officials, lawyers and media members gathered on July 29 for the Open Government Summit in Madison, Wis., according to the *Journal Sentinel* on Aug. 2, 2015. Attendees agreed that technological advancements raise considerable privacy issues for officials under the open records law, but argued that measured changes should be made to the current law, rather than a complete overhaul.

"You have to think long and hard before you toss something that is working," said Jeff Mayers, president of WisPolitics.com, an online political news service, in the aforementioned *Journal Sentinel* article. "We must be very cautious, very skeptical, and review proposed change carefully, so it doesn't hinder the presumption of complete public access."

Minnesota Supreme Court Eases Restrictions on Courtroom Cameras in Criminal Cases

On Aug. 12, 2015, the Minnesota Supreme Court issued an order relaxing restrictions on camera usage in courtrooms during criminal cases, declaring that the media need only a judge's approval to broadcast or take pictures in certain limited circumstances. The previous rule required all parties in a case to consent prior to recording. The order is part of a two-year pilot project that will be evaluated in January 2018. "We conclude there is good reason to lift the blanket exclusion of electronic coverage of public criminal proceedings so that we can study the impact of electronic coverage of those proceedings," the court wrote in the order. (For more information about the evolution of cameras in Minnesota courtrooms, see "Minnesota High Court Approves Cameras-in-Court Pilot Program" in the Winter 2009 issue of the Silha *Bulletin*, "Federal and State Courts Consider Proposals to Permit Cameras in Trial Proceedings" in the Fall 2010 issue, "Battles to Gain Camera/Audio Access to State and Federal Courtrooms Continue" in the Fall 2011 issue, "Minnesota Senate Expands Floor Access; State Supreme Court Approves Cameras" in the Winter/Spring 2011 issue, "Silha Spring Ethics Forum Focuses on Cameras in the Courtroom, Status of Minnesota Pilot Project" in the Spring 2012 issue, and "Minnesota Supreme Court Approves Use of Cameras in Civil Cases, Considers Expansion to Criminal Cases" in the Fall 2013 issue.)

According to the *Star Tribune* on Aug. 12, 2015, the decision came in response to recommendations from an advisory committee in 2014 consisting of attorneys, judges, and professors. Although the order relaxed restrictions, it did not eliminate them. Cameras will only be allowed for sentencing after a defendant pleads or is found guilty. Juries may not be present during coverage, and cameras will not be allowed in juvenile proceedings or in specialized court hearings involving drug, DWI, veteran, or mental health hearings. Judges and court administrators hold the power to approve or refuse coverage, and, according to an August 12 story by the Associated Press, further guidelines on this approval process are expected in the future. The court's full order is available at http://www.mncourts.gov/mncourtsgov/media/CIOMediaLibrary/OpinionsSC/ORADM098009-081215.pdf.

Despite these restrictions, media members were satisfied with the Minnesota Supreme Court's decision. "We are excited about any crack of the window that allows us to give transparency to the public, and make the court process clearer to Minnesota," said Mike Caputa, news director at WCCO-TV in Minneapolis, to the *Star Tribune*.

Dillon White
Silha Research Assistant

Journalists Abroad Face Uncertain Legal Challenges; U.S. Television News Reporters Slain During Live Report

During the summer of 2015, journalists around the world, including in the United States, faced threats of arrest, harsh prison sentences, and the loss of their lives. In the United States, two journalists were slain on live television, sparking debates over press safety and how news organizations should publish violent video images. Abroad, *Washington Post* reporter Jason Rezaian faced trial in Iran for espionage, and journalists in Egypt were convicted of "falsifying news." Several press advocacy organizations have denounced the violence and governmental interference with journalists.

ENDANGERED JOURNALISTS

Iranian Trial of Washington Post *Reporter Jason Rezaian Concludes*

After being detained in Iran for more than a year, the trial of *Washington Post* reporter Jason Rezaian concluded on Aug. 10, 2015. Rezaian, who holds dual American and Iranian citizenship, was arrested on July 22, 2014, along with his wife Yeganeh Salehi, who is an Iranian correspondent for *The National*, and two other unnamed journalists. According to several reports, Salehi and the unnamed journalists were released on bail. Rezaian has since remained in Evin Prison, one of Iran's most notoriously inhumane facilities, was reportedly kept in isolation, and was denied medical treatment, according to *The Atlantic* on July 22, 2015. (For more information on Rezaian's arrest, see "Journalists Arrested During Protests in Missouri; Journalists Abroad Face Dire Situations" in the Fall 2014 issue of the Silha *Bulletin*.)

The Iranian government has provided little information about why it arrested the journalists. It was not until April 2015 that Rezaian's lawyer learned of the specific charges against him. According to a statement issued from Tehran by Leila Ahsan, Rezaian's attorney, which was published by *The Washington Post* on April 20, 2015, Rezaian faced several charges, including espionage, "collaborating with hostile governments," and "propaganda against the establishment." The charges carried a maximum sentence of 10 to 20 years in prison. Rezaian was permitted to meet with his attorney only once since his arrest in July 2014.

Rezaian's trial began on May 26, 2015, and was closed to the public, including members of his family. The U.S. State Department and many news organizations, including the Committee to Protect Journalists (CPJ), called on Iran to open the Tehran Revolutionary Court's proceedings to the public, but the Iranian government refused. "Iran must end this travesty of justice immediately," said Sherif Mansour, CPJ Middle East and North Africa Program Coordinator in a May 22, 2015 press release. "After more than 300 days of unwarranted detention, the least Iran could do is to release Rezaian on bail and grant his employer entry to the country and access to the legal proceedings."

According to the *Post* on April 20, Ahsan said that the case file presents no evidence to justify the accusations against Rezaian, and that the charges are related to his journalistic pursuit of stories about Iran. Rezaian's brother, Ali Rezaian, told *The New York Times* on May 26 that the Iranian government was going to present two pieces of evidence of espionage during the trial: an American visa application for Salehi, and a form letter sent by Rezaian to President Barack Obama's 2008 White House transition team, which offered to help work toward improving relations between Iran and the United States. However, because the trial was closed to the press and the public, it was unclear why the Iranian authorities believed those documents to be incriminating and whether authorities offered any more evidence related to the charges against Rezaian.

The White House and the U.S. State Department criticized Iran's handling of the case. "If the reports are true, these charges are absurd, should be immediately dismissed and Jason should be freed immediately, so that he can return home to his family," said White House Press Secretary Josh Earnest on April 20, 2015 during a press conference.

"After just four secret hearings in 10 weeks, the sham trial of *The Washington Post*'s Jason Rezaian has ended in Tehran, but it remains unclear even to Jason's lawyer what might happen next," said *Post* Executive Editor Martin Baron in an Aug. 10, 2015 statement. "No verdict was announced and Iran's Revolutionary Court has offered no official indication of when such an announcement might come. The process has been anything but transparent and just, and that pattern persists. The only thing that is clear is Jason's innocence."

No verdict for Rezaian had been made public as the *Bulletin* went to press.

Egypt Sentences 3 Al-Jazeera Reporters

On Aug. 29, 2015, an Egyptian court sentenced Al-Jazeera journalists Baher Mohammed, Peter Greste, and Mohamed Fahmy to three years in jail after finding them guilty of "aiding a terrorist organization." According to an August 29 report by Al-Jazeera, Judge Hassan Farid announced that he sentenced the journalists to prison because they had not registered with the country's journalist syndicate, brought in equipment without security officials' approval, and had used a hotel as a broadcasting point without permission. The judge also said that the journalists had broadcast "false news."

The case began in December 2013, when Egyptian security forces raided the hotel suite that Al-Jazeera used at the time to report from Egypt. Authorities arrested Fahmy, Greste, and Mohammed, later charging them with allegedly being part of Morsi's Muslim Brotherhood, which authorities have declared a terrorist organization, and airing falsified footage intended to damage national security. The journalists were initially found guilty in June 2014. Greste and Fahmy were previously sentenced to seven years in prison, while Mohamed received 10 years in prison. The initial verdict sparked worldwide outrage from the United States government as well as many media organizations and rights groups. (For more information regarding the initial trial, see "Journalists Arrested During Protests in Missouri; Journalists Abroad Face Dire Situations" in the Fall 2014 issue of the Silha *Bulletin*).

In January 2015, an appeals court ordered a retrial, saying the initial verdict lacked evidence against the three journalists. However, the appeals court, using the same evidence as the trial court, still convicted the journalists, causing press freedom groups, human rights advocates, and Al-Jazeera itself to condemn the verdict. "Today's verdict defies logic and common sense," Al-Jazeera Media Network's acting director Mostefa Souag said in an August 29 statement. "Today's verdict is yet another deliberate attack on press freedom. It is a dark day for the Egyptian judiciary; rather than defend liberties and a free and fair media, they have compromised their independence for political reasons." Amnesty International called the guilty verdicts "an affront to justice that sound the death knell for freedom of expression in Egypt," in a statement published the same day. Accord-

Journalists, *continued on page 26*

Journalists, *continued from page 25*

ing to CPJ, at least 22 journalists are jailed in Egypt as of Aug. 12, 2015.

The Associated Press reported on Aug. 29, 2015, that the journalists plan to appeal the verdict and seek a pardon from President Abedel-Fattah el-Sissi, who has spoken out against their prosecution. Lawyer Amal Clooney, who represented Fahmy, said that she would be meeting with Egyptian officials. "The verdict today sends a very dangerous message in Egypt," Clooney told the AP. "Journalists can be locked up for simply doing their job, for telling the truth and reporting the news. And it sends a dangerous message that there are judges in Egypt who will allow their courts to become instruments of political repression and propaganda."

Charlie Hebdo *Cartoonist to Quit*

Charlie Hebdo cartoonist Renal Luzier, who drew the satirical magazine's front cover picture of the prophet Muhammad following the high-profile attacks on the magazine's offices in January 2015 that left several members of the editorial team dead, has said that he is leaving the publication. Luzier, who goes by Luz, told *The Guardian* on May 18, 2015 that the job without his slain colleagues had become "too much to bear." (For more information about the *Charlie Hebdo* attacks, see "*Charlie Hebdo* Attack Leaves Several Dead, Sparks International Debate on Limits of Free Speech" in the Winter/Spring 2015 issue of the Silha *Bulletin*.)

"This is a very personal choice," Luz, who joined *Charlie Hebdo* in 1992, said in an interview with French newspaper *Libération* on May 18, 2015. "Each issue is torture because the others are gone. Spending sleepless nights summoning the dead, wondering what Charb, Cabu, Honoré, Tignous would have done is exhausting," the cartoonist said, referring to his colleagues killed during the January 7 attacks.

The week following the attack, Luz drew the magazine's cover image, which depicted Muhammad with a sign saying "Je suis Charlie" under the words "All is forgiven." According to *The Guardian*'s May 18 story, the issue following the attack had a record-breaking print run of eight million issues. In late April, Luz announced that he would not draw the prophet again, saying it no longer interested him to do so. "Many people push me to keep going, but they forget that the worry is finding inspiration," Luz told *Libération*.

Gérard Biard, the top editor of *Charlie Hebdo*, told *The New York Times* on May 19 that Luzier would be sorely missed, and he acknowledged that grief after the attacks had taken a toll on staff members. "Certainly the grief continues to weigh on us, and the trauma is not the same for everyone," Biard said.

Two Virginia Journalists Shot and Killed On Live Television

On Aug. 26, 2015, two television journalists from Roanoke, Virginia, CBS affiliate WDBJ were shot and killed during a live broadcast. The journalists were 24-year-old Alison Parker and 27-year-old cameraman Adam Ward. A woman being interviewed was also wounded in the shooting, which took place at a shopping mall. Hours after the shooting, the gunman, identified by the authorities as Vester Lee Flanagan II, committed suicide after a chase with state police.

> "News organizations have to ask themselves what [showing the Flanagan video] would do to contribute to public understanding. There is no rulebook for this."
>
> **— Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law**

Flanagan was a former television reporter for WDBJ who also went by the name of Bryce Williams. According to *The New York Times*, Flanagan had worked at the station for less than a year before he was fired in 2013 and had a history of being volatile by threatening co-workers at the news station.

The attack and the horrifying images it produced marked a new chapter in the intersection of video, violence, and social media according to the *Times*. Not only did Flanagan wait until Parker and Ward were on air to begin the attack, but he also recorded his own video from a camera that was seemingly attached to his chest. After the shooting, Flanagan wrote about the event on Twitter, uploaded the video to Facebook, and sent a manifesto to ABC News stating that he was influenced by a June 17, 2015 shooting in Charleston, S.C., as well as the Virginia Tech shooting in 2007 that left 32 people dead. The social media sites disabled Flanagan's profile pages hours after he made the posts.

The images and self-filmed video by Flanagan raised questions about how social media platforms and media organizations should handle such graphic footage. Some major news outlets, including Buzzfeed, CBS News, Yahoo, and the *Daily Beast*, initially embedded Flanagan's point of view video of the shooting in their stories about the event. Other news outlets, such as Fox News, did not show either Flanagan's video or the video from the live broadcast. CNN warned its viewers that it would show the video from the live news broadcast only once an hour and gave a warning before it did. CNN did show Flanagan's point of view video. In an Aug. 26, 2015, YouTube video by the Poynter Institute, senior faculty Al Tompkins and chief ethicist Kelly McBride discussed whether the video would be appropriate in news reporting. McBride said that news organizations should consider what other alternatives, such as editing or commentary, would be available for using the information from Flanagan's self-filmed video while avoiding any promotion of Flanagan's objectives. "News organizations have to ask themselves what [showing the Flanagan video] would do to contribute to public understanding," said Jane Kirtley, director of the Silha Center and professor of media ethics and law at the University of Minnesota on an August 29 broadcast of KPCC Radio's "AirTalk." "There is no rulebook for this."

Debates also arose about default social media website settings that automatically play videos, such as the settings that Twitter and Facebook use. The autoplay features forced some users to unwittingly see Flanagan's video in social media update feeds because others had posted or retweeted the video. Many users expressed outrage when the videos with the graphic images played even though they did not choose to view them. "While autoplay has been embraced by some and called an annoyance by others, its removal of viewer consent is causing trouble when the video in question is about life and death," wrote Jason Abbruzzese in an Aug. 26, 2015 story on *Mashable*.

Media analysts also questioned the decisions of Facebook and Twitter to suspend the social media accounts of Flanagan, removing the comments and video he had posted to their sites. "Every news organization and social media platform observes certain standards of decorum and decency. But sometimes odious material is of great value in understanding the news. Even as the events seemed to still be unfolding, Twitter, Facebook, and LinkedIn should have left the accounts up," wrote *Slate*'s Justin Peters on August 26.

Despite the criticism, some social media sites remained steadfast in their decisions to delete the violent content, pointing

Journalists, *continued on page 27*

Update: Tech Companies, Law Enforcement Continue To Battle Over Strong Encryption for Mobile Devices

Throughout the first half of 2015, the debate over data encryption for mobile phones continued among law enforcement officials, tech companies, and data privacy advocates. Criminal justice officials continued to maintain that strong data encryption created barriers for preventing crime while also calling for updates to laws that would permit law enforcement access to mobile communications. However, tech companies and privacy advocates responded, arguing that the lack of encrypted data on mobile devices created significant cybersecurity problems. Several former national security officials also weighed in on the debate, arguing that strong data encryption processes should not be viewed as a hindrance to law enforcement efforts.

DATA PRIVACY

In September 2014, both Apple and Google announced that they would begin to offer strong encryption as a default setting for the operating systems on their mobile devices. The updated settings would require mobile device users to create a unique passcode in order to access the encrypted data on the devices. Additionally, both Apple and Google said that they had no intention to create "back door" tools that would permit access to any encrypted data on users' devices without the user-created passcode. Although data privacy advocates hailed the new developments, many criminal justice officials, including Federal Bureau of Investigation (FBI) Director James Comey, denounced the new encryption settings, claiming that strong encryption on mobile devices would prevent effective law enforcement. The criminal justice officials argued that the government should be required to establish new laws that require tech companies to build back door tools for access to data found on mobile devices. (For more information on the debate over mobile device encryption, see "Law Enforcement, Tech Companies Clash on Built-in Privacy Features" in the Fall 2014 issue of the Silha *Bulletin*).

> "[T]his is a public conversation that we should end up having. I lean probably further in the direction of strong encryption than some do inside of law enforcement. But I am sympathetic to law enforcement because I know the kind of pressure they're under to keep us safe. And it's not as black-and-white as it's sometimes protrayed."
>
> **— President Barack Obama**

In early 2015, President Barack Obama's administration began weighing whether it would seek new laws mandating tech companies to create back door access to devices. During a February 2015 interview with *Re/code*, Obama explained that he was attempting to find a balance between privacy and law enforcement. "[T]his is a public conversation that we should end up having. I lean probably further in the direction of strong encryption than some do inside of law enforcement," Obama said. "But I am sympathetic to law enforcement because I know the kind of pressure they're under to keep us safe. And it's not as black-and-white as it's sometimes portrayed."

On May 19, 2015, *The New York Times* reported that a group of tech companies, data security experts, and privacy advocates sent a letter to Obama that pushed back against law enforcement officials' arguments for back door access to encrypted devices. The letter emphasized the value of strong data encryption to ensure cybersecurity. "We urge you to reject any proposal that U.S. companies deliberately weaken the security of their products," the group wrote. "We request that the White House instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology. Such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad." The letter was signed by various individu-

Encryption, *continued on page 28*

Journalists, *continued from page 26*

to their policies for removing offensive content. "Our hearts go out to the families affected by this terrible crime," the Google-owned company said in an Aug. 26, 2015 statement. "YouTube has clear policies against videos of gratuitous violence and we remove them when they're flagged."

University of Minnesota Alum Detained in Thailand

Photojournalist and former University of Minnesota student Anthony Kwan was detained at Bangkok's international airport on Aug. 23, 2015 for possessing a bulletproof vest and helmet. The items were discovered in his baggage as he was about to leave Thailand. Kwan had been working for Hong Kong-based Initium Media and covering the aftermath of an August 17 bombing in Bangkok that killed 20 people.

Under Thai law, a license is needed to possess body armor, which is treated as a weapon. Violating the law carries a prison sentence of up to five years. According to a September 8 Associated Press report, many large news organizations require their staff to wear protective gear in dangerous situations. However, freelance foreign journalists have complained that it is difficult to get a license that would allow them to import such equipment.

"I think it's a disgrace to suggest that for a journalist to protect himself constitutes engaging in warfare, it's outrageous," Jane Kirtley, told Minneapolis' Fox 9 News on August 24. "It's a classic example of using the law to intimidate the press."

"Body armor and helmets used by journalists are not offensive weapons and should not be treated as such," said the Foreign Correspondents' Club of Thailand (FCCT) in an August 24 statement about Kwan's arrest. The FCCT urged authorities to drop the criminal case against Kwan.

On September 8, the Minneapolis *Star Tribune* reported that a Thailand court had granted Kwan permission to leave the country until a September 17 bail renewal hearing.

Sarah Wiley
Silha Research Assistant

Encryption, *continued from page 27*

als and organizations such as University of Chicago Law Professor Geoffrey Stone, former White House counterterrorism czar Richard Clarke, the American Civil Liberties Union, Reporters Committee for Freedom of the Press, Electronic Frontier Foundation, Apple, Microsoft, and Cisco Systems, among others. The full letter is available at https://static.newamerica.org/attachments/3138–113/Encryption_Letter_to_Obama_final_051915.pdf.

During a July 2015 hearing before the U.S. Senate Judiciary Committee, Obama administration officials said that they still had not made a decision whether to seek legislation mandating that tech companies create back doors for strong encryption on mobile devices for law enforcement purposes, according to a July 8, 2015 story by Bloomberg BNA. The officials said that the administration would work with tech companies in the immediate future to find individualized solutions to balance law enforcement concerns and mobile data security. However, a joint statement submitted to the committee by Deputy Attorney General Sally Quillian Yates and FBI Director Comey continued to raise concerns over the challenges that new technologies create for older laws intended to aid law enforcement. Specifically, Yates and Comey called for updates to the 1994 Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-1010, which requires telecommunications carriers to build surveillance tools into their technological infrastructure and communications systems for law enforcement purposes.

"At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement," Yates and Comey wrote in their joint statement. "However, due to the revolutionary shift in communications technology in recent years, the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA." The joint statement also noted that the White House administration had not ruled out the possibility of seeking future legislative options. The statement is available at http://www.judiciary.senate.gov/imo/media/doc/07-08 15%20Yates%20and%20Comey%20Joint%20 Testimony1.pdf.

In a July 28, 2015 op-ed, former national intelligence and NSA director Mike McConnell, former Homeland Security Secretary Michael Chertoff, and former Deputy Secretary of Defense William Lynn disagreed with current law enforcement officials' arguments against strong encryption for mobile devices. "We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption," the former officials wrote. "We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."

> "Due to the revolutionary shift in communications technology in recent years, the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by [the Communications Assistance for Law Enforcement Act]."
>
> **— Sally Quillian Yates, Deputy Attorney General James Comey, Federal Bureau of Investigation Director**

The former officials argued that many of the U.S. government officials' ideas about building in back door access to devices for law enforcement purpose were misguided because "malicious actors" could exploit such tools. They also noted, "if the United States can demand that companies make available a duplicate key, other nations such as China will insist on the same." This situation would be problematic because "[t]here will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of government access regimes with varying degrees of due process."

McConnell, Chertoff, and Lynn concluded by observing that previous efforts toward greater encryption of information had not hindered law enforcement efforts, which always adapt. "[In the 1990s], the Clinton administration and Congress rejected [government access to encryption keys] based on reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the '90s and into the new century," they wrote. "Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals."

Casey Carmody
Silha *Bulletin* Editor

Update: *Rolling Stone* Continues to Face Backlash For Campus Rape Story

DEFAMATION

During the summer of 2015, *Rolling Stone* magazine continued to manage the fallout created by the retraction of a November 2014 story detailing an alleged sexual assault on the University of Virginia (UVA) campus. *Rolling Stone* was the target of two separate defamation lawsuits filed in May and July 2015. However, observers have suggested that the plaintiffs in the lawsuits may have to overcome significant legal hurdles in order to be successful in their cases against the magazine. The *Rolling Stone* editor who oversaw the publication of "A Rape on Campus" resigned from his position in August 2015, an action which was directly linked to the retracted story and subsequent legal challenges.

On Nov. 19, 2014, *Rolling Stone* published "A Rape on Campus," which depicted the account of the alleged gang rape of UVA student "Jackie" during a 2012 party at the Phi Kappa Psi fraternity house. The report, written by Sabrina Rubin Erdely, suggested that sexual assaults against women were a regular occurrence during UVA fraternity life. The *Rolling Stone* story also criticized UVA administrators for being more concerned about the institutions' reputation rather than providing adequate support services for rape victims. The story quickly garnered national attention, but Erdely's reporting unraveled under closer scrutiny by other news organizations. On April 5, 2015, the Columbia School of Journalism published a report describing the magazine's failures in investigating the story as well as detailing mistakes that *Rolling Stone* made in adhering to proper journalistic ethical conduct. Specifically, the report criticized Erdely's failure to corroborate derogatory information, the story's use of pseudonyms to obscure information, editors ignoring concerns raised by the story's fact checker, and the magazine not providing Phi Kappa Psi officials with complete information when asking them to respond to the rape allegations, among other problems. That same day, *Rolling Stone* formally retracted "A Rape on Campus." (For more on the publication and criticism of "A Rape on Campus," see "News Organizations Backpedal after Failures to Fact Check, Anchor's False Stories" in the Winter/Spring 2015 issue of the Silha *Bulletin*).

On May 12, 2015, *The Washington Post* reported that UVA Associate Dean of Students Nicole Eramo filed a defamation lawsuit against *Rolling Stone*, the magazine's parent company Wenner Media, and Erdely in Virginia state court. In the complaint, Eramo, who was one of the named UVA administrators in a "Rape on Campus," alleged that *Rolling Stone* had harmed her reputation by casting her as "the chief villain of the story." Eramo argued that *Rolling Stone*'s story and Erdely's subsequent press interviews falsely reported that the associate dean was "indifferent to Jackie's allegations" and misquoted her in saying that "UVA withholds rape statistics 'because nobody wants to send their daughter to the rape school,'" among other false statements. The complaint claimed that once Eramo learned of the alleged rape, she made several efforts to "assist Jackie in holding [the] attackers accountable." Eramo's complaint also argued that *Rolling Stone* and Erdely had demonstrated actual malice, acting with knowledge of falsity or reckless disregard of the truth as defined by *New York Times v. Sullivan*, 376 U.S. 254 (1964), throughout their reporting. She cited several examples, including the fact that the magazine held serious doubts about Jackie's reliability as a source, failed to sufficiently investigate contradictory information, and defended the veracity of the story during subsequent criticism, among other actions. The lawsuit also quoted the Columbia School of Journalism's report as evidence to support its claims. Eramo sought $7.5 million in compensatory damages for the harm to her reputation caused by "A Rape on Campus." The full complaint is available at http://apps.washingtonpost.com/g/page/local/eramo-vs-rolling-stone-complaint/1692/.

> "I am filing this defamation lawsuit to set the record straight — and to hold the magazine and the author of the article accountable for their actions in a way they have refused to do themselves."
>
> **— Nicole Eramo, University of Virginia Associate Dean of Students**

According to the Associated Press, Eramo released a statement the same day she filed the lawsuit, saying, "I am filing this defamation lawsuit to set the record straight — and to hold the magazine and the author of the article accountable for their actions in a way they have refused to do themselves." *The Washington Post* also reported that UVA released a statement in support of Eramo. "[UVA] fully supports and appreciates the professional competency and contributions of Dean Eramo and all of her colleagues who work tirelessly in the support of our students and their safety and well[-]being," the University said in the statement, according to the *Post*. The *Post* reported on May 22 that *Rolling Stone* and Erdely declined to comment on the lawsuit.

In a May 12 post on *The Washington Post*'s *Volokh Conspiracy* blog, Eugene Volokh analyzed Eramo's complaint, suggesting that the dean could face several challenges that might hinder a successful lawsuit. Volokh observed that one major challenge could be a determination of whether Eramo is a public official. As a public official, Eramo would need to prove that *Rolling Stone* and Erdely acted with actual malice, as required by *New York Times v. Sullivan*, which is often difficult to prove. "Eramo, as associate dean of students at a public university — and head of the university's Sexual Misconduct Board — is likely a 'public official,'" Volokh wrote. "[R]elatively high-level university administrators, including ones at Eramo's level, likely are public officials, because they exercise significant influence over a public institution."

Volokh also wrote that Eramo could have difficulty proving that several of Erdely's statements during press interviews about the story are defamatory because the comments appear to be opinions rather than statement of fact. He also wrote that Eramo would need to prove that any statements of fact were indeed false and must "show by clear and convincing evidence that the defendants knew the statements were likely false." Volokh believed that associate dean's best chance for success in the case would center on *Rolling Stone* reporting of Eramo's comments about the university's reputation. "I think that Eramo's strongest claim is about the 'Because nobody wants to send their daughter to the rape school,' because the allegation is clearly a factual claim about her," Volokh wrote. "But even there, she would have to show she didn't say it, and show by clear

Rolling Stone, *continued on page 30*

***Rolling Stone*,** *continued from page 29*

and convincing evidence that Erdely and the *Rolling Stone* editors knew that she likely didn't say it, and that Jackie was lying (or misremembering)."

On July 29, *The Washington Post* reported that three members of Phi Kappa Psi filed a separate defamation lawsuit against *Rolling Stone*, Erdely, and Wenner Media in the United States District Court for the Southern District of New York. The plaintiffs, George Elias IV, Stephen Hadford, and Ross Fowler, claimed that although they were not specifically named in "A Rape on Campus," their reputations had been harmed because people had come to believe that the three were the perpetrators of the sexual assault due to contextual information found in the story. Specifically, Elias, Hadford, and Fowler each graduated from UVA in 2013, which was one of the years that Erdely had reported that the alleged perpetrators had graduated. The complaint also noted that the story's description of the scene where the alleged sexual assault took place was similar to the location of Elias' room in the Phi Kappa Psi house. As a result, "family, friends, acquaintances, coworkers, and reporters easily matched [Elias] as one of the alleged attackers and, among other things, interrogated him, humiliated him, and scolded him. Plaintiffs Hadford and Fowler suffered similar attacks," the complaint alleged. The Phi Kappa Psi members' complaint also pointed to the Columbia School of Journalism's report as evidence that the *Rolling Stone* and Erderly were negligent in their reporting which led to publishing a false story. The fraternity brothers sought $75,000 in damages for each of their two counts of defamation and one count of negligent infliction of emotional distress. The full complaint is available at http://www.scribd.com/doc/272985322/U-Va-Phi-Psi-members-sue-Rolling-Stone.

In a July 30 interview on National Public Radio's "All Things Considered," Media Law Resource Center Deputy Director Jeff Hermes noted the challenges that the Elias, Hadford, and Fowler faced in the pursuit of their lawsuit. "The plaintiffs in this case would need to show not only that they felt embarrassed or felt bad about their association with the fraternity, but that reasonable readers of the article would've understood the statements to refer to them personally," Hermes said during the interview. "They also need to prove that the media outlet failed to take the care that a reasonable person would have in investigating and reporting the story."

The outcome of the lawsuit could turn on the U.S. district court's decision about which state defamation law is most applicable to the case. The federal court could hear the case under Virginia's defamation law, where Erdely's work was completed, or under New York's law, where *Rolling Stone* is located. According to the U.S. Supreme Court's decision in *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974), states have the ability to determine the standard of liability for defamatory statements about private individuals so long as they do not impose strict liability. "Virginia requires proof of negligence. New York requires [the stricter standard of] gross irresponsibility," Hermes told NPR.

> "I really think it's important to keep the line between the law and ethics very firmly drawn. It's up to the lawyers representing these [media] organizations to make sure judges and juries know the ethics codes aren't directly relevant. … The law gives journalists a lot of leeway to do a lot of things that as an ethical matter would be questionable."
>
> **— Jane Kirtley, Silha Center Director and Silha Professor of Media Ethics and Law**

Legal observers also raised concerns over the fact that both Eramo's and the Phi Kappa Psi members' lawsuits pointed to the Columbia School of Journalism's report as evidence that *Rolling Stone* and Erdely acted improperly in their reporting. In the Spring 2015 issue of the Reporters Committee for Freedom of the Press' (RCFP) *The News Media and The Law*, Director of the Silha Center and professor of media ethics and law at the University of Minnesota Jane Kirtley argued that journalism ethics codes, such as the kind described in the Columbia School of Journalism's report, should not be used to enforce the law. "I really think it's important to keep the line between law and ethics very firmly drawn," Kirtley told the RCFP. "It's up to the lawyers representing these [media] organizations to make sure judges and juries know the ethics codes aren't directly relevant. … The law gives journalists a lot of leeway to do a lot of things that as an ethical matter would be questionable."

However, attorney Howard Cooper, who has represented plaintiffs in other libel cases against media organizations, told the RCFP that journalism codes of ethics, such as the Code of Ethics of the Society of Professional, were useful to show "some evidence on issues of negligence and actual malice," despite the fact that such codes were not legally binding. "I think the [Columbia School of Journalism] report will be a tremendous guide during discovery," Cooper said. "It may serve to nail down the testimony of witnesses who are quoted and who are referenced, but it may not be usable in its findings against *Rolling Stone*."

Adding to *Rolling Stone*'s troubles, *The New York Times* reported on July 29 that Managing Editor Will Dana, who had limited involvement with the reporting of "A Rape on Campus" but oversaw publication of the story, announced that he would resign from the magazine on August 7. During the initial criticism of the story, Dana published an apology on the magazine's website that appeared to blame Jackie for the story's discrepancies, which he later amended to clarify that *Rolling Stone* was to blame. In an August 2 story, *Rolling Stone* publisher Jann Wenner told *The New York Times* that Dana's resignation was "a conscious uncoupling" and "it was very important for us to figure out a way to move on" after the controversy over "A Rape on Campus." In the same story, the *Times* reported that Jason Fine, the editor of *Men's Journal*, would become the new managing editor of *Rolling Stone* in mid-August.

Casey Carmody
Silha *Bulletin* Editor

30th Annual Silha Lecture to Feature New York Times Investigative Reporter James Risen and Attorney Joel Kurtzberg

New York Times investigative reporter James Risen, winner of two Pulitzer Prizes, will present the 30th Annual Silha Lecture, "Clear and Present Danger: Covering National Security Issues in the Post-9/11 World" on Monday evening, Oct. 19, 2015. Risen, who fought the U.S. Department of Justice for four years to protect the identity of an anonymous source for his 2006 book, *State of War*, will be joined by attorney Joel Kurtzberg, who led Risen's legal defense in the Justice Department case. Risen and Kurtzberg will discuss the legal and journalistic challenges that arise when reporting the national security beat and using confidential sources.

SILHA CENTER EVENTS

Risen's work focuses on national security and intelligence issues. He won his first Pulitzer Prize for his work in 2001 as part of *The New York Times* reporting team covering the Sept. 11, 2001 terrorist attacks. The second was for his reporting with Eric Lichtblau in 2006 that revealed an illegal National Security Agency wiretapping program. In 2006, Risen published *State of War*, which examined the George W. Bush administration's U.S. intelligence operations after the September 11 attacks.

In 2010, federal prosecutors indicted Jeffrey Sterling, a former Central Intelligence Agency (CIA) officer under the Espionage Act, alleging that Sterling had provided classified information to Risen for *State of War*. Risen's book contained information about the CIA's botched attempt to sabotage Iran's nuclear program, but Risen did not identify his source for this information. In 2011, Attorney General Eric Holder authorized a subpoena that ordered Risen to testify at Sterling's trial. Prosecutors sought Risen's testimony because they claimed that the journalist was the only person who had direct knowledge about whether Sterling actually disclosed any classified information. Risen argued that he had a First Amendment right to protect his source and refused to testify.

In July 2011, United States District Court Judge Leonie M. Brinkema issued an order preventing prosecutors from asking Risen the name of his source, which the DOJ appealed to the United States Court of Appeals for the Fourth Circuit. *United States v. Sterling*, 818 F.Supp.2d 945 (E.D. Va. 2011). In 2013, a Fourth Circuit three-judge panel overturned Brinkema's order. *United States v. Sterling*, 724 F.3d 482 (4th Cir. 2013). Risen petitioned the U.S. Supreme Court in June 2014 to review the Fourth Circuit decision, but the court declined to hear the case. (For more information on the background to Risen's case, see "Espionage Conviction Ends Lengthy Struggle to Compel Journalist's Testimony" in the Winter/Spring 2015 of the Silha *Bulletin*, "Attorney General Holder Leaves Problematic Legacy on Press Rights and Civil Liberties" in the Fall 2014 issue, "Update: Supreme Court Declines to Hear Reporter's Privilege Cases" in the Summer 2014 issue, "Reporters Struggle to Claim Privilege to Avoid Testifying About Confidential Sources" in the Fall 2013 issue, and "Judges Rebuke Government on Leak Prosecutions" in the Summer 2011 issue.)

On Jan. 12, 2015, *The New York Times* reported that the DOJ would not seek Risen's testimony during Sterling's actual trial. "Mr. Risen's under-oath testimony [during a Jan. 5, 2015 moot hearing] has now laid to rest any doubt concerning whether he will ever disclose his source or sources for Chapter 9 of *State of War*. ... As a result, the government does not intend to call him as a witness at trial." Sterling's trial began the following day, and he was subsequently found guilty on several felony counts of violating the Espionage Act despite federal prosecutors relying primarily on circumstantial evidence, according to the *Times*' January 26 story. *The Washington Post* reported on May 11 that Judge Brinkema sentenced Sterling to three and a half years in prison.

The DOJ's decision not to subpoena Risen was welcome news but remained frustrating for press advocates because of the lengthy legal battle the government was willing to pursue for the reporter's testimony. *Times* Executive Editor Dean Baquet said in a statement on Jan. 12, 2015, "I'm glad the government realizes that Jim Risen was an aggressive reporter doing his job and that he should not be forced to reveal his source."

"We said from the very beginning that under no circumstances would Jim [Risen] identify confidential sources to the government or anyone else," Joel Kurtzberg, the lawyer for Risen, told the *Times* the same day. "The significance of this goes beyond Jim Risen. It affects journalists everywhere. Journalists need to be able to uphold that confidentiality in order to do their jobs."

Joel Kurtzberg is a partner at the law firm Cahill Gordon & Reindel LLP in New York who focuses on general commercial litigation. Kurtzberg has extensive experience in legal issues related to media organizations and the First Amendment. He also teaches a mass media law course as an adjunct professor at Brooklyn Law School as well as a course on Internet law as an adjunct professor at Fordham University School of Law. Kurtzberg formerly served as the New York State Bar Association's chair of the Media Law Committee and was an editor of the American Bar Association's *First Amendment and Media Litigation Committee Newsletter*. Kurtzberg graduated from Harvard Law School in 1996 and is admitted to the bar in New York.

At the conclusion of the lecture, Risen and Kurtzberg will take audience members' questions. Copies of Risen's book will be available for purchase, and a book signing will follow the lecture. The Silha Lecture is free and open to the public. No reservations or tickets are required. The lecture will begin at 7:30 p.m. in the Coffman Memorial Union Theater on the East Bank of the Twin Cities campus of the University of Minnesota. Parking is available in the East River Road Garage. Additional information about directions and parking can be found at www1.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 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

Clear and Present Danger

Covering National Security Issues in the Post-9/11 World

1985-2015
THIRTIETH ANNUAL SILHA LECTURE

> OCTOBER 19, 2015
> 7:30PM
> COFFMAN UNION THEATER, UNIVERSITY OF MINNESOTA, EAST BANK
> FREE & OPEN TO THE PUBLIC; NO RESERVATIONS NEEDED
> A SIGNING WILL FOLLOW FOR JIM RISEN'S BOOK, *PAY ANY PRICE: GREED, POWER, AND ENDLESS WAR*

On Monday, October 19, the Silha Center will welcome *New York Times* journalist **James Risen** and his attorney **Joel Kurtzberg** for the 30th Annual Silha Lecture. They will discuss the legal and journalistic challenges of reporting the national security beat and using confidential sources

James Risen covers national security and intelligence issues for the *Times*. He has won the Pulitzer Prize twice—for his work on the team that covered the September 11 terrorist attacks and for his reporting with Eric Lichtblau in 2006 that revealed the National Security Administration's illegal wiretapping program. In 2006, Risen published *State of War,* examining U.S. intelligence operations in the George W. Bush administration after September 11. Federal prosecutors later subpoenaed him for the name of a confidential source for information disclosed in *State of War*. Even after a federal appeals court ruled that he must testify, Risen refused, arguing that he had a First Amendment right to protect his source. Despite the threat of jail, Risen never revealed his source during his years-long battle with the federal government.

A partner at Cahill Gordon & Reindel, **Joel Kurtzberg** has long experience representing media organizations and journalists on First Amendment issues and other constitutional matters. After the Justice Department ended its quest to compel Risen's testimony, Kurtzberg said the battle shows how far the government will go to force a reporter to reveal confidential communications. "The significance of this goes beyond Jim Risen," he told the *Times*. "It affects journalists everywhere. Journalists need to be able to uphold that confidentiality in order to do their jobs."

SILHA CENTER
FOR THE STUDY OF MEDIA ETHICS & LAW