TERROR IN TINSELTOWN: WHO IS ACCOUNTABLE WHEN HOLLYWOOD GETS HACKED

Jessica E. Easterly†

CONTENTS

† J.D. Candidate, Syracuse University College of Law, 2016; B.A. in Mass Communications and Diplomacy & Global Politics, Miami University, 2013. I would like to thank Professor Roy Gutterman for his guidance and patience throughout the note-writing process. Special thanks to my parents for their constant stream of love and support, and to my younger brother, for being a seemingly endless source of irritation and entertainment.

INTRODUCTION

The obsession with celebrity culture has been widespread, pervasive, and heavily critiqued.[1] Movies, television, and celebrity happenings dominate news pages, our conversations, and social media. Hollywood not only has significant say in what information we receive and how we receive it, but also has incredible pull in American politics.[2] When scandal strikes Hollywood, it sends waves through the rest of society,[3] and that is what we saw, and will continue to see, in the wake of the celebrity nude photo leak[4] (known as "the Fappening") and Sony Hacking.

As both hacking events have garnered more and more media attention, conversations involving accountability and the state of the United States' cybersecurity have come to the forefront. This Note will explore the issues associated with each potential party blamed for the hacking or for spreading the content and identify weaknesses in U.S.

1. *See generally* Carlin Flora, *Seeing By Starlight: Celebrity Obsession*, PSYCHOLOGY TODAY (July 1, 2004), https://www.psychologytoday.com/articles/200407/seeing-starlight-celebrity-obsession; Jamie Tehrani, *Viewpoint: Did Our Brains Evolve to Foolishly Follow Celebrities?*, BBC NEWS (June 26, 2013), http://www.bbc.com/news/magazine-23046602.

2. *See generally* KATHRYN CRAMER BROWNELL, SHOWBIZ POLITICS: HOLLYWOOD IN AMERICAN POLITICAL LIFE (2014); TIMOTHY STANLEY, CITIZEN HOLLYWOOD (2014); *see also* Judy Kurtz, *Hollywood Pumps Cash to Save Senate Majority for Democrats*, THE HILL (Aug. 13, 2014, 6:00 AM), http://thehill.com/news/campaign/214990-hollywood-tries-to-save-senate-for-dems.

3. Some notable Hollywood scandals involve Bill Cosby, Heidi Fleiss, and Natalie Wood. Throughout 2014 and 2015, dozens of women have come forward with allegations of Bill Cosby drugging and raping them. *See generally* Charlotte Atler, *Everything You Need to Know About the Bill Cosby Scandal*, TIME (Nov. 24, 2014), http://time.com/3602131/bill-cosby-sexual-assault-allegations-guide/; Noreen Malone, *35 Bill Cosby Accusers Tell Their Stories*, N.Y. MAG. (July 25, 2015), http://nymag.com/thecut/2015/07/bill-cosbys-accusers-speak-out.html. In the early 1990s, news broke of Heidi Fleiss's prostitution ring whose clientele featured many high-powered Hollywood figures. *See generally* Pam Lambert, *Heidi's High Life*, PEOPLE MAG. (Aug. 23, 1993), http://www.people.com/people/archive/article/0,,20106113,00.html. *West Side Story* actress, Natalie Wood, died in a suspicious drowning accident while boating with her husband, Richard Wagner. *See generally* Steve Shapiro, *Natalie Wood's Death, Still Shrouded in Mystery—and the Clues that Remain*, VANITY FAIR (Mar. 2000), http://www.vanityfair.com/news/2000/03/natalie-wood-s-fatal-voyage.

4. The language used in this Article will reflect statistical data that indicate that females constitute the majority of sex crime victims and that most sex crimes are male-on-female. *See* End Revenge Porn, *Revenge Porn by the Numbers*, END REVENGE PORN BLOG (Jan. 3, 2014), http://www.endrevengeporn.org/revenge-porn-infographic/. With that being said, female pronouns will be used to describe victims. This is not meant to discount the experiences of male victims. As of date, the only male to be targeted in this scandal is Nick Hogan, son of famous wrestler, Hulk Hogan. *See* Stephanie Marcus, *Nick Hogan Is the First Male Victim of the Celebrity Photo Hacking Ring*, HUFFINGTON POST (Oct. 6, 2014, 1:59 PM), http://www.huffingtonpost.com/2014/10/06/nick-hogan-hacked_n_5940142.html.

cybersecurity policy. Some people have pointed fingers at the celebrities and Sony, bringing up questions of privacy expectations as a celebrity, consent, and proactivity.[5] The obvious group to blame are the hackers themselves, but how is it possible to track down and prosecute those individuals when it is done anonymously? If the hackers are tracked down, there are further challenges with prosecuting offshore hackers and finding appropriate laws to address all the harm incurred. The websites like Twitter and Reddit have been blamed for facilitating the spread of the stolen content, but in the face of § 230 of the Communication Decency Act,[6] it is nearly impossible to impose liability. The media capitalized on the celebrities' and Sony's misfortunes, presenting questions about the First Amendment and the newsworthiness of the stolen and private information.

Within this Article, Parts I and II will discuss background information and implications on the parties affected by the Fappening and the Sony Hacking, in addition to an overview of current U.S. cybersecurity policies. Subsequent sections will discuss who, if anyone, should be held accountable. In Part III, the Article will address if we should even care at all and place the blame squarely in the celebrities' hands and Sony for not protecting their information, and whether or not one hacking is more or less deserving of recourse. Part IV will examine what redress is available against the hackers themselves. Parts V and VI will explore the question of whether those who spread stolen documents around should be accountable for anything. Specifically, Part V will address whether third-party websites such as Twitter and Reddit can be held liable for their users reposting the stolen information, and Part VI will discuss holding the media accountable, highlighting issues of the First Amendment and privacy.

5. *See* Jenny Kutner, *Ricky Gervais and Fox News Take the Lead in Victim Blaming Over Celebrity Nude Photo Leak*, SALON (Sept. 2, 2014, 12:30 PM), http://www.salon.com/2014/09/02/ricky_gervais_and_fox_news_take_the_lead_in_victim_blaming_over_celebrity_nude_photo_leak/ ("There's this thing called a mirror. If you want to see yourself naked, look in the mirror, don't take a picture of yourself."); Tom Fox-Brewster, *Sony Needed to Have Basic Digital Protection. It Failed*, GUARDIAN (Dec. 20, 2014), http://www.theguardian.com/commentisfree/2014/dec/21/sony-hacking-north-korea-cyber-security ("Sony could have averted this catastrophe if it had simply protected its data better.").

6. Communications Decency Act (CDA), 47 U.S.C. § 230 (2012).

I. THE "HACKGROUND"

Hollywood is quite fond of using cybercrime as a plotline in its films.[7] Little did it know that by the end of 2014, the community would be targeted not once, but twice by computer hackers. The Fappening and the Sony Hacking were real life manifestations of many hacking-centric movies that shook Hollywood to its core and spurred conversations about the United States' cybersecurity policies.

A. The tl;dr[8] of the Fappening

On August 31, 2014, hundreds of nude and compromising photographs of dozens of female celebrities flooded Internet message boards and social media sites.[9] Some of the female celebrities targeted included Kate Upton, Gabrielle Union, and Kirsten Dunst.[10] Jennifer Lawrence, who had almost sixty intimate photos posted, has arguably been the most candid about the event.[11] Upon her photographs being released to the public following the first massive Internet dump, she called for an investigation into the hacking.[12] Her representative deemed it a "flagrant violation of privacy" and even went as far as to warn posters that the authorities would "prosecute anyone who posts the stolen photos."[13]

4chan, a message board-style website, is credited as the source of the photo explosion.[14] It is believed that a few individuals collectively

7. *See* Elizabeth Weise, *Eight All-Time Great Hacking Movies*, USA TODAY (Jan. 15, 2015, 9:12 AM), http://www.usatoday.com/story/tech/2015/01/14/hacking-movies-list-cyber-blackhat/21713327/ (ranking movies such as *War Games*, *The Matrix*, and *Live Free or Die Hard*).

8. A common term standing for "too long, didn't read" used by redditors to summarize lengthy posts. *See tl;dr*, URBAN DICTIONARY (Nov. 20, 2003), http://www.urbandictionary.com/define.php?term=tl%3Bdr.

9. Laurel O'Connor, *Celebrity Nude Photo Leak: Just One More Reminder That Privacy Does Not Exist Online and Legally, There's Not Much We Can Do About It*, GOLDEN GATE UNIV. L. REV. BLOG (Oct. 21, 2014), http://digitalcommons.law.ggu.edu/ggu_law_review_blog/30.

10. *See* Fay Strang, *Celebrity 4chan Shock Naked Picture Scandal: Full List of Star Victims Preyed Upon by Hackers*, MIRROR (Oct. 10, 2014), http://www.mirror.co.uk/3am/celebrity-news/celebrity-4chan-shock-naked-picture-4395155.

11. *See id.*; Kevin Fallon, *Jennifer Lawrence's Furious, Perfect Response to Nude Photo Leak: "It Is a Sex Crime"*, DAILY BEAST (Oct. 7, 2014, 12:14 PM), http://www.thedailybeast.com/articles/2014/10/07/jennifer-lawrence-s-furious-perfect-response-to-nude-photo-leak-it-is-a-sex-crime.html.

12. *See* Ian Simpson, *Actress Jennifer Lawrence Contacts Authorities After Nude Photos Hacked*, REUTERS (Sept. 2, 2014, 6:33 AM), http://in.reuters.com/article/2014/09/02/entertainment-photos-idINL1N0R301820140902.

13. *Id.*

14. *See* O'Connor, *supra* note 9. 4chan, commonly referred to as "one of the darkest

hacked into the celebrities' phones and computers, and then collected and posted these photographs.[15] 4chan users indicated that the hackings took place over several months, with some users even suggesting it has been in the works for years.[16] Further "batches" of nude celebrity photographs were released on September 20, September 26, and October 5.[17]

The incident was deemed "The Fappening," a name inspired by the /r/TheFappening subreddit where most of these photos were posted.[18] In this subreddit, users posted the photos initially released on 4chan, bringing mainstream attention to the leak.[19] At first, the photograph leak was seen simply as gossip fodder and people were clicking on these pictures out of curiosity, not realizing the true harm and implications.[20] But as details of the scandal unfolded, it became clear that the release of these pictures was a clear invasion of privacy and crossed the line into being a sex crime.[21]

B. The Sony Hacking "Cache"-22

The Fappening was not the end to the entertainment industry's hacking woes. In November 2014, Sony Pictures Entertainment's sensitive data and e-mails between employees were leaked to the public.[22] The Sony Hacking is viewed as the first hacking of a company

corners of the Web," is a website that serves as a message board for over twenty million users. Mary-Ann Russon, *What is 4chan? A Look at the Dark Side of the Internet*, INT'L BUS. TIMES (Apr. 22, 2014), http://www.ibtimes.co.uk/what-4chan-look-dark-side-internet-1445644. Initially started as a place to facilitate discussion of anime and Japanese comic books, it has morphed into an amorphous blob of Internet activity, ranging from benign postings to illegal activity. *See id.* 4chan provides an opportunity for users to post comments and photographs unanimously, even allowing users to sign up without any personal information. *Id.* This permits users to hide behind their computer screens and say whatever they want to whomever they want without any punishment. *Id.*

15. *See* Gabrielle Bluestone, *Everything We Know About the Alleged Celeb Nude "Trading Ring" and Leak*, GAWKER (Sept. 1, 2014, 9:05 PM), http://gawker.com/everything-we-know-about-the-alleged-celeb-nude-tradin-1629340923.

16. *See id.*

17. *See* O'Connor, *supra* note 9.

18. *See* Emma Woollacott, *Reddit Gives Mixed Messages After Pulling Leaked Celebrity Photos*, FORBES (Sept. 8, 2014, 9:08 AM), http://www.forbes.com/sites/emmawoollacott/2014/09/08/reddit-gives-mixed-messages-after-pulling-leaked-celebrity-photos/.

19. *Id.*

20. *See* Stan Schroeder, *Perez Hilton Apologizes and Removes Nude Images of Jennifer Lawrence*, MASHABLE (Sept. 1, 2014), http://mashable.com/2014/09/01/perez-hilton-apologizes-and-removes-nude-images-of-jennifer-lawrence/#J8v2ol5NiPkf (apologizing for hastily putting uncensored photos on his gossip blog).

21. *See* Fallon, *supra* note 11.

22. Timothy B. Lee, *The Sony Hack: How It Happened, Who Is Responsible, and*

on U.S. soil from an outside territory.[23] What was also startling about the event was the sheer volume of information with reports suggesting that over 100 terabytes of data were stolen.[24]

A group calling itself the Guardians of Peace (GOP) claimed responsibility for the Sony Hacking.[25] Not only did the GOP obtain information from upcoming Sony movies, but they released hundreds of private e-mails between top Sony executives and well-known celebrities,[26] the documentation of employee's salaries, and personal information of employees and their families such as Social Security numbers.[27]

The hackers threatened they would release more information if Sony did not cancel the release of its movie *The Interview*.[28] Though North Korea initially denied involvement in the hacking, North Korean officials praised the attempt to prevent the release of the movie, claiming that it was an "undisguised sponsoring of terrorism."[29] United States intelligence suggested that the network source and techniques were traced back to North Korea.[30] Many critics viewed the

What We've Learned, VOX (Dec. 17, 2014, 9:00 PM), http://www.vox.com/2014/12/14/7387945/sony-hack-explained.

23. Mark Hosenball & Jim Finkle, *U.S. Suspects North Korea Had Help Attacking Sony Pictures*, REUTERS (Dec. 29, 2014, 7:44 PM), http://www.reuters.com/article/2014/12/30/us-northkorea-cyberattack-idUSKBN0K71FK20141230.

24. James Cook, *The Sony Hackers Still Have a Massive Amount of Data That Hasn't Been Leaked Yet*, BUS. INSIDER (Dec. 16, 2014, 2:19 PM), http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12.

25. William Boot, *Shocking New Reveals From Sony Hack: J. Law, Pitt, Clooney, & Star Wars*, DAILY BEAST (Dec. 12, 2014, 9:30 AM), http://www.thedailybeast.com/articles/2014/12/12/shocking-new-reveals-from-sony-hack-j-law-pitt-clooney-and-comparing-fincher-to-hitler.html.

26. *See id.* Many of the e-mails between top executives have sexist and racist undertones. Records show that popular movie stars like Jennifer Lawrence and Amy Adams were paid significantly less than their male co-stars. *See* Lee, *supra* note 22. Sony executive, Amy Pascal, was exposed calling Angelina Jolie a "spoiled brat" and "talentless." *Id.* Executives made remarks about President Obama only wanting to see *12 Years a Slave* and other movies centered around black characters. Pamela Engel, *Leaked Sony Emails Show Obama Racist Jokes*, BUS. INSIDER (Dec. 11, 2014, 7:55 AM), http://www.businessinsider.com/leaked-sony-emails-show-obama-racist-jokes-2014-12.

27. *See* Steven Musil, *Sony Hack Leaked 47,000 Social Security Numbers, Celebrity Data*, CNET (Dec. 4, 2014, 4:05 PM), http://www.cnet.com/news/sony-hack-said-to-leak-47000-social-security-numbers-celebrity-data/.

28. Lee, *supra* note 22. *See generally* THE INTERVIEW (Sony Pictures Entertainment 2014).

29. Ben Beaumont-Thomas, *North Korea Complains to UN About Seth Rogen Comedy* The Interview, GUARDIAN (July 10, 2014, 3:37 PM), http://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco.

30. Lee, *supra* note 22.

government's findings as "flimsy"[31] but government officials refuted this, claiming the hackers' failure to cover their tracks directly led officials to a North Korean computer system.[32]

With the threat of another release of confidential documents and potential terrorist attacks at the New York premiere of *The Interview*, Sony caved and decided to pull the movie from theaters.[33] This decision was a catch-22 for Sony because if the movie was not pulled from theaters, they would be blamed for a terrorist attack (assuming the hackers carried through with their threats), but if the movie was pulled, Sony would be (and was) crucified for caving to terrorists' demands and diminishing the First Amendment.[34]

II. THE STATE OF CYBERSECURITY

According to a 2013 global threat assessment, cyberattack is the number one global threat against the United States.[35] With that in mind, the United States needs to be taking greater steps toward strengthening the nation's cybersecurity with a concerted effort between the executive and legislative branches.

As stated by the Department of Homeland Security (DHS), "our daily life, economic vitality and national security depend on a stable, safe, and resilient cyberspace."[36] Data suggests that the United States loses $100 billion due to cybercrimes annually, but that number is

31. Dawn Chmielewski, *What If North Korea Wasn't Behind the Sony Hack?*, RE/CODE (Dec. 31, 2014), http://recode.net/2014/12/31/what-if-north-korea-wasnt-behind-the-sony-hack/.

32. FBI James Comey stated at the International Conference on Cybersecurity: "We could see that the IP addresses they used . . . were IPs that were exclusively used by the North Koreans. It was a mistake by them. It was a very clear indication of who was doing this." *FBI: "Sloppy" Hacking Pointed to North Korea Servers*, RE/CODE (Jan. 7, 2015), http://recode.net/2015/01/07/fbi-sloppy-sony-hacking-pointed-to-north-korea-servers/; *see also* Arik Hesseldahl, *How the U.S. Knew North Korea Was Behind the Sony Hack*, RE/CODE (Jan. 18, 2015), http://recode.net/2015/01/18/how-the-u-s-knew-north-korea-was-behind-the-sony-hack/; Bob Orr, *Why the U.S. Was Sure North Korea Hacked Sony*, CBS NEWS (Jan. 19, 2015), http://www.cbsnews.com/news/why-the-u-s-government-was-sure-north-korea-hacked-sony/.

33. Lee, *supra* note 22.

34. *See* Kelly Lawler, *Celebs React to Sony Pulling 'The Interview'*, USA TODAY (Dec. 18, 2014, 9:45 AM), http://www.usatoday.com/story/life/movies/2014/12/17/celebs-react-to-sony-pulling-the-interview/20556345/ (reposting celebrities' negative reactions on social media following Sony cancelling the movie's release).

35. *See Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 113-89 (2013) (statement of James R. Clapper, Dir. of Nat'l Intelligence).

36. *Cybersecurity Overview*, DEP'T HOMELAND SEC. (Sep. 22, 2015), https://www.dhs.gov/cybersecurity-overview.

bound to increase as cybercriminals and cyberattacks become more sophisticated and their growth continues to accelerate.[37] Though the government clearly recognizes the importance of securing cyberspace, it is evident that our Internet laws are being outpaced by cybercriminals.

Cybercrime does not have a universal definition, but generally encompasses two categories of activities.[38] The first category encompasses activities that specifically target computers, such as tampering with networks and programs.[39] The other category consists of using computers to commit traditional offenses like theft and fraud.[40] Cybercrime also covers a wide range of offenses from economic offenses, infringements on privacy, propagations of illegal and harmful content, and even terrorism.[41] Because cybercrime is comprised of multiple activities, it is difficult for lawmakers to properly conceptualize and define it.[42]

For most of the twenty-first century, Congress has not presented a united front in the face of cybercrime. There has been minimal legislative progress since Congress passed two significant acts calling for cybersecurity improvements in 2002. The Federal Information Security Management Act (FISMA) provided mechanisms for federal agencies to improve management and oversight for cybersecurity programs.[43] Also in 2002, Congress passed the Cybersecurity Research and Development Act (CRDA), which called for investments in cybersecurity research and development, including increasing the cybersecurity workforce and strengthening the sharing of data between the public and private sector.[44] CRDA delegated these responsibilities to the Department of Homeland Security, the National Science Foundation, and the National Institute of Standards and Technology.[45] Since then, Congress has been largely unsuccessful in passing more

37. Siobhan Gorman, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, WALL ST. J. (July 22, 2014, 6:49 PM), http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990.

38. *See* Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 249 (2013).

39. *See id.*

40. *See id.*

41. *See id.*

42. *See* KRISTEN FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONG. & U.S. LAW ENFORCEMENT (2015).

43. Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 (2006).

44. *See* Cybersecurity Research and Development Act, Pub. L. No. 107-305, 116 Stat. 2367 (2002).

45. *See id.*

legislation. Acts aimed to further strengthen the cybersecurity infrastructure failed to get through Congress in both 2010 and 2012.[46] Perhaps as a telling illustration of the government's inaction, the biggest accomplishment Congress has had since FISMA and CRDA is passing legislation in support of National Cyber Security Awareness Month.[47]

Recognizing the looming threats to cybersecurity, President Obama issued Executive Order 13636 in early 2013, calling for improvements to the nation's cybersecurity standards and for the development of a national cybersecurity framework.[48] On February 12, 2014, the Official Framework for Improving Critical Infrastructure Cybersecurity was released after a collaborative effort between the public and private sectors.[49] The framework's goal was to provide cost-effective measures to manage cybersecurity risks, and it implemented a voluntary process for businesses and organizations to address their cybersecurity needs.[50]

Following the Fappening and Sony Hacking, the White House announced plans to better protect the United States against cyberattacks.[51] President Obama announced a series of legislative proposals that would help ensure privacy protections of personal information as well as open the lines of communication between the government and the private sector.[52] Furthermore, the Obama Administration announced that the U.S. Department of Energy would provide a twenty-five million dollar grant to support cybersecurity education.[53]

In April 2015, President Obama signed an Executive Order giving the U.S. Treasury Department power to sanction entities worldwide for cyberattacking the United States.[54] It is intended to be a tool to restrict

46. *See* Cybersecurity Act of 2010, S. 773, 111th Cong. (2010); Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

47. S. Res. 306, 112th Cong. (2011).

48. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

49. *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

50. *See id.* at 1.

51. Allison Grande, *White House Unveils Proposal To Bolster Cyber Info-Sharing*, LAW360 (Jan. 13, 2015, 12:23 PM), http://www.law360.com/articles/610916/white-house-unveils-proposal-to-bolster-cyber-info-sharing.

52. *Id.*

53. *Id.*

54. Exec. Order No. 13, 694, 80 Fed. Reg. 18,077 (Apr. 1, 2015); Robert Hackett, *Sanctions: America's Best New Weapon Against Cyber Crime*, FORTUNE (Apr. 2, 2015, 9:47 AM), http://fortune.com/2015/04/02/us-cyber-crime-sanctions/.

resources of those suspects by freezing assets and restricting ability to conduct business in the United States.[55] This was crafted in response to the Sony Hacking, which revealed the need for broader sanctioning authority for cyberattacks rather than seeking individual sanction programs.[56]

Despite the recent barrage of cyberattacks,[57] the United States has never sanctioned individuals specifically for cyberattacks under this new authority.[58] However, experts suggest that it may be employed against China in order to make an example.[59]

First introduced in July 2014, the Cybersecurity Information Sharing Act (CISA) is a controversial piece of legislation designed to improve cybersecurity through the sharing of information of potential threats.[60] The primary purpose is to make it easier for private companies to share information with the government in exchange for legal immunity from privacy and antitrust laws.[61] Opponents maintain CISA encroaches too much on personal privacy even calling it "a surveillance bill by another name."[62] Despite a highly contentious enactment process,[63] Congress later attached a version of CISA as a rider to the

55. *Id.*

56. *Id.*

57. Multiple hackings following both the Fappening and the Sony Hacking have occurred targeting both the private and public sectors. China allegedly stole personal data of millions of federal employees from the Office of Personnel Management. Evan Perez & Shimon Prokupecz, *First on CNN: U.S. Data Hack May Be 4 Times Larger Than the Government Originally Said*, CNNPOLITICS (June 23, 2015), http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/; *see also* Robert Hackett, *Massive Federal Data Breach Affects 7% of Americans*, FORBES (July 9, 2015, 4:22 PM), http://fortune.com/2015/07/09/opm-second-breach-21-million-americans/. United Airlines's systems were breached by China-backed hackers in July 2015. Michael Riley & Jordan Robertson, *China-Tied Hackers That Hit U.S. Said to Breach United Airlines*, BLOOMBERG BUS. (July 29, 2015, 5:00 AM), http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines. Users of the extramarital affair website, Ashley Madison, had their information released and stolen in July 2015. Rich McCormick, *Ashley Madison Hackers Follow Through on Threat to Expose Users*, THE VERGE (Aug. 18, 2015, 8:01 PM), http://www.theverge.com/2015/8/18/9174381/ashley-madison-hack-data-released-by-hackers.

58. Tal Kopan & Jim Sciutto, *Officials: China Cyber Sanctions Could Come Next Week*, CNNPOLITICS (Sept. 5, 2015, 8:49 AM), http://www.cnn.com/2015/09/04/politics/china-cyber-sanctions-us/index.html?eref=rss_latest.

59. *Id.*; *see infra* Part IV.B.

60. *See* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

61. *Id.*

62. Russell Brandom, *Congress Passes Controversial Cybersecurity Bill Attached to Omnibus Budget*, THE VERGE (Dec. 18, 2015, 12:08 PM), http://www.theverge.com/2015/12/18/10582446/congress-passes-cisa-surveillance-cybersecurity.

63. Karoun Demirjian, *Senate Punts Cybersecurity Bill to September*, WASH. POST (Aug. 5, 2015), http://www.washingtonpost.com/news/powerpost/wp/2015/08/05/

"must-pass" omnibus spending package, a 2000-page piece of legislation providing funding for the federal government.[64] President Obama signed the entire bill into law on December 18, 2015.[65] The version of CISA passed allows companies to hand over information directly to the FBI and law enforcement without any vetting system, and it changed the timeliness requirement needed prior to investigation from "imminent threat" to a "specific threat."[66] Critics fear the new version will lead to warrantless surveillance.[67]

Though the government is slowly making progress, it is obvious that as a nation we are not where we should be with ensuring protection of our infrastructure. These weaknesses are making it difficult to address the harm caused to the celebrities and Sony, as well as to deter further attacks. The government needs to take greater initiative and make cybersecurity a top priority instead of placing the onus of protection on individuals. There is reason to believe that cyberwarfare is the weapon of the future and the government needs to take adequate measures to ensure the safety and vitality of the United States.

III. THE VICTIMS

In the aftermath of any crime, there tends to be a discussion of what the victim could have done to prevent the crime. Instead of the perpetrator's reprehensible behavior being the focus, the blame wrongly shifts to the actions of the victim. This has happened both to the celebrities affected through the Fappening and Sony Hacking. Initially, many celebrities were blamed for taking the salacious photos to begin with, but as more and more celebrities spoke out and humanized the crime, the public and media were more willing to understand the incident as it truly was: a sex crime. In comparison, Sony has been nothing short of crucified for not protecting its cyber-infrastructures and its employees. In the face of moral relativism, it is then wrong for Sony to be blamed when both hackings are, at their core, the same.

cybersecurity-faces-key-senate-vote/.

64. *See* Consolidated Appropriations Act, H.R. 2029, 114th Cong. (2015); Andy Greenberg, *Congress Slips CISA into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015, 12:24 PM), http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Tara Seals, *U.S. Congress Passes Controversial Info-Sharing Bill*, INFOSECURITY MAG. (Dec. 21, 2015), http://www.infosecurity-magazine.com/news/us-congress-passes-controversial/.

65. Everett Rosenfeld, *The Controversial 'Surveillance' Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

66. Greenberg, *supra* note 64.

67. Seals, *supra* note 64.

A. Is Consent to Being a Celebrity Consent to Everything?

In the context of celebrity, we have a long standing notion that those who put themselves into public life—whether it be as an actor, musician, athlete, reality television superstar, or even as a politician—should not have an expectation of privacy.[68] Once they thrust themselves into the spotlight, they become a public commodity and every aspect of their lives becomes an issue of public concern.[69] However, just because an individual consents to being in the public life does not mean that such consent extends to all aspects of their lives.[70]

Debates surrounding consent are also implicated with sex offenses. A common argument is that if a victim of sexual assault previously consents to sexual activity with the perpetrator, she consents to *all* sexual activity with the perpetrator.[71] It is superimposing consent in a narrow circumstance to all circumstances. Danielle Citron and Mary Franks in their article about revenge porn analogize the following:

> When a person gives her credit card to a waiter, she is not consenting to let the waiter use that card to make personal purchases. When a person entrusts a doctor with sensitive health information, he is not authorizing that doctor to share that information with the public. What lovers share with each other is not equivalent to what they share with coworkers, acquaintances, or employers. Consent is contextual; it is not an on/off switch.[72]

Unfortunately, the events of the Fappening constitute a sex crime since it is a violation of an individual's bodily autonomy through ways of the Internet.[73] With the Fappening, the idea of celebrities' lives

68. *See* Jamie E. Nordhaus, *Celebrities' Rights to Privacy: How Far Should the Paparazzi Be Allowed to Go?*, 18 REV. LITIG. 285, 289–91 (1999) (explaining justifications for why celebrities' private lives have smaller degree of protections); Donna Freydkin, *Celebrities Fight for Privacy*, USA TODAY (July 6, 2004), http://usatoday30.usatoday.com/life/people/2004-07-06-celeb-privacy_x.htm ("A celebrity is like an elected official. If you're getting paid $20 million a movie, you have to rely on public goodwill to stay in office. You have to accept the fact that you're a public commodity.").

69. *See* Jamie E. Nordhaus, *Celebrities' Rights to Privacy: How Far Should the Paparazzi Be Allowed to Go?*, 18 REV. OF LITIG. 285, 289–91 (1999).

70. Daniel Solove, *Should Celebrities Have Privacy? A Response to Jennifer Lawrence*, LINKEDIN: PULSE (Nov. 17, 2014), https://www.linkedin.com/pulse/20141117100047-2259773-should-celebrities-have-privacy-a-response-to-jennifer-lawrence ("There's no contract that says that in order to be famous one has to surrender privacy").

71. *See Myths/Truths*, SANTA BARBARA RAPE CRISIS CENTER, http://www.sbrapecrisiscenter.org/04Information/myth2.html (last visited Jan. 11, 2016).

72. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 355 (2014).

73. *See* James Kosur, *The Fappening: When Sex Crimes Become Easily Consumable*

belonging to the public collides with the argument that an individual who takes nude photographs and consensually shares them with one trusted individual, consents to sharing them to many individuals. Combined, it creates a horrible concept of female celebrities' bodies belonging to the public.[74]

B. Does Lack of Protection Warrant Blame?

Many critics suggest that Sony was too lax in its cybersecurity infrastructure and made the company vulnerable to attacks. A class action lawsuit filed by Sony's former employees detailed some of the questionable practices that exposed Sony employees' personal information.[75] The complainants alleged that Sony had warning of the attack since the company has been victim to attack in the past, like in 2011 when the PlayStation Network was compromised.[76] Further allegations made were that Sony chose to not provide "adequate data security" for the sake of saving money.[77] In a 2007 interview, Sony's Executive Director of Information Security, Jason Spaltro, said, "it's a valid business decision to accept the risk [of breach]. I will not invest $10 million to avoid a possible $1 million loss."[78] The complaint asserted that internal security was also subpar at the time of the hacking, citing that network and other important passwords were saved in files labeled "password."[79]

The plaintiffs alleged "the hacking has left them vulnerable to identity theft, tax fraud and financial theft," and that in the aftermath, Sony has only cared about protecting its intellectual property and public

Entertainment, BUS. 2 CMTY. (Sept. 2, 2014), http://www.business2community.com/social-buzz/fappening-sex-crimes-become-easily-consumable-entertainment-0995479.

74. *See id.*; *see also Commodifying the Body: Leaked Photos Violate Women's Privacy*, EMORY WHEEL (Sept. 7, 2014), http://emorywheel.com/commodifying-the-body-leaked-photos-violate-womens-privacy/ ("We believe such theft is encouraged by society's commodification of sexuality . . . in which individuals are objectified and open to a system of public transaction and viewing.").

75. Class Action Complaint at 3, Corona v. Sony Pictures Entm't, Inc., No. 2:14-cv-09600 (C.D. Ca. Dec. 15, 2014); *see* Andrea Peterson, *Lawsuits Against Sony Pictures Could Test Employer Responsibility for Data Breach*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/19/lawsuits-against-sony-pictures-could-test-employer-responsibility-for-data-breaches/.

76. Class Action Complaint at 4, 19, *Corona*, No. 2:14-cv-09600 (C.D. Ca. Dec. 15, 2014); Peterson, *supra* note 75.

77. Class Action Complaint at 3, *Corona*, No. 2:14-cv-09600 (C.D. Ca. Dec. 14, 2014); Peterson, *supra* note 75.

78. Peterson, *supra* note 75.

79. *Id.*

image instead of minimizing the harm felt by its employees.[80] Sony and its former employees reached a settlement on September 1, 2015 that was announced in a filing seeking class action status on behalf of nearly 50,000 current and former employees.[81] Released in October 2015, the settlement terms provided for a $2 million cash fund to reimburse 435,000 class members[82] for identity theft preventative members, a two-year plan for identity theft protection services, $2.5 million for class members unable to show damage from the hacking, and $3.5 million in attorney fees.[83] Overall, the settlement is worth between $5.5 million and $8 million and will be approved in March 2016.[84]

There is no clear-cut answer to whether or not Sony should be blamed for its own misfortune for failing to protect itself from a cyber attack. If all of the allegations are true, it is hard to sympathize with Sony, and the company should be accountable to its employees. But to analogize, should a homeowner be responsible for someone breaking into their home if the homeowner does not have security alarms and guard dogs? It is necessary, without a doubt, for Sony to be proactive in the face of crime and also compensate its employees for the harm incurred—but this should not mean removal of all options for redress for Sony as a company.

C. Moral Relativism: Who's More Worthy?

Famed Hollywood producer, Judd Apatow, tweeted the following question: "Releasing private Sony e mails to hurt people is the same as releasing nude photos of Jennifer Lawrence. Why are they ok to print?"[85] Though the Fappening and the Sony Hacking are different in

80. Ted Johnson, *Sony Reaches Settlement in Hacking Lawsuit*, VARIETY (Sept. 2, 2015, 4:02 PM), http://variety.com/2015/film/news/sony-hack-lawsuit-settlement-1201584589/.

81. Associated Press, *Former Sony Employees Whose Data Was Leaked After the Hack Agree to a Settlement*, BUS. INSIDER (Sept. 3, 2015, 10:10 AM), http://www.businessinsider.com/ap-federal-sony-data-breach-lawsuit-settled-lawyer-says-2015-9.

82. The settlement included more class members than what plaintiffs initially anticipated, because the deal covered all Sony Pictures subsidiaries, not just Sony Pictures. Eriq Gardner, *Sony Hack Settlement Gets Judge's Preliminary Approval*, THE HOLLYWOOD REP. (Nov. 25, 2015, 10:29 AM), http://www.hollywoodreporter.com/thr-esq/sony-hack-settlement-gets-judges-843928.

83. *Id.*

84. *Id.*, Associated Press, *Judge Gives Preliminary OK to $8M Settlement Over Sony Hack*, NBC NEWS (Nov. 25, 2015, 8:33 PM), http://www.nbcnews.com/tech/security/judge-gives-preliminary-ok-8m-settlement-over-sony-hack-n469791.

85. Judd Apatow (@JuddApatow), TWITTER (Dec. 11, 2014, 11:11 AM), https://twitter.com/juddapatow/status/543120950552576000.

major and substantive ways, does that make one cybercrime more "worthy" of punishment than another?

The reactions to both Hollywood cybercrimes have received two different responses, possibly a result of who the targets are. The media has generally praised the Sony leak for removing the veil of secrecy surrounding a major corporation, even at the expense of exposing employees' Social Security numbers and family health records.[86] The Sony Hacking is framed as a triumph more than a travesty. Comparatively, the Fappening has been lambasted by the public and media for being a gross invasion of privacy and has correctly been framed as a sex crime.[87] Beloved public figures like Jennifer Lawrence, made vulnerable by having their naked bodies non-consensually exposed to the world, are more sympathetic characters than a faceless multinational corporation.

As stated in a *Washington Post* article, "even if the Sony hack was 'wrong,' the leak of celebrity nudes was more wrong . . . [i]f hacking private documents is wrong, it should be wrong all the time . . . ."[88] When push comes to shove, the issue surrounding both events is the same: someone stole something that was not theirs. Yes, sex crimes are horrible and unfortunate incidents, but simple thefts of property can have potentially devastating consequences as well. Those who are victims of theft are just as deserving of legal recourse as any other victims of crime.

86. *See* Gene Marks, *Can You Guess Who Benefits The Most From Sony's Data Breach?*, FORBES (Dec. 8, 2014, 11:15 AM), http://www.forbes.com/sites/quickerbettertech/2014/12/08/can-you-guess-who-benefits-the-most-from-sonys-data-breach/; Kevin Roose, *Hacked Documents Reveal a Hollywood Studio's Stunning Gender and Race Gap*, FUSION (Dec. 1, 2014), http://fusion.net/story/30789/hacked-documents-reveal-a-hollywood-studios-stunning-gender-and-race-gap/; Sam Biddle, *Sony Hack Reveals 25-Page List of Reasons It Sucks to Work at Sony*, GAWKER (Dec. 3, 2014 3:15 PM), http://gawker.com/sony-hack-reveals-25-page-list-of-reasons-it-sucks-to-w-1666264634.

87. The Washington Post made the following commentary:

> When hackers unknown published the stolen nude photographs of female celebrities in September, the backlash was both fierce and nearly instantaneous: "Anybody who looked at those pictures, you're perpetuating a sexual offense," the actress Jennifer Lawrence told Vanity Fair. "You should cower with shame." But when hackers unknown leaked the stolen salaries, e-mails and PowerPoint presentations of Sony Pictures Entertainment, the public reaction was . . . well, celebratory. For days, sites like Gawker and Buzzfeed have reveled in gossipy dishes from the leaks, such as stars' secret names and the gory details of celebrity feuds. Think pieces have been penned on actors' and executives' salaries. E-mails and salary lists were reprinted in full.

Caitlin Dewey, *What Makes the Sony Hack Any Different From the 'Fappening'?*, WASH. POST (Dec. 12, 2014), http://www.washingtonpost.com/news/the-intersect/wp/2014/12/12/what-makes-the-sony-hack-any-different-from-the-fappening/.

88. *Id.*

IV. THE HACKERS

The obvious parties to blame for hacking the celebrities and Sony are the ones who sat behind the keyboards and perpetrated the crimes: the hackers themselves. Though the hackers are the glaring option to go after, the anonymity of the perpetrators, international laws, and lack of appropriate statutes for prosecution all present challenges in obtaining justice.

A. The Fappening Hackers

In many hacking situations, it is exceptionally difficult to pinpoint who the exact perpetrator is. For example, a hacker may use another computer system to serve as a proxy or employ other methods such as encryption.[89] Social media's facilitation of spreading the nude photos also makes it difficult to track down the source, since the images are shared and reposted on websites throughout the Internet.[90] As of yet, the FBI is still investigating the identity of the hacker or hackers.[91]

In October 2014, investigators identified computers that appeared to have accessed multiple iCloud accounts, including the Fappening celebrities.[92] The FBI raided two homes in the Chicago area, including thirty-year-old Emilio Herrera, and seized multiple technological devices and hard drives.[93] Federal prosecutors regularly filed motions to keep the search warrants sealed until June 2015 when *Chicago Sun-Times* and *Gawker* published Herrera's warrant and corresponding affidavits.[94] On January 15, 2016, *Gawker* identified a second hacker after gaining access to another search warrant and affidavit.[95]

89. Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), http://www.scientificamerican.com/ article/ tracking-cyber-hackers/.

90. Harry Bradford, *Everything We Know About The Unnamed Celebrity Photo Hacker*, HUFFINGTON POST (Sept. 2, 2014, 3:38 PM), http://www.huffingtonpost.com/2014/ 09/02/celebrity-photo-hacker_n_5752642.html.

91. *See id.*

92. Kashmir Hill, *Do the Feds Really Know Who Stole All Those Celebrity Nudes?*, FUSION (June 10, 2015), http://fusion.net/story/148802/fappening-investigation/. *See also* Jon Seidel, *Hollywood's 'Celebgate' Scandal Led Feds from LA to Chicago*, CHI. SUN-TIMES (May 17, 2015), http://chicago.suntimes.com/news/7/71/607529/hollywoods-celebgate-scandal-led-feds-la-chicago; Sam Biddle, *Feds Seized Chicago Man's Computers in Celeb Nude Leak Investigation*, GAWKER (June 9, 2015, 11:41 AM), http://gawker.com/feds-seized-chicago-mans-computers-in-celeb-nude-leak-i-1709153721.

93. *Id.*

94. *Id.*

95. Sam Biddle, *Feds Raided Another Chicago Home in Nude Celebrity Hack Investigation, Still No Charges Pressed*, GAWKER (Jan. 15, 2016, 8:41 PM), http://gawker.com/feds-raided-another-chicago-home-in-nude-celeb-hack-inv-1753200305.

The warrants illuminate the Fappening's scope and potential method. Herrera's IP address was allegedly used 3236 times to access 572 iCloud accounts between May 31, 2013 and August 31, 2014.[96] The exact number of celebrity accounts was not included in the affidavit, but the FBI indicated that "a number" belonged to celebrities and their families and friends.[97] Additionally, it is asserted that the hacking was conducted by phishing for emails and then resetting passwords.[98] Ed Majercyzk used a series of phony e-mail addresses to trick celebrities into giving over their passwords.[99] He gained access to over 300 iCloud accounts over 6000 times, downloaded the photos, and then posted them on 4chan.[100]

Despite this damning evidence, no federal criminal charges have been brought against Herrera or Majercyzk as of January 2016, over one year after the Fappening occurred.[101] In March 2016, Justice Department reached a plea deal with Ryan Collins of Pennsylvania, who claimed responsibility for accessing at least fifty iCloud and seventy-two Gmail accounts during a two-year period.[102] It is unclear if he had any connection with Herrera or Majercyzk.[103] Even if the hackers can be identified, there may be issues with finding appropriate laws under which to prosecute them. Though there are laws on the books to punish for the act of hacking, it is more difficult to find laws to punish for non-consensually posting nude photos since not all states have revenge porn laws, nor is there a federal statute criminalizing it.

The author indicated that these court documents were "more difficult than usual" to obtain after being placed under "restricted access." *Id.*

96. Biddle, *supra* note 92.

97. *Id.* Several of the victims identified in the affidavit stated that they were locked out of their iCloud accounts prior to August and were sent e-mails asking to reset their passwords. *See* Application and Affidavit for a Search Warrant, No. 1:14-mc-00553 (N.D. Ill. Oct. 15, 2014), https://assets.documentcloud.org/documents/2094588/fappening warrant1.txt.

98. *Id.* at 3.

99. Biddle, *supra* note 95.

100. *Id.*

101. *Id.*

102. *See infra* Part IV.A.1; David Gilbert, *'The Fappening' Hacker Pleads Guilty and Reveals How iCloud Accounts Were Hacked*, INT'L BUS. TIMES (Mar. 16, 2016, 5:18 AM), http://www.ibtimes.com/fappening-hacker-pleads-guilty-reveals-how-icloud-accounts-were-hacked-2337354.

103. Sam Biddle, *Man Pleads Guilty to Celebrity "Fappening" Hacks*, GAWKER (Mar. 15, 2016, 5:33 PM), http://gawker.com/man-pleads-guilty-to-celebrity-fappening-hacks-1765100174.

1. Criminal Redress for Hacking

Whoever the Fappening hacker is, prosecutors have federal and state laws that criminalize hacking at their disposal. Many of these laws impose harsh punishments on those convicted, and penalties can range from a few months in prison[104] and a $1000 fine, to up to thirty years in prison and a $10,000 fine.[105]

The federal hacking statute falls under the Cyber Fraud and Abuse Act (CFAA).[106] The statute protects computers connected to the Internet from "trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud."[107] The CFAA makes it a crime to attempt or conspire to commit any of the offenses outlined in § 1030(a) and provides penalties, ranging from a year-long prison sentence to a maximum of life in prison when death results from intentional computer damage.[108]

The CFAA has been used to prosecute celebrity hackers. In 2011, Christopher Chaney was indicted under multiple provisions of § 1030 for hacking the e-mails of and stealing nude photographs and other personal information from about fifty celebrities, including actresses Scarlett Johansson and Mila Kunis.[109] The U.S. District Court of Central California sentenced Chaney to ten years in federal prison and ordered $66,179 in restitution.[110] Though not as wide scale as the Fappening, this case shows that it is possible for whomever the Fappening perpetrator is to be held accountable under hacking statutes.

If the Fappening hacker can be traced, federal prosecutors could charge the hacker under the CFAA. That individual may be held liable under § 1030(a)(2)(C) for intentionally accessing a protected computer without consent of the computer owner.[111] If convicted, the hacker could receive a hefty punishment under § 1030(c)(2)(B)(ii). Since the crime was committed "in furtherance of any criminal or tortious act in

104. *See* CONN. GEN. STAT. ANN. § 53a-251 (West 2014).

105. *See* FLA. STAT. ANN. § 815.01 (West 2014).

106. Cyber Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (1986).

107. CHARLES DOYLE, CONG. RESEARCH SERV., CYBERCRIME: AN OVERVIEW OF THE FED. COMPUTER FRAUD & ABUSE STATUTE AND RELATED FED. CRIMINAL LAWS 1 (2014), https://www.fas.org/sgp/crs/misc/97-1025.pdf.

108. CFAA, 18 U.S.C. § 1030(c); *see* DOYLE, *supra* note 107, at 2.

109. *See* Indictment, United States v. Chaney, No. 1100958 (D. Cal. Oct. 11, 2011), http://www.wired.com/images_blogs/threatlevel/2011/10/hackerazzi-Chaney-indictment.pdf.

110. Alan Duke, *Nude Scarlett Johansson Pic, Hacking Celebs' E-mail Gets Man 10 Years in Prison*, CNN (Dec. 18, 2012, 1:26 PM), http://www.cnn.com/2012/12/17/showbiz/hackerazzi-sentenced/index.html.

111. CFAA, 18 U.S.C. § 1030(a)(2)(C) (1986).

violation of the Constitution or laws of the United States or of any State," the hacker may be fined or imprisoned for up to five years for each celebrity's computer that is hacked.[112]

In fact, federal prosecutors used the CFAA against one of the alleged hackers, Ryan Collins.[113] Collins agreed to plea guilty to a felony violation of CFAA and to one count of unauthorized access to a protected computer to obtain information.[114] Though he admitted to illegally accessing computers, there was insufficient evidence to show he shared or uploaded the information he obtained.[115] Collins' prison sentence has a statutory maximum of five years, but prosecutors have agreed to only recommend eighteen months.[116]

2. Criminal Redress for Revenge Porn

Though there are plenty of laws to address the physical hacking, there are few laws penalizing individuals for non-consensually posting sexually explicit photos of another.[117] The action of posting online nude or sexually explicit photographs or videos of a non-consenting individual with the intent to humiliate has been branded as revenge porn, or non-consensual pornography.[118] Some states have passed revenge porn statutes, providing prosecutors with a valuable tool to combat revenge porn. However, many states and Congress have not been able to pass legislation due to challenges with drafting a statute that casts a wide net of protection while also upholding the First Amendment.

Revenge porn encompasses four categories of activities. The first is the consensual taking and sharing of the photos or videos of a specified individual and the non-consensual sharing of those photos and videos to others by that specified individual.[119] The second category is

112. *Id.* § 1030(c)(2)(B)(ii).

113. Press Release, U.S. Attorney's Office for the C.D. Cal., Pennsylvania Man Charged with Hacking Apple and Google E-mail Accounts Belonging to More than 100 People, Mostly Celebrities (Mar. 15, 2016), https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100.

114. *Id.*

115. *Id.*

116. Plea Agreement at 2, 9, U.S. v. Collins, No. 16-0157 (C.D. Cal. 2016), http://www.scribd.com/doc/304908005/Collins-Plea-Agreement.

117. Less than half of the states have revenge porn laws and there is no federal criminal law. *See infra* note 130.

118. *Frequently Asked Questions*, END REVENGE PORN, http://www.endrevengeporn.org/faqs/ (last visited Jan. 11, 2016).

119. Jenna K. Stokes, Note, *The Indecent Internet: Resisting Unwarranted Internet Exceptionalism in Combating Revenge Porn*, 29 BERKELEY TECH. L.J. 929, 929 (2014).

the non-consensual taking of the photos or videos during consensual sexual activity and then the subsequent, non-consensual sharing of such media.[120] The third category encompasses instances where sexual assault is filmed or documented and then shared online.[121] Situations such as the Steubenville[122] and Rehtaeh Parsons[123] rape cases fall within this category. Finally, the fourth category encompasses photos and videos that are taken through the hacking of phones and computers.[124] The circumstances of the Fappening fall within this category of revenge porn.

Federal legislation has been in the works since March 2014 when Representative Jacki Speier (D-CA) announced she was drafting legislation.[125] Representative Speier will be introducing her bill upon the House's return from recess.[126] A mirror bill will be presented in the Senate.[127] If passed, this could have significant effects on websites allowing user-posted content, because federal criminal law is the exception to § 230 liability.[128] According to Danielle Citron, Professor of Law at the University of Maryland who specializes in cyber-harassment and is a staunch anti-revenge porn advocate, "[a] federal criminal law would be a crucial companion to state efforts. It would provide legal protection against revenge porn in cases where the states

120. *Id.*

121. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014).

122. This case arose after multiple high school football players sexually assaulted a teenage girl in Steubenville, Ohio. The perpetrators videotaped and posted the video on social media. *See generally* Juliet Macur & Nate Schweber, *Rape Case Unfolds on Web and Splits City*, N.Y. TIMES (Dec. 16, 2012), http://www.nytimes.com/2012/12/17/sports/high-school-football-rape-case-unfolds-online-and-divides-steubenville-ohio.html?pagewanted=all&_r=0.

123. Parsons was a Canadian teenager who committed suicide after photographs of her gang rape were circulated on social media websites. Classmates relentlessly bullied her to the point of her family relocating. *See generally Rehtaeh Parsons, Canadian Girl, Dies After Suicide Attempt; Parents Allege She Was Raped By 4 Boys*, HUFFINGTON POST (Apr. 9, 2013, 3:17 PM), http://www.huffingtonpost.com/2013/04/09/rehtaeh-parsons-girl-dies-suicide-rape-canada_n_3045033.html.

124. Stokes, *supra* note 119, at 929.

125. Steven Nelson, *Federal 'Revenge Porn' Bill Will Seek to Shrivel Booming Internet Fad*, U.S. NEWS & WORLD REP. (Mar. 26, 2014, 6:01 PM), http://www.usnews.com/news/articles/2014/03/26/federal-revenge-porn-bill-will-seek-to-shrivel-booming-internet-fad.

126. Kaveh Waddell, *Bill to Criminalize Revenge Porn Coming After Recess*, NAT'L J. (Aug. 12, 2015), http://www.nationaljournal.com/s/70267/bill-criminalize-revenge-porn-coming-after-recess?q=bill%20to%20criminalize%20porn%20coming%20after%20recess&a=&t=&c=&s=None&e=None.

127. *Id.*

128. *See infra* Part V.A; Communications Decency Act, 47 U.S.C. § 230(c)(1) (2012).

either failed to pass legislation or state law enforcement refused to act."[129]

As of March 2016, twenty-six states and the District of Columbia have applicable revenge porn statutes.[130] Even though revenge porn is receiving media and legislative attention, many lawmakers have issues with drafting legislation that encompasses all four categories of revenge porn while protecting the First Amendment. This challenge has been highlighted as California and Arizona have drafted their own laws.

A. California

California's first attempt at revenge porn legislation in October 2013 exemplified problems with victim coverage.[131] Under the initial draft, a revenge porn perpetrator could only be prosecuted if he or she took *and* shared the images.[132] Though it was seemingly satisfactory, it left a substantial subsection of revenge porn victims uncovered: the ones who took "selfies" and then sent them to their partners.[133] This is a

129. Michelle Dean, *The Case for Making Revenge Porn a Federal Crime*, GAWKER (Mar. 27, 2014, 2:45 PM), http://gawker.com/the-case-for-making-revenge-porn-a-federal-crime-1552861507; *see generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (Harvard Univ. Press ed. 2014).

130. ALASKA STAT. § 11.61.120(a)(6) (2014) (harassment in the second degree); ARK. CODE ANN. § 5-26-314 (2013) (class A misdemeanor); CAL. PENAL CODE § 647(j)(4) (West 2014) (misdemeanor); COLO. REV. STAT. ANN. §§ 18-7-107, 18-7-108 (West 2014) (class 1 misdemeanor); D.C. CODE § 20-903 (2012) (felony); DEL. CODE ANN. tit. 11, § 1335 (2014) (class B Misdemeanor, class G Felony); FLA. STAT. § 784.049 (first degree misdemeanor, third degree felony for recidivism); GA. CODE ANN. § 16-11-90 (2015) (misdemeanor); HAWAII REV. STAT. § 711-1110.9 (2014) (class C felony); IDAHO CODE § 18-6609 (2015) (felony, video voyeurism); 720 ILL. COMP. STAT. 5/11-23.5 (2015) (class 4 felony); LA. STAT. ANN. § 14:283.2 (2015) (misdemeanor); ME. STAT. § 511-A (2014) (class D crime); MD. CODE ANN., CRIM. LAW § 3-809 (LexisNexis 2015) (misdemeanor); NEV. REV. STAT. § 2.6 (category D felony); N.J. STAT. ANN. § 2C:14-9 (West 2005) (third degree); N.M. STAT. ANN. § 30-37A-1 (West 2015) (misdemeanor, fourth degree felony); N.C. GEN. STAT. § 14-190.5A (West 2015) (class 1 misdemeanor); N. D. CENT. CODE § 12.1-17-07.2 (class A misdemeanor); OR. REV. STAT. § 161.006 (class A misdemeanor, class C felony if recidivist); 18 PA. STAT. AND CONS. STAT. ANN. § 3131 (West 2015) (second degree misdemeanor, first degree is a minor); TEX. PENAL CODE ANN. § 21.16 (Class A Misdemeanor); UTAH CODE ANN. § 76-5b-203 (LexisNexis 2015) (misdemeanor); VT. STAT. ANN. tit. 13, § 2606 (2014) (misdemeanor); VA. CODE ANN., § 18.2-386.2 (2014) (misdemeanor); WASH. REV. CODE § 9A.90.010 (2010) (gross misdemeanor); WIS. STAT. ANN. § 942.09 (West 2014) (misdemeanor).

131. *See* Julia Dahl, *"Revenge Porn" Law In California a Good First Step, But Flawed, Experts Say*, CBS NEWS (Oct. 3, 2013, 11:54 AM), http://www.cbsnews.com/news/revenge-porn-law-in-california-a-good-first-step-but-flawed-experts-say/.

132. CAL. PENAL CODE § 647(j)(4)(A)–(B) (West 2015).

133. A selfie is defined as "an image of oneself taken by oneself using a digital camera especially for posting on social networks." *Selfie*, MERRIAM WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/selfie (last visited Jan. 11, 2016).

problematic exclusion from the statute's purview since up to eighty-three percent of revenge porn victims fall within this category.[134] California responded to the above concerns regarding the limited category of revenge porn that the statute covered and revised the statute to criminalize revenge porn, no matter who took the photograph or video.[135]

In December 2014, California successfully convicted someone for posting revenge porn under the new law. Noe Iniguez posted topless photographs of his ex-girlfriend on her employer's Facebook page, referring to her as a "slut" and encouraging the employer to fire her.[136] In conjunction with violating multiple restraining orders, Iniguez was sentenced to a year in prison and three years of probation.[137] Los Angeles City Attorney Mike Feuer praised the law and conviction, stating, "California's new revenge porn law gives prosecutors a valuable tool to protect victims whose lives and reputations have been upended by a person they once trusted."[138] He further asserted that the conviction and sentence sends a "strong message" that posting revenge pornography is something the state of California will not tolerate.[139]

B. Arizona

One of the more controversial pieces of legislation combating revenge porn was the law passed in Arizona. Described as "particularly draconian," it has incurred the wrath of First Amendment advocates.[140] It has been criticized as "so poorly written it affects just about anyone who shares or publishes any nude image without explicit consent."[141] The statute, which made it a felony to violate this law, read as follows:

> It is unlawful to intentionally disclose, display, distribute, publish,

134. MARY ANNE FRANKS, DRAFTING AN EFFECTIVE "REVENGE PORN" LAW: A GUIDE FOR LEGISLATORS (2014), http://www.endrevengeporn.org/guide-to-legislation/.

135. Hunter Schwarz, *California's Revenge Porn Law, Which Notoriously Didn't Include Selfies, Now Will*, WASH. POST. (Aug. 27, 2014), http://www.washingtonpost.com/blogs/govbeat/wp/2014/08/27/californias-revenge-porn-law-which-notoriously-didnt-include-selfies-now-will/.

136. Press Release, Office of the L.A. City Attorney, City Attorney Feuer Secures Conviction Under State's "Revenge Porn" Law (Dec. 1, 2014), freepdfhosting.com/b9b7570cb1.pdf.

137. *Id.*

138. *Id.*

139. *Id.*

140. Sarah Jeong, *Is Arizona's Revenge Porn Law Overbroad?*, FORBES (Sept. 23, 2014, 3:58 PM), http://www.forbes.com/sites/sarahjeong/2014/09/23/is-arizonas-revenge-porn-law-overbroad/.

141. *Id.*

> advertise or offer a photograph, videotape, film or digital recording of another person in a state of nudity or engaged in specific sexual activities if the person knows or should have known that the depicted person has not consented to the disclosure.[142]

The Arizona lawmakers neglected to include a newsworthiness exception that would provide protection to those who are using the photographs to accompany news stories and other media.[143] In late September 2014, the American Civil Liberties Union (ACLU) filed suit challenging the constitutionality of the statute in *Antigone Books v. Horne*.[144] On November 28, 2014, the U.S. District Court for the District of Arizona put the Arizona law on hold following an agreement between the American Civil Liberties Union and the State Attorney General, allowing legislators to revise the law.[145] U.S. District Judge Susan Bolton issued a permanent restraint on the revenge porn law in July 2015 after the legislature failed to make changes prior to adjourning in April.[146] On January 13, 2016, the Arizona House of Representatives passed an updated version of the bill, and it is likely to be enacted following the Senate's vote.[147] Described as "a significant improvement," the legislation seeks to rectify past mistakes by adding that the distributor must have malicious intent and the victim must have a "reasonable expectation of privacy."[148]

142. H.B. 2515, 51 Leg., 2d Reg. Sess. (Ariz. 2014).

143. *Id.*

144. Complaint for Declaratory & Injunctive Relief at 30, Antigone Books v. Horne, No. 2:2014-cv-02100 (D. Ariz. Sept. 23, 2014). The plaintiff in this case is a bookseller who distributes books that include depictions of nude models. *See id.* at 5. The nude models consented to the photographs being taken, but did not *specifically* consent to having their nude bodies displayed in the books. *See id.* This legislation is problematic because it encompasses so many different activities that practically anyone could be in violation of the act. *See id* at 4. It also has no harm requirement, which further stretches the category of individuals who could bring lawsuits. *See id* at 5.

145. Bob Christie, *Judge Puts Arizona 'Revenge Porn' Law on Hold*, HUFFINGTON POST (Nov. 26, 2014, 7:53 PM), http://www.huffingtonpost.com/huff-wires/20141126/us-xgr-revenge-porn/.

146. Katie Rucke, *Judge Issues Permanent Restraint on Arizona Revenge Porn Law*, WASH. INTERNET DAILY (July 14, 2015), http://www.washingtoninternetdaily.com/article/view?s=54196&p=1&id=470821.

147. Howard Fischer, *Arizona House Approves 'Revenge Porn' Bill*, ARIZ. DAILY STAR (Jan. 13, 2016, 7:57 PM), http://tucson.com/news/state-and-regional/arizona-house-approves-revenge-porn-bill/article_3a7fee3b-09c7-5e53-8152-0a1fd199918d.html.

148. Elizabeth Stuart, *Revenge Porn Ban Pushed by Arizona Legislators*, PHX. NEW TIMES (Jan. 19, 2016), http://www.phoenixnewtimes.com/news/revenge-porn-ban-pushed-by-arizona-legislators-7983339.

C. Revenge Porn Challenges for the Fappening

Depending where charges against the hacker are filed, the revenge porn option may or may not be available to prosecutors. It is important for the hacker to not only be held liable for the physical hacking, but for the sex crime as well. This would send a strong message that engaging in revenge porn is unacceptable behavior that will be punished severely. However, with only some states having revenge porn statutes and without applicable federal law, there is a chance the hacker would not be punished for violating these celebrities.[149] If suit is filed in California, prosecutors may have success similar to that of Feuer against Iniguez and may be able to provide some justice for the wrong caused by revenge porn.

B. Offshore Hacking

Assuming the validity of the U.S. government's findings that North Korea is behind the Sony Hacking, it will be near impossible for any type of retribution.

First, there are challenges with attempting to redress harm caused by offshore hackers. In May 2014, the United States indicted five members of the People's Liberation Army in China on charges of cyber-espionage.[150] Though the officials will never stand trial, analysts believe that an indictment sends a strong message to China and the world that the United States is capable of tracking down hackers.[151] Though the U.S. Department of Justice could indict North Korean officials if they collect enough proof, it will never lead to a trial, and it is unlikely to deter North Korea from acting again since they know Sony will fold under the threat of potential terrorist attacks.

Second, other methods of punishment are likely to be ineffective against North Korea. The United States' go-to method for punishing other countries is to impose economic sanctions.[152] However, the United States has little to no leverage within the North Korean economy and stringent sanctions against the country are already in place.[153] Following the Sony Hacking, President Obama signed an executive order that

149. *See supra* note 130; *see also supra* text accompanying notes 125−29.

150. Ryan W. Neal, *U.S. Charges Against Chinese Hackers Meant As Warning on Corporate Spying*, INT'L BUS. TIMES (May 20, 2014, 9:58 PM), http://www.ibtimes.com/us-charges-against-chinese-hackers-meant-warning-corporate-spying-1587501.

151. *Id.*

152. Kaveh Waddell, *How Will the U.S. Punish North Korea?*, NAT'L J. (Dec. 23, 2014), http://www.nationaljournal.com/defense/how-will-the-u-s-punish-north-korea-20141223.

153. *Id.*

targeted North Korean officials and its intelligence agency.[154] Analysts suggest that the United States would have to partner with Russia and China, two of North Korea's largest partners, in order to really make an impact on North Korea's financial situation.[155] This would be difficult in and of itself because Russia and China have both been pinpointed as the culprits in other hackings against the United States, such as the April 2015 hacking of the Office of Personnel Management.[156] The United States is planning to impose sanctions on China for the "unrelenting stream of cyberespionage," which will be the first exercise of the executive order.[157]

V. THIRD-PARTY WEBSITES

In the search to find someone accountable for the hackings, many people have been pointing fingers at social media websites such as Reddit and Twitter since they facilitated the spread of the stolen photos and information.[158] However, there will be issues holding these websites accountable due to § 230 of the Communications Decency Act, an important statutory provision that upholds the vitality of the Internet.[159]

A. Section 230 Conundrum

Sony and the celebrities affected by the Fappening will have difficulties in holding websites such as Twitter and Reddit liable, primarily because of the protections websites that allow third-party content have under § 230. Section 230 is considered "both as the savior of free speech in the digital age and as an ill-conceived *shield for scoundrels*."[160] This statutory provision provides immunity to service

154. *See generally* Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 2, 2015); *see also* Jim Acosta & Kevin Liptak, *U.S. Slaps New Sanctions on North Korea After Sony Hack*, CNN (Jan. 3, 2015, 10:01 AM), http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/.

155. *See* Waddell, *supra* note 152; *see also* Shane Harris & Tim Mak, *Obama Could Hit China to Punish North Korea*, THE DAILY BEAST (Dec. 19, 2014, 7:43 PM), http://www.thedailybeast.com/articles/2014/12/19/obama-could-hit-china-to-punish-north-korea.html.

156. Devlin Barrett et al., *U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say*, WALL ST. J. (June 5, 2015, 6:33 AM), http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

157. Kopan & Sciutto, *supra* note 58.

158. *See* Letter from David Boies, Attorney, Sony Pictures Entm't, to Vijaya Gadde, Gen. Counsel, Twitter, Inc. (Dec. 22, 2014), http://www.scribd.com/doc/250802459/Sony-Letter-to-Twitter.

159. CDA, 47 U.S.C. § 230(c)(1) (2012).

160. David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical*

and content providers who allow for third-party users to post content.[161] The implementation of § 230 was "a conscious policy decision by Congress to protect individuals and companies who would otherwise be vulnerable targets to litigants who want to silence speech to which they object, illegal or not."[162] However, there is a potentially dangerous loophole that permits website operators to contain highly objectionable user-submitted content while avoiding liability and still profiting.

Immunity from liability granted to providers and users who publish information provided by others is codified in § 230(c)(1). This provision specifically states, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[163] An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[164] Essentially, intermediaries that host or republish speech are protected against laws that would hold them liable for what other people do and say. Entities that are protected under this provision include Internet Service Providers (ISPs) as well as any website or online service that publishes third-party content.[165] Examples include blog comment sections, message boards, and listservs.[166]

Though many courts have interpreted this provision as an absolute immunity for websites and providers, there are four areas of law that are considered to be exceptions. These exceptions are federal criminal law, intellectual property law, state laws consistent with § 230, and application of the Electronic Communications Privacy Act of 1986.[167] Another limitation is that a site must take action if a user posts child pornography or violates federal intellectual property laws.[168] If

Study of Intermediary Immunity Under Section 230 of the Communications Decency Act, 43 LOY. L.A. L. REV. 373, 379–80 (2014).

161. *See id.* at 379.

162. Matt Zimmerman, *Beyond "Censored": What Craigslist's "Adult Services" Decision Means for Free Speech*, ELEC. FRONTIER FOUND. (Sept. 8, 2010), https://www.eff.org/deeplinks/2010/09/craigslist-beyond-censored.

163. CDA, 47 U.S.C. § 230(c)(1) (2012).

164. *Id.* § 230(f)(2).

165. *See Section 230 of the Communications Decency Act*, DIG. MEDIA LAW PROJECT, http://www.dmlp.org/section-230 (last updated Feb. 18, 2011).

166. *See, e.g.*, Zeran v. AOL, 129 F.3d 327, 328 (4th Cir. 1997) (finding AOL immune from liability for a user's defamatory postings on a message board); Batzel v. Smith, 333 F.3d 1018, 1030–31 (9th Cir. 2003) (conferring immunity on a listserv operator).

167. CDA, 47 U.S.C. § 230(e).

168. *Id.* § 230(e)(1)–(2); *see infra* Part V.A.1.

Congress passes federal revenge porn legislation,[169] it would trigger the exception provision and websites would be liable for users posting revenge porn. This would be a significant change for the Fappening because victims could go after the websites for failing to take down all images.

Within the first decade of its passage, the courts made decisions that broadened the scope of the statute. In *Zeran v. American Online, Inc.*, the Fourth Circuit expanded the scope of § 230 and held that American Online was not liable for a user's defamatory speech on its bulletin board.[170] The court viewed the usage of "publisher" in the statute to encompass both distributors and original publishers.[171] The idea of "absolute immunity" under § 230 has been reigned in within recent years after several circuits addressed questions about what should happen if websites induce the illegal behavior. For example, in 2008, the Ninth Circuit ruled in *Fair Housing Council of San Fernando Valley v. Roommates.com, L.L.C.* that § 230 immunity was not available because the website contributed to user conduct that violated the Fair Housing Act.[172] Roommates.com matched apartment landlords and potential tenants, but required users to answer questions about gender and sexual orientation when signing up for the website.[173] No § 230 immunity was granted because the court said that the website materially contributed to the illegality of the conduct.[174] A similar holding was reached in the Tenth Circuit in *FTC v. Accusearch, Inc.*, after a website solicited users to request phone records protected by the Telecommunications Act of 1996.[175]

Section 230 has been a hurdle for anti-revenge porn advocates after websites post the objectionable photos without the victim's consent.[176] In *Jones v. Dirty World Entertainment Recordings LLC*, the Sixth Circuit overturned the Eastern District of Kentucky's ruling that the website was ineligible for § 230 immunity.[177] TheDirty.com posted the plaintiff's images with a caption describing her sex life and sexually

169. *See supra* Part IV.A.2.

170. 129 F.3d 327, 328 (4th Cir. 1997).

171. *Id.* at 332 (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 113, at 799 (5th ed. 1984)).

172. 521 F.3d 1157, 1164 (9th Cir. 2008).

173. *Id.* at 1161.

174. *Id.* at 1165, 1168.

175. 570 F.3d 1187, 1200 (10th Cir. 2009).

176. *See* GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 759 (Tex. Ct. App. 2014) (overruling lower court decision after finding no material contribution to the illegal content).

177. 755 F.3d 398, 402 (6th Cir. 2014).

transmitted infections.[178] The plaintiff sued both the website and its host for defamation, libel per se, false light, and intentional infliction of emotional distress.[179] However, the Sixth Circuit overturned this ruling in June 2014 by using the "material contribution" analysis under *Roommates.com*, reasoning that simply encouraging the offensive or illegal behavior does not preclude a website from immunity.[180]

Threats have been thrown around regarding potential lawsuits against Reddit and Twitter for having the stolen content on their websites.[181] These lawsuits will not be fruitful due to Reddit and Twitter's § 230 immunity. Reddit and Twitter fall under the definition of "interactive computer service," because these websites host and republish content. It would be inefficient and costly for Reddit and Twitter to comb through the millions of postings and tweets for content that could be potentially objectionable such as libel and harassment and to reallocate resources and manpower to do so. They are also neither encouraging nor materially contributing to the content. Sony threatened to sue Twitter if Twitter failed to stop users from sharing the hacked information, even going so far as requesting tweets regarding the stolen information to be removed and accounts of offending users suspended.[182] If a lawsuit ever did materialize, Sony would not be successful since Twitter would most likely assert a § 230 defense.

1. Some Relief Under Digital Millennium Copyright Act

For the celebrities affected by the Fappening, there is a limited option to circumvent § 230 immunity and force websites to remove photographs. Revenge porn victims generally have the goal of getting these images offline. Though it will not result in monetary damages, celebrities affected by the Fappening can use the Digital Millennium Copyright Act (DMCA), as a method to remove the images.[183]

Under the DMCA, anyone who takes a photo has ownership of the copyright.[184] Therefore, the owner has the exclusive rights to distribute and display the photo.[185] Through DMCA, service providers are protected from liability so long as they comply with "notice and

178. *Id.* at 403, 405.
179. *Id.*
180. *Id.* at 414−17.
181. *See* Letter from David Boies to Vijaya Gadde, *supra* note 158.
182. *Id.*
183. Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(c)(1)(C) (2012).
184. 17 U.S.C. § 201(a).
185. *See id.*

takedown" procedures.[186] A copyright holder can issue a notice to remove or disable access to specific content, and if the website does not comply, the copyright holder can sue for copyright infringement.[187] The statute provides that service providers must "act expeditiously" in response to the takedown request or face potential litigation.[188]

Though this is a solid option to get the photos offline, it does not cover all revenge porn victims and only covers a subsection of what constitutes revenge porn. Copyright ownership extends to those who took the photograph. Therefore, copyright will protect those who took "selfies" of their naked bodies, but does not cover victims who had their partners take the photographs or videos with or without consent.[189] This leaves roughly twenty percent of revenge porn victims uncovered.[190]

Sony sent Twitter twenty DMCA takedown requests and Twitter only removed two tweets from the website.[191] One of the two tweets taken down included screenshots of a *James Bond* script, a work clearly protected by copyright law.[192] The other eighteen tweets were screenshots of Sony e-mails and were not removed by Twitter.[193] There is reason to believe that a fair use defense could be used, because the original tweeter made commentary.[194]

2. Reddit Under Fire

Many of the websites implicated in the spread of the celebrity photos and Sony hackings have been scrutinized for the way they handled each scandal. Considered the primary forum for the spread of the nude photos, Reddit came under significant criticism for the way it responded to the Fappening subreddit even though administrators eventually took down the photographs.

186. *Id.* § 512(c)(1)(C).

187. *Id.*

188. *Id.* § 512(c)(1); *see* Ariel Ronneburger, *Sex, Privacy, and Webpages: Creating a Legal Remedy for Victims of Porn 2.0*, 21 SYRACUSE SCI. & TECH. L. REP. 1, 25–26 (2009).

189. Ronneburger, *supra* note 188, at 18.

190. *See* Mary Anne Franks, *Drafting an Effective "Revenge Porn" Law: A Guide for Legislators*, END REVENGE PORN 1, 9 (Nov. 2, 2015), http://www.endrevengeporn.org/guide-to-legislation/.

191. Jason Koebler, *Sony Tries Again to Make Twitter Delete Hacked Emails, But Twitter Isn't Budging*, MOTHERBOARD (Dec. 25, 2014, 12:50 AM), http://motherboard.vice.com/read/sony-tries-again-to-make-twitter-delete-hacked-emails-but-twitter-isnt-budging.

192. *Id.*; 17 U.S.C. § 102(a)(1) (2012).

193. Koebler, *supra* note 191.

194. *See* 17 U.S.C. § 107 (2012) (permitting individuals to use copyrighted work within the context of commentary and news reporting).

The Fappening highlighted tensions between the First Amendment and privacy rights and pointed out the hypocrisy exhibited by many redditors. The site is deemed to be an outlet to exercise free speech in an unfiltered manner, and the community is fiercely protective over their privacy.[195] Following the Fappening, many redditors claimed the website violated their free speech and effectively censored them.[196] One redditor, arguing the merits of allowing the photographs to be online and the Fappening to continue, stated "[n]o one has the right to say what you shouldn't see . . . it's a slippery slope from some celebrity nudes to political statements to media alteration and blackout."[197] The irony of fighting for the pictures online is that the community that is "fiercely protective" over their own privacy appears to be accepting of revenge porn, which is a clear invasion of privacy, being posted.

In response to the criticism following the Fappening, Reddit officially banned the posting of naked photos without the subject's consent starting in March 2015 and alluded to the website's failure to quickly remove the Fappening.[198] The updated privacy policy incorporates a protocol for those whose illicit photos or videos were non-consensually posted in order to "expedite its removal as quickly as possible."[199]

Though the law may not be able to hold third-party websites liable, market forces can pressure websites to act in conformance with societal values. It is up to the websites themselves to create clear posting policies and hold their users to the terms of service; however, that comes at the risk of angering loyal users.

195. Rob Price, *Celebrity Nude Photo Leaks Reveal Cracks in Reddit's Rules*, DAILY DOT (Sept. 1, 2014, 8:04 AM), http://www.dailydot.com/business/reddit-jennifer-lawrence-kate-upton-nude-photos-leak-privacy-dox-ban/.

196. *Id.*

197. Megaross, TECH. SUBREDDIT, http://www.reddit.com/r/technology/comments/2f568m/in_the_wake_of_reddit_admins_and_mods_censoring/ck653ob (last visited Jan. 11, 2016).

198. Poiutrewq, TECH. SUBREDDIT, http://www.reddit.com/r/technology/comments/2f568m/in_the_wake_of_reddit_admins_and_mods_censoring/ck653ob (last visited Jan.11, 2016); Zach Miners, *Reddit Bans Nude Photos, Sex Videos Posted Without Consent*, PCWORLD (Feb. 24, 2015, 1:30 PM), http://www.pcworld.com/article/2888492/reddit-bans-nude-photos-sex-videos-posted-without-consent.html.

199. *Reddit Privacy Policy*, REDDIT (Apr. 14, 2015), https://www.reddit.com/help/privacypolicy/.

VI. THE MEDIA

In the search to find someone responsible for the Fappening and the Sony Hacking, the media has come under criticism for drawing attention to each event. The First Amendment was implicated through the press as journalists sifted through the nude photographs and Sony documents, and media outlets started to publish and air stories about the Fappening and the Sony Hacking. The Supreme Court has generally supported broad First Amendment protections for the press, but issues of privacy come into play with stolen information from digital sources.

A. History of Press Protection with Stolen Documents

Some critics have called out the media for reporting on content never meant for the public's eyes, but the First Amendment jurisprudence protects the press even when using stolen documents and information. In *New York Times Co. v. United States ("Pentagon Papers")*, the government attempted to prevent publication of classified documents regarding the Vietnam War.[200] The U.S. government petitioned the U.S. District Court of the Southern District of New York to prevent the *New York Times* from publishing the documents.[201] After working its way up to the Supreme Court, it was decided that the government could not prevent the press from publishing information of great public concern obtained from documents stolen by a third party.[202]

In *Pearson v. Dodd*, the court addressed whether or not a newspaper could be held liable for an invasion of privacy cause of action if it published information from stolen documents.[203] The plaintiff in this case, Senator Thomas Dodd, sued reporters Drew Pearson and Jack Anderson for publishing a column of Dodd's misdeeds while in office.[204] Senator Dodd's employees made copies of files from the office unbeknownst to Dodd and provided the material to the defendants, who knew of their stolen nature.[205] The D.C. Circuit Court held that the defendants could not be held liable for an invasion of privacy tort, using the rationale that a claim of invasion of privacy by publication could not stand if the published matter is of a general public

200. 403 U.S. 713, 714 (1971).

201. *Id.*

202. Bartnicki v. Vopper, 532 U.S. 514, 528 (2001) ("In *New York Times Co. v. United States*, the Court upheld the right of the press to publish information of great public concern obtained from documents stolen by a third party").

203. 410 F.2d 701, 703 (D.C. Cir. 1969) (citing Dodd v. Pearson, 279 F. Supp. 101, 102 (D.D.C. 1968)).

204. *Id.*

205. *Id.* at 704–05 (citing *Dodd*, 279 F. Supp. at 102).

concern.[206]

The Supreme Court grappled with the legality of using stolen information once again in *Bartnicki v. Vopper*.[207] The Court also asked what degree of protection the First Amendment provides to "speech that discloses the contents of an illegally intercepted communication."[208] In this case, an unidentified person intercepted and recorded a cellphone conversation between leaders of a teacher's union.[209] This recording was made during a period of time when the school district was in highly disputed collective-bargaining negotiations.[210] A local radio station gained access to the recording and played it on air as a part of a discussion of public affairs.[211] It is different than the *Pentagon Papers* and *Pearson* because the disclosure of the information was not made by the person who stole it, but the disclosing party did know or had reason to know that the information was stolen.[212] The Court pulled from prior First Amendment decisions to reach the conclusion that the First Amendment protects the press from publishing stolen information.[213] Ultimately, the Court found that "a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern."[214]

However, there is reason to believe that the courts may be sympathetic to those who had their privacy invaded and disclosed to the public. An owner of a phone does not waive his or her privacy by using that phone, and the Supreme Court appeared to support that notion in *Riley v. California*.[215] In 2014, the Supreme Court unanimously ruled in favor of privacy rights where police accessed the phone information of a person who they had arrested.[216] Writing for the Court, Chief Justice Roberts acknowledged the great importance cellphones now hold in American society.[217] The Court held that police needed a search warrant before going through an arrested person's phone.[218] Ultimately, this

206. *Id.* at 703, 706 (citing Afro-Am. Publ'g Co. v. Jaffe, 366 F.2d 649, 653 (D.C. Cir. 1966)).
207. 532 U.S. 514 (2001).
208. *Id.* at 517.
209. *Id.*
210. *Id.* at 518.
211. *Id.* at 519.
212. *See Bartnicki*, 532 U.S. at 519.
213. *Id.* at 517.
214. *Id.* at 534.
215. 134 S. Ct. 2473, 2494–95 (2014).
216. *See id.* at 2495.
217. *See id.* at 2489–90.
218. *Id.* at 2495.

shows that we have a reasonable expectation of privacy with our phones, including their contents.[219]

B. Privacy and Celebrity

The right of privacy and privacy torts are fairly recent legal concepts arising from Samuel Warren and Louis Brandeis's 1890 law review article.[220] Warren and Brandeis asserted the need to protect an individual's "right 'to be let alone.'"[221] They were particularly concerned with the media intruding into the affairs of private citizens.[222]

The area of privacy law developed further in the 1960s with William Prosser identifying four categories of rights under the umbrella of privacy.[223] The four rights are as follows: (1) intrusion, or the unreasonable and offensive interference with the seclusion of another; (2) public disclosure of private facts, or giving offensive publicity to private information; (3) false light, or the presentation of information that would provide the general public a false and offensive impression of the individual; and (4) appropriation, or the use of someone else's name or likeness for one's own benefit.[224] The courts have held that celebrities still have a right to some privacy.[225] As a virtue of their newsworthiness, however, celebrities have a lesser amount of privacy than what is enjoyed by ordinary citizens.[226]

Arguably out of the four privacy torts, public disclosure of private facts would be the most applicable to the Fappening. In order to establish this cause of action, the disclosure would need to be highly offensive to a reasonable person and not of a legitimate public

219. Jonathan Bailey, *Celeb Nude Leaks and the Future of Privacy and Copyright*, PLAGIARISM TODAY (Sept. 2, 2014), https://www.plagiarismtoday.com/2014/09/02/celeb-nude-leaks-future-privacy-copyright.

220. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). *See* PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 5 (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf ("Unlike many other torts, which have ancient roots, the privacy torts have a discrete foundation that is only a little over 100 years old").

221. *Id.* at 195.

222. *See id.* at 196.

223. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

224. *Id.*

225. *See* Galella v. Onassis, 487 F.2d 986, 994–95 (2d Cir. 1973) (holding that Jackie Onassis and her family could hold a paparazzo accountable for intruding on their privacy); *see also* Ali v. Playgirl, Inc., 447 F. Supp. 723, 728–29 (S.D.N.Y. 1978) (ruling that an authorized nude caricature of Muhammad Ali violated his right to privacy).

226. Ann-Margret v. High Soc'y Magazine, Inc., 498 F. Supp. 401, 404–05 (S.D.N.Y. 1980).

concern.[227] Disclosing sexual relations is generally considered offensive.[228] Liability for this tort may be circumvented by showing that disclosure is of a public concern, or "newsworthy."

C. Is This Really Newsworthy?

Though there are clear First Amendment protections afforded to the media in its coverage of the Fappening and the Sony Hacking, there is debate about whether or not the content is truly of a legitimate public concern.

The Restatement (Second) of Torts explains what is considered to be a legitimate public concern. It extends to all "matters . . . customarily regarded as 'news'" and also information for educating, amusing, and enlightening the public.[229] Though "newsworthy topics" is a broad category, it is not without limits. The Restatement comments assert that newsworthiness should be determined by taking into account the customs and conventions of the community and that information is no longer of a public concern when it crosses the line into a "morbid and sensational prying into private lives for its own sake."[230]

Though the media has defended the reporting of the Sony Hacking,[231] many have viewed the media as reckless. George Clooney and Aaron Sorkin have spoken out about the media's treatment of the Sony Hacking.[232] In Sorkin's scathing *New York Times* op-ed, he commented on media only contributing to the harm Sony felt by publishing information and not taking the hacking seriously.[233] Calling out journalistic ethics, he states:

> The Guardians just had to lob the ball; they knew our media would crash the boards and slam it in. First, salaries were published. Not by the hackers, but by American news outlets.
>
> Then came the emails. . . .

227. RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

228. *Id.* at cmt. b.

229. *Id.* at cmt. g & j.

230. *Id.* at cmt. f.

231. *See* Alan Murray, *How Fortune Got Inside the Sony Hack*, FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/2015/06/25/fortune-sony-hack-coverage/.

232. *See generally* Mike Fleming Jr., *Hollywood Cowardice: George Clooney Explains Why Sony Stood Alone in North Korean Cyberterror Attack*, DEADLINE (Dec. 18, 2014, 6:14 PM), http://deadline.com/2014/12/george-clooney-sony-hollywood-cowardice-north-korea-cyberattack-petition-1201329988.

233. *See* Aaron Sorkin, Opinion, *The Sony Hack and the Yellow Press*, N.Y. TIMES (Dec. 14, 2014), http://www.nytimes.com/2014/12/15/opinion/aaron-sorkin-journalists-shouldnt-help-the-sony-hackers.html.

> Finally the media got serious. Not because no one gets more use out of the First Amendment than they do, and here was a group threatening to kill people for exercising it. Not because hackers had released Social Security numbers, home addresses, computer passwords, bank account details, performance reviews, phone numbers, the aliases used when high-profile actors check into hotels (a safety measure to keep stalkers away), and even the medical records of employees and their children. But because a stolen email revealed that Jennifer Lawrence was being undervalued.[234]

The legal position that many journalists have put forth represents current understanding and interpretation of the press's First Amendment rights. As stated by Anne Helen Peterson in an exposé for BuzzFeed:

> These documents were obtained through illegal means, but accessing them is not, in fact, illegal; reporting on documents made available through the hack, and even excerpting from them, are covered under both the First Amendment and Fair Use, which protects the reproduction of copyrighted content under the aegis of "enriching" or educating the general public.[235]

Applying the *Pentagon Papers*, *Pearson*, and *Bartnicki* to both the Sony Hacking and the Fappening, it is likely that the First Amendment will protect any media websites who posted the photographs, e-mails, and information. Both incidents are issues of public concern due to the target of the hackings. Celebrities and Hollywood play a pervasive role within our society—whether it be from tabloids in grocery stores or the E! Network. The societal obsession leads to any scandal that affects a portion of Hollywood, especially a large scandal, to become front-page news, and the Fappening and the Sony Hacking are no exception.

While it may be a public concern regarding who was hacked, it might be less of a public concern what the actual content of the stolen items is. The public does not need to know what the naked body of a celebrity looks like or need to know the Social Security numbers and health records of Sony's employees. What makes both the Fappening and the Sony Hacking newsworthy is *who* was hacked, not *what* was hacked.

Media outlets should not be punished for publishing the stories, because it is absolutely necessary to uphold the First Amendment. However, that does not mean the media should not be held to a higher

234. *Id.*

235. Anne Helen Petersen, *The Messy Media Ethics Behind The Sony Hack*, BUZZFEED (Dec. 11, 2014, 5:32 PM), http://www.buzzfeed.com/annehelenpetersen/complicated-sony-ethics.

ethical standard for the type of things they are publishing.[236] Nude photographs of celebrities and the nitty-gritty inner workings of Sony may be salacious and draw in viewers, but at the end of the day, the media needs to put a collective foot down and not publish such devastating private content.

CONCLUSION

Though the Fappening and the Sony Hacking are substantively different, they both are deserving of legal recourse. As seen throughout this Article, there are many parties and circumstances that could be blamed for the actual events or for exacerbating the problem. Though the celebrities and Sony may have made themselves vulnerable to attack, they should not be blamed for being hacked. The hackers are the clear and obvious choice to blame, but it is nearly impossible to identify who the perpetrator is in the case of the Fappening and unlikely for North Korea to be indicted for the Sony Hacking. If the Fappening hacker could be identified, that person could be punished for the act of hacking, but it would be challenging to prosecute for the revelation of nude photos given the limited state of revenge porn laws.

Critics have also pointed the finger at the media and third-party websites such as Reddit and Twitter for exacerbating both situations. Social media websites are immune from liability through § 230, but still need to follow intellectual property laws. Essentially, it comes down to social media websites having clear-cut posting policies stating what content is acceptable. With the media, there are First Amendment protections when it comes to publishing stolen material supported through a long line of cases. However, the media should think twice about who will be harmed when they publish stolen material and exercise some restraint in the case of private nude photos and the personal information of a company's employers.

All in all, the Fappening and the Sony Hacking are a testament that the U.S. cybersecurity policies are not up to par. It is of the essence that the government takes more aggressive steps in revamping our cybersecurity policy. In the meantime, the burden falls on companies and individuals to be proactive to protect themselves.

236. *See generally* Richard T. Karcher, *Tort Law and Journalism Ethics*, 40 LOY. U. CHI. L.J. 781 (2009) (discussing ethical obligations when reporting on high profile people especially in tabloid-style journalism).