NOTE

LOOK OVER YOUR FIGURATIVE SHOULDER: HOW TO SAVE INDIVIDUAL DIGNITY AND PRIVACY ON THE INTERNET

I. INTRODUCTION

Pervasive image capture via modern handheld technologies, combined with the universal and excessive use of the Internet, has caused a breakdown of privacy norms.[1] Erin Andrews, a sports news journalist, has provided a face to the victimization of the masses of people whose privacy has been infringed due to the unlawful capture and online dissemination of their private images.[2] In July 2009, Andrews received a phone call from a friend telling her there was a video on the Internet of a naked girl in a hotel room, and people were identifying her as that woman.[3] Until that summer, Andrews—"one of ESPN's most popular sideline reporters"[4]—was mostly known only to football fans.[5] In an article published two years after the surreptitiously captured video of Andrews went viral, she explained that even though her stalker is behind bars, her legal battles continue.[6] She commenced a civil suit against the hotel where her stalker filmed her, lobbied for better

1. *See* Jacqueline D. Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 927 (2010).

2. *See* Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspace*, 18 CARDOZO ARTS & ENT. L.J. 469, 476-77 (2000) (explaining how often people are unknowingly taped in situations where they expect to have privacy); Leslie Casimir, *The ESPN Girl Takes a Stand*, GLAMOUR, Apr. 2010, at 161, 162 (explaining how Andrews was a stalking victim, an issue that has become widespread in the United States, and how she can be a public voice against stalking); Abigail Pesta, *The Haunting of Erin Andrews*, MARIE CLAIRE, Aug. 2011, at 94, 96 (highlighting the efforts made by Andrews, as a well-known victim, to publicly address this issue).

3. Pesta, *supra* note 2, at 95.

4. *ESPN's Erin Andrews Speaks Out*, OPRAH (Sept. 11, 2009), http://www.oprah.com/oprahshow/ESPNs-Erin-Andrews [hereinafter OPRAH].

5. Casimir, *supra* note 2, at 161.

6. Pesta, *supra* note 2, at 94; *Lawyer: Erin Andrews to Sue over Nude Video*, FOX SPORTS (Feb. 23, 2010, 2:19 PM), http://msn.foxsports.com/other/story/Lawyer:-Erin-Andrews-to-sue-over-nude-video [hereinafter FOX SPORTS].

legislation against stalkers, and sought to obtain the copyright to the viral video in order to send cease-and-desist letters to websites still providing access to the footage.[7] Most, but not all, traces of this video have been removed from the Internet.[8]

The wide scale removal of Andrews's viral video from the Internet was an incredible accomplishment because removing any image from the Web that is not protected by copyright is almost impossible.[9] In fact, even in Andrews's case she was warned that she was "just going to have to get used to the fact [that she would] probably never get it all off."[10] The almost complete wipeout of Andrews's video from the Internet was primarily a result of Andrews's celebrity status, and the additional power that status provides to fight these legal battles.[11] She has also used this influence to raise awareness about stalking and online dissemination, which plague countless women.[12]

This Note proposes that Congress enact "takedown" legislation to deal with the void in telecommunications law that fails to address the cyber-exposure of individuals who are filmed in their private quarters unknowingly and unlawfully. It further seeks to explain why the Internet can no longer go completely unregulated with regard to these issues in particular. Finally, this Note will suggest that takedown measures are both the most effective and least restrictive means of salvaging what is left of our individual privacy rights, as they exist in the age of the Internet. In Part II, a history of privacy law will be provided, including early conceptions of privacy and modern developments of the somewhat ambiguous right. The historical background will then shift to the creation of the Internet and the structural mechanisms available for its

---

7. Pesta, *supra* note 2, at 94-95.

8. *See id.* at 95; FOX SPORTS, *supra* note 6; OPRAH, *supra* note 4.

9. *See* Lipton, *supra* note 1, at 930 (explaining that no law currently exists that provides a takedown structure for images violating individual privacy if the victim does not own a copyright on the material); Pesta, *supra* note 2, at 95 (describing Andrews's difficulty in having her unauthorized image removed from the Internet, and the need for her legal team to obtain a copyright in order to send cease-and-desist letters to websites using the image); OPRAH, *supra* note 4 (expressing that Andrews's lawyers have worked to remove "every trace of the video").

10. OPRAH, *supra* note 4.

11. *See* Andy Soltis, *ESPN Hottie in Peep Shocker*, N.Y. POST, July 21, 2009, at 3 (reporting that ESPN took action on behalf of Andrews to ensure the video would be yanked from the Internet, including derivative versions that popped up on YouTube).

12. *See* Casimir, *supra* note 2, at 162 (explaining that Andrews feels "she has a duty to help other victims who are not in the national spotlight"); Pesta, *supra* note 2, at 96 (stating that she received "a ton of letters from women who were stalking victims" who asked her to be their voice and fight this widespread invasion of privacy); *see also* Martha C. Nussbaum, *Objectification and Internet Misogyny*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 68, 68 (Saul Levmore & Martha C. Nussbaum eds., 2010) (explaining how a "significant proportion" of harmful material on the Internet objectifies women, "treating women as objects for men's use and abuse").

regulation. Then the two discussions will merge to address the ways in which the Internet has changed privacy standards and reshaped the American public's understanding of privacy.

Part III will lead to the formulation of the problem, including the rise of Internet crime, the larger issues of needing to change the present system of an almost entirely unregulated Internet, the increased issues of unlawful Internet postings, and the lack of remedial options for those who have been harmed by third party postings. Part IV will discuss the proposed twofold solution. The enactment of wholly new legislation, which will provide a new regulatory structure enabling the tracking of Internet misconduct to specific individuals, and will address the takedown of unlawful and privacy infringing images, within proposed parameters. In explaining this proposal the paper will further delve into previously enacted statutory provisions along with other past attempts to regulate certain content on the Internet. There will also be a discussion of potential constitutional concerns, including First and Fourth Amendment issues. Part V will synthesize the discussion and will explain why, from a humanistic perspective, society must demand that privacy be protected. Altogether, this Note will hopefully lead to a better understanding of why society does not need to capitulate to the changes new technologies impose, specifically why utilizing the benefits of the Internet and other technologies does not necessarily conflict with protecting our basic value system.

II. HISTORY OF PRIVACY, PRIVACY LAW, AND THE INTERNET

Privacy over one's personal information, choices, or space is often taken for granted until it is infringed upon, but recently, sensitivity to such violations has increased due to the frequency and severity of privacy infringements on the Internet.[13] Privacy law has been continuously reshaped since its inception, and the "right" has been defined in terms of constitutional, statutory, and common law structures.[14] This evolution is in large part due to changes in society, most recently the introduction of the Internet into our daily lives. The Internet, like privacy, has also changed over time.[15] This change is evidenced by the Web's increasingly widespread and regular use by the

13. *See* Calvert & Brown, *supra* note 2, at 478 (stating how more than a hundred websites provided private videos of unsuspecting victims); Lipton, *supra* note 1, at 922 (discussing the "worrying new trend [of] peers intruding into each other's privacy"); *see, e.g.*, Pesta, *supra* note 2, at 95 (describing Andrews's shocked reaction when she found out a secret video of her undressing in a private hotel room had been publicly disseminated over the Internet).

14. *See* discussion *infra* Part II.A.1–3.

15. *See infra* text accompanying notes 76-79.

masses.[16] The Internet has made daily life easier in many ways, but it has also presented new dangers.[17] Thus, a difficult balancing act has ensued in protecting the public from Internet crime and privacy infringements while remaining true to constitutional principles.

A. The History of Privacy

In 1890, Samuel Warren and William Brandeis proposed the idea of a privacy tort and adopted Judge Cooley's concept of every individual's "right to be let alone."[18] Their goal was to protect the idea of respecting one's fellow neighbor and friend, and subsequent scholarship found that privacy tort law protects "socially-accepted codes of civility."[19] The concept of privacy has varied in many ways.[20] Most legal theorists define privacy as a person's right to control his or her own personal information.[21] Others see it as a function of accessibility or control over one's public appearance,[22] while still others see privacy as the basic definition of maintaining secrecy and one's personhood.[23] Some legal scholars have been able to break down the multitude of privacy rights into four general spheres of interest: the right over one's personal information; autonomy; physical space; and property.[24] In his essay titled *Privacy*, Justice Charles Fried dug beyond general spheres by deeming privacy as the essence of relationships and the underlying values of respect and trust.[25] These various explanations of privacy provide guidance, but without a clear definition of this "right," courts have had to resort to basic "concepts of space, subject matter, secrecy,

16. *See infra* text accompanying notes 85, 94-97.

17. *See infra* text accompanying notes 98-101.

18. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 195, 213, 219 (1890).

19. *See* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 8 (2007).

20. *See* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 88-89 (2002) (discussing the various ways definitions of privacy apply to the Internet, including the right to privacy of one's personal information such as their name, address, medical, or financial records; the right to confidentiality in one's online exchanges or anonymity while conducting certain transactions online; the right to personal security; and the right to be free from misuse of one's information); *see also* text accompanying notes 291-94 (discussing the legislative enactments that forced a certain level of privacy protection when new wiretap technology began to be used more frequently in police investigations).

21. *See* Hahn & Layne-Farrar, *supra* note 20, at 88.

22. *See id.* at 88-89.

23. Abril, *supra* note 19, at 7-8.

24. *See* JON L. MILLS, PRIVACY: THE LOST RIGHT 14 fig. (2008) (providing a diagram to show what types of information and what types of invasive actions fall within each category or how they might fall into more than one of the categories).

25. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).

and seclusion."[26] Even today, judges and legal practitioners remain confused about how to define privacy and whether or not it is an inherent right.[27]

1. The Constitution on Privacy

The Constitution does not explicitly grant a right to one's privacy, but the U.S. Supreme Court has defined certain "zones of privacy" within the Bill of Rights.[28] The Justices of the Court have recognized the importance of the right to privacy under certain circumstances, such as in the case of *Griswold v. Connecticut*[29] where the Court held that the right to privacy in marriage is fundamental.[30] At other times its decisions have required that privacy take a back seat to freedom of speech, as in the case of *Cox Broadcasting Corp. v. Cohn*,[31] where the Court held that the First and Fourteenth Amendments protected the press from civil liability for posting the name of a rape victim, whose information was derived from a public court record.[32] In *Cohn*, as in many other cases, the preservation of privacy has often been balanced against First Amendment concerns of "chilling speech."[33]

The Fourth Amendment and the framework of property rights are the legal tools most often drawn by the Court to resolve issues involving the right to privacy.[34] Two legally recognized classes of "privacy" rights have come from constitutional jurisprudence: (1) the individual interest in protecting sensitive information from disclosure or misuse, and (2) the interest in making personal decisions independently, or conducting one's personal activities without observation or intrusion.[35] These categories of

---

26. *See* Abril, *supra* note 19, at 3-4 (describing how classic conceptions of privacy are linked to physical space); Hahn & Layne-Farrar, *supra* note 20, at 88-90 (explaining how the concept of a privacy right in property can extend to the Internet and technological space, and further confirming that there has been no consensus on a general definition of privacy as a "right").

27. *See* Lipton, *supra* note 1, at 941-43.

28. JONATHAN ROSENOER, CYBERLAW: THE LAW OF THE INTERNET 130 (1997) (internal quotation marks omitted).

29. 381 U.S. 479 (1965).

30. *See id.* at 485-86; *see also id.* at 494 (Goldberg, J., concurring) ("[T]he right of privacy is a fundamental personal right, emanating 'from the totality of the constitutional scheme under which we live.'" (quoting Poe v. Ullman, 367 U.S. 497, 521 (1961) (Douglas, J., dissenting))).

31. 420 U.S. 469 (1975).

32. *Id.* at 472-73, 491.

33. *See id.* at 489; Lipton, *supra* note 1, at 944. Free speech often clashes with privacy because one person's "privacy can be in direct conflict with another's desire to speak about that person's life." Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 761 (2007).

34. *See* ROSENOER, *supra* note 28, at 130.

35. *Id.* at 130-31.

protection sometimes overlap to ensure various informational privacy protections, but they only protect infringements by government actors.[36]

2. Legislation on Privacy

Congress has addressed some specific privacy issues that have arisen in the age of the Internet through the enactment of privacy protection laws.[37] In the mid-to-late nineties, when criminals started to figure out ways to manipulate the open structure of the Internet, Congress stepped in with legislation.[38] The laws protected particularly sensitive information like financial and health records, or especially vulnerable groups like children.[39] Some of these laws are more effective than others, but the mere enactment of such legislation is part of an ongoing effort to protect personal information from public exposure as developing Internet technology makes it more readily available.[40]

3. Common Law on Privacy

To fill in the fairly large gaps in privacy legislation, the common law is another means of protecting individual privacy interests from interference by non-government entities. William L. Prosser "cemented" the common law right to privacy by categorizing four activities that give rise to liability.[41] The first category includes the invasion of privacy by intrusion upon seclusion, which encompasses the act of "physical, electronic or mechanical intrusion into someone's personal life," including gathering personal information even if that information is never publicized.[42] The second tort, public disclosure of private facts, protects individuals from having private (often truthful) facts published

---

36. MILLS, *supra* note 24, at 124; ROSENOER, *supra* note 28, at 13.

37. ROSENOER, *supra* note 28, at 132; *see also infra* text accompanying notes 304-08. U.S. legislation pales in comparison to the European Union Data Protection Directive, which takes a much stronger stance on protecting personal information, specifically in terms of who may collect information and for what purposes. Hahn & Layne-Farrar, *supra* note 20, at 116-17, 120.

38. *See* Hahn & Layne-Farrar, *supra* note 20, at 120-24, 126. Some states also passed legislation. *Id.* at 125.

39. *Id.* at 121-23. Some of the more significant federal legislation includes: the Identity Theft and Assumption Deterrence Act, the Consumer Credit Reporting Reform Act, the Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, and the Electronic Communications Privacy Act. *Id.*

40. *See id.* at 126, 134-36. Various tools are used to protect a person's online identity, due to the fact that websites and e-mail servers can easily detect one's identity through an IP address or online cookies. *Id.*

41. Abril, *supra* note 19, at 8-9 (describing Prosser's four categories privacy torts). Prosser based his privacy tort structure off of Warren and Brandeis's 1890 paper titled *The Right to Privacy*, which provided the underpinnings of privacy law. *See id.* at 8.

42. Brian Kane, *Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy*, 20 ALB. L.J. SCI. & TECH. 327, 347-49 (2010).

when the revelation of such intimacies would offend a reasonable person.[43] The third kind of harm, publicity placing a person in false light, includes malicious conduct that gives an inaccurate—usually negative or embarrassing—impression of another, which is offensive to a reasonable person.[44] Finally, the fourth invasion of privacy by appropriation governs the unauthorized "use of someone's likeness for commercial purposes."[45]

The two torts most affected by the changes arising from the Internet and other technologies are the intrusion upon seclusion and the public disclosure of private facts.[46] These torts "are largely incapable of remedying the intrusiveness" of increasingly invasive technologies.[47] According to the *Restatement (Second) of Torts*, to succeed on an intrusion upon seclusion claim, a plaintiff must show that the defendant: (1) "intentionally intrude[d], physically or otherwise"; (2) "upon the solitude or seclusion" of the plaintiff's "private affairs or concerns"; and that (3) the invasion of the plaintiff's privacy "would be highly offensive to a reasonable person."[48] In the Internet context, this tort is used to protect against the unlawful gathering of information which a reasonable person would expect to remain private.[49] For the tort of publicity of private life, there must be a showing of: (1) publicity; (2) of a private matter; and (3) that the material publicized "would be highly offensive to a reasonable person"; and (4) "not of legitimate concern to the public."[50] However, this tort does not provide protection for observations in public places or activities that are considered newsworthy.[51]

Existing criminal laws and tort statutes cover some online activity, specifically online postings of images captured unlawfully or by means that invade the image subject's privacy. For example, Erin Andrews's stalker, Michael David Barrett, was charged with "interstate stalking with intent to harass, intimidate and cause emotional distress."[52] After

43. *Id.* at 347-48, 350.

44. *Id.* at 347-49.

45. *Id.* at 347-48.

46. *See* Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet*, 49 SANTA CLARA L. REV. 313, 314 (2009).

47. *Id.*

48. RESTATEMENT (SECOND) OF TORTS § 652B (2000).

49. Kane, *supra* note 42, at 349.

50. RESTATEMENT (SECOND) OF TORTS § 652D.

51. Kane, *supra* note 42, at 350; *see also* MILLS, *supra* note 24, at 17 (explaining that "the law will bend to allow the disclosure of personal information under the First Amendment when the social value of such information is 'newsworthy'").

52. Kevin Deutsch, *Erin Andrews Peephole Video Arrest: Suspect Michael David Barrett a Caring Dad, Family Says*, N.Y. DAILY NEWS (Oct. 3, 2009), http://articles.nydailynews.com/2009-

pleading guilty, Barrett received two and a half years in prison.[53] Andrews also filed a civil lawsuit against the hotel where she was taped because it cooperated with her stalker's requests for information about her stay there.[54] This is an example of a case where the laws allowed the victim to feel a sense of justice for the underlying crime and privacy infringement.[55] The Erin Andrews case clearly contains the elements of intrusion upon seclusion and publicity of private life.[56] However, in scenarios where the perpetrator cannot be identified or when the law does not provide a remedy for the infringement, justice is not possible.[57]

There is a call for tort reform to address the gaps in the law, which presently do not cover an array of new online intrusions.[58] The boom in social networking and blogging, in combination with the modern world's extensive use of camera phones and small recording devices, has complicated the definition of privacy and exposed the limitations of the antiquated tort structure in the United States.[59] For example, publicly captured images may sometimes include private interactions or moments, but do not receive tort protection if disseminated without permission.[60] With the abundance of surveillance cameras, the creation

---

10-03/gossip/17934811_1_erin-andrews-peephole-videos.

53. *Erin Andrews' Video Voyeur Gets 2½ Years*, CNN (Mar. 15, 2010), http://articles.cnn.com/2010-03-15/justice/espn.erin.andrews.sentence_1_erin-andrews-michael-david-barrett-videos?_s=PM:CRIME [hereinafter *2½ Years*].

54. *See* Pesta, *supra* note 2, at 94, 96 (describing how Andrews "filed a civil suit against the hotel where the video was shot" and the ease with which one could find out about her hotel reservations simply by calling the hotel); Deutsch, *supra* note 52 (reporting that Andrews's lawyer stated that various hotels provided her stalker with her reservation information and would give him a room adjoining hers).

55. *See 2½ Years*, *supra* note 53; Pesta, *supra* note 2, at 96.

56. *See* RESTATEMENT (SECOND) OF TORTS § 652B, D (2000) (providing the elements of the intrusion upon seclusion and publicity of private life torts).

57. *See* Lipton, *supra* note 1, at 930 (discussing the limitations of privacy torts with specific emphasis on state codes that have no application in certain online contexts); Wesley Burrell, Note, *I Am He As You Are He As You Are Me: Being Able to Be Yourself, Protecting the Integrity of Identity Online*, 44 LOY. L.A. L. REV. 705, 713 (2011) (discussing anonymous Internet users and the failure of Internet Service Providers ("ISPs") to collect or retain their identifying information via IP addresses).

58. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1827-28, 1830 (2010) (describing how privacy torts do not redress a variety of potential intrusions into privacy on the Internet).

59. *See* Abril, *supra* note 19, at 12 (describing the flaws in traditional tort law when applied to social networking); Lipton, *supra* note 1, at 927 (describing the ease with which people can capture images and disseminate them via the Internet); *see also* Kane, *supra* note 42, at 352 (explaining that there has been an unintentional stagnation in traditional privacy law and how now might be the appropriate time to modify privacy laws in relation to the Internet).

60. *See* Kane, *supra* note 42, at 350; Lipton, *supra* note 1, at 930 (explaining that peer photographs are generally not covered under present tort structures, especially when the concern is not with the taking of the photograph, but rather its online dissemination).

of Google Maps, and the snap-happy culture of tiny digital and cell phone cameras, there is a greater likelihood that a publicly captured image will find its way to the Internet without the subject's permission.[61] Tort law currently does not include a legal cause of action for the objectionable dissemination of images captured publicly[62] or the broadcast of private information that constitutes newsworthy material.[63]

The issue of what constitutes newsworthy material, and who has the authority to report news, is ever more complicated in the age of online information sharing. The last prong of the public disclosure tort is the "newsworthiness test," which means that if the speech is of legitimate public concern, the case will be dismissed.[64] It is unclear what kind of information amounts to newsworthy material.[65] In fact, "newsworthiness" is often used as an excuse for publicizing controversial images along with shocking stories.[66] In the cyber world there is also an unclear distinction between *who* is authorized as a legitimate news source to show controversial images for the purpose of informing the public,[67] and those who are simply posting inappropriate images and commentary.[68] When newspapers were the primary source of current events news and gossip, information could not be published to the masses unless it fell into the right hands, and those individuals were,

---

61. *See* Kane, *supra* note 42, at 355; Lipton, *supra* note 1, at 927.

62. Kane, *supra* note 42, at 350.

63. *See* Lipton, *supra* note 1, at 932.

64. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 129 (2007) (internal quotation marks omitted).

65. Lipton, *supra* note 1, at 932. Some guidance is provided by "the Restatement of Torts [which] distinguishes between 'information to which the public is entitled' and 'morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.'" SOLOVE, *supra* note 64, at 132 (quoting RESTATEMENT (SECOND) OF TORTS § 652D cmt. h (2000)).

66. *See, e.g.*, Steve Johnson, *Web Spins Hypocrisy on Erin Andrews Video*, CHI. TRIB., July 23, 2009, at 1 (scolding news outlets for attacking the "peephole pervert" while at the same time exploiting Andrews by posting her naked images to accompany their own articles on the story); Pesta, *supra* note 2, at 95 ("News sites claimed they showed [Andrews's nude] video because it was 'news.'").

67. *See* Meghan Peters, *Internet Surpasses Television as Main News Source for Young Adults [Study]*, MASHABLE: SOC. MEDIA (Jan. 4, 2011), http://mashable.com/2011/01/04/internet-surpasses-television-as-main-news-source-for-young-adults-study/ (explaining the increased use of the Internet as a news source by young adults and the specific increase in the use of Facebook's newsfeed and Twitter for news as well, while fewer people in that age group look to television for news); *see also* FAIR, http://www.fair.org/index.php?page=134 (last visited July 27, 2012) (listing various online news sources from alternative and mainstream sources to sources of media criticism).

68. *See, e.g.*, DIRTY, http://www.thedirty.com (last visited July 27, 2012) (exemplifying a website that makes fun of non-famous people); *see also* Tracie Egan Morrissey, *The Man Behind TheDirty.com Is Just As Awful in Person*, JEZEBEL (Nov. 11, 2010, 5:57 PM), http://www.jezebel.com/5687873/the-man-behind-thedirtycom-is-just-as-awful-in-person (describing The Dirty website and how it affects private peoples' lives).

at least in theory, subject to ethical codes of conduct.[69] Today, anyone can take photographs or write a story and then globally disseminate that information with ease.[70] Due to the ease of starting a website, a myriad personal blogs have been created, making it more difficult to differentiate between legitimate news sources and online junk.[71] Tort law must be redefined to include some parameters for what is in fact newsworthy as opposed to strictly private, and which actors should be given the opportunity to use the defense.

There are also concerns that existing tort law does not address the gravity of the emotional and reputational damage of online disclosure.[72] In light of the lack of protections against these harms, the emotional and reputational injuries that result from those exposures are very painful.[73] In fact, those harms are exacerbated by the Internet, which keeps the information continuously available for public viewing.[74]

B. History of the Internet and the Way It Has Transformed Society

The Internet has had an interesting, albeit fairly short history. After the Soviet Union launched Sputnik, scientists began developing a mechanism for sharing research over a network.[75] Five decades later, the Internet has become the nucleus of sharing anything and everything—from photographs and videos to news commentary and personal minute-by-minute updates. The history of the Internet began in the 1960s with J.C.R. Licklider's "idea of a computer 'network of networks,'" a technology he developed with the Defense Advanced Research Projects

---

69. *See* Lipton, *supra* note 1, at 927.

70. *See id.*

71. *See* SOLOVE, *supra* note 64, at 145. Professor Solove explained:

> [A]nybody can spread information online, [so] it becomes harder to know what information to trust and what information not to trust. . . . [E]ntries in the *Encyclopedia Britannica* . . . are written by experts and carefully vetted. Wikipedia entries are a collaborative exercise, and . . . can be written by . . . any fool stumbling along the information superhighway.

Id.; Burrell, *supra* note 57, at 734 (explaining that Internet usage has increased as part of the "[p]henomena [of] blogging and social networking, as well as web services like Google, YouTube, and Wikipedia, [which] have revolutionized the way Internet content is created, organized, collected, and viewed").

72. *See* Citron, *supra* note 58, at 1831-32.

73. *See id.* at 1813-14, 1818 (describing in detail the emotional and reputational damages from traditional privacy torts, as well as modern online privacy torts).

74. *Id.* at 1813.

75. *See* Kane, *supra* note 42, at 333. Sputnik was the first artificial satellite launched into space by the Soviet Union in 1957. *Sputnik and the Dawn of the Space Age*, NAT'L AERONAUTICS & SPACE ADMIN., http://history.nasa.gov/sputnik/ (last updated Oct. 10, 2007). The event triggered the beginning of the U.S.-U.S.S.R. space race and many new scientific and technological developments. *Id.*

Agency ("DARPA") of the U.S. Department of Defense.[76] The network was known as the Advanced Research Projects Agency Network ("ARPANET"), and it was developed for the purpose of sharing information with ease and speed.[77] The first major hurdle for this new "network of networks" was unifying the system, and allowing agencies to communicate with greater ease.[78] In 1973, a solution known as the Transmission Control Protocol/Internet Protocol ("TCP/IP") system was implemented.[79] The TCP/IP system was adopted by multiple national networks, and the integration of these systems was successful.[80] Drawing from this achievement, the government decided to form the Federal Networking Council to facilitate further coordination in pursuit of a global Internet.[81]

In 1992, Congress permitted commercial traffic on the National Science Foundation Network ("NSFNET"),[82] which ultimately led to the development of the World Wide Web.[83] Tim Berners-Lee conceived of the idea of a World Wide Web and created the first Internet browser in 1989; and in 1992, Marc Andreessen and Eric Bina developed another browser called "Mosaic" that would serve as a precursor for more user-friendly browsers.[84] Eventually the Web became a part of popular culture when Netscape Communications developed a browser that could easily be installed on personal computers.[85]

The technical makeup of the Internet allows it to work efficiently for its users, but its regulatory components could be better developed to curb Web-based crimes and privacy violations. The Internet is made up of "an interconnected web of 'host' computers," and as such there is no central repository of information.[86] The system works as a packet-switched network, which means that data transmitted is split up during transmission.[87] These technical elements make the Internet a durable and efficient system, but it also makes regulation difficult.[88] There are,

---

76. STUART MINOR BENJAMIN ET AL., TELECOMMUNICATIONS LAW AND POLICY 905-06 (2d ed. 2006).

77. *Id.* at 906.

78. *See id.* at 907 (internal quotation marks omitted).

79. *Id.*

80. *See id.*

81. *Id.*

82. *See The Launch of NSFNET*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/nsf0050/internet/launch.htm (last visited July 27, 2012).

83. BENJAMIN ET AL., *supra* note 76, at 912.

84. *Id.*

85. *Id.*

86. *Id.* at 908.

87. *Id.* at 908-09.

88. *Id.* at 908, 910.

however, some regulatory devices built into the system.[89] For example, the TCP/IP system defines locations on the Internet using IP numbers (i.e., addresses).[90] Information is transmitted via the numerical locations.[91] As such, IP addresses are a means of detecting where information comes from as well as its destination.[92] Although IP addresses do not necessarily link perpetrators to their Internet crimes, they provide a mechanism that connects online conduct with particular computer sources.[93]

1. How the Internet Has Changed Lives

In addition to shifting public notions of privacy, the Internet has changed our lives by giving every person the ability to broadcast or publish their thoughts and the power to report news through blogs and image capture.[94] The World Wide Web is used for personal shopping, streaming television shows, and networking with friends. Statistics gathered about the use of the Internet show that it is "growing, adapting, and becoming our main source of almost everything we do."[95] Some statistics show that ninety-one percent of people use e-mail, eighty-one percent utilize the medium for research purposes, sixty-eight percent book travel reservations on the Internet, and thirty-two percent read blogs.[96] "In 2010, [sixty-five percent] of people younger than [thirty] cited the Internet as their go-to source for news."[97]

Besides making daily lives easier, the Internet has also created a world for individuals to engage in or further perpetuate certain crimes.[98] In this way, it has affected our sense of privacy[99] and has made the public more vulnerable to theft, widespread exposure to pornography and sexual deviancy, and has also placed children at greater risk of harm

89. *See, e.g.*, *id.* at 908.

90. *Id.* at 910.

91. *Id.* at 910-11.

92. *Id.* at 910.

93. *See* Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 515 (1999) (describing how "there is no necessary link between an [IP] address and a person").

94. *See* BENJAMIN ET AL., *supra* note 76, at 905.

95. Jessekurth, *Quick Online Shopping Statistics*, FIFTH GEAR (July 27, 2010, 3:07 PM), http://www.infifthgear.com/2010/quick-online-shopping-statistics/.

96. *Id.*

97. Peters, *supra* note 67.

98. *See Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 6 (2011) [hereinafter *Internet Crime Hearings*] (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

99. *See* Abril, *supra* note 19, at 11.

from sexual predators.[100] To address these negative effects, Congress has assembled committees to address the various possibilities of monitoring online crime in order to capture criminals more effectively.[101]

2. Regulating the Internet

Congress has been hesitant to regulate the Internet, but has passed laws in limited situations to address very specific Internet crimes.[102] The Digital Millennium Copyright Act ("DMCA")[103] was passed in 1998 to adopt the Word Intellectual Property Organization ("WIPO") Copyright Treaty and the WIPO Performances and Phonograms Treaties, which addressed the emergent global problem of copyright infringement.[104] In addition to copyright, other laws were enacted to protect children from exposure to certain content.[105] The Communications Decency Act of 1996 ("CDA"),[106] prohibited the transmission of obscene or indecent messages or images to any recipient the sender knew to be under 18 years of age.[107] In *Reno v. Am. Civil Liberties Union*,[108] the Supreme Court held that two provisions of the CDA intended to protect children from "indecent" and "patently offensive" material on the Internet were unconstitutional because of the overly broad language of the statute, and because the Court was not ready to allow such regulation of the

100. *See Internet Crime Hearings*, *supra* note 98, at 6 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice); *see also* Susan Donaldson James, *'Misty Series' Haunts Girl Long After Rape*, ABC NEWS (Feb. 8, 2010), http://abcnews.go.com/Health/Internet-porn-misty-series-traumatizes-child-victim-pedophiles/story?id=9773590 (explaining that various technologies have "enabled and facilitated" crimes against children (internal quotation marks omitted)).

101. *See, e.g.*, *Internet Crime Hearings*, *supra* note 98, at 1 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary); *see also id*. at 5 (statement of Rep. Lamar Smith, Chairman, H. Comm. on the Judiciary) (describing the previous introduction of the "Internet Stopping Adults Facilitating the Exploitation of Today's Youth, SAFETY, Act," which require[s] "providers to retain records pertaining to the identity of an IP address user for at least 2 years" and "ensures that the online footprints of predators are not erased").

102. *See* BENJAMIN ET AL., *supra* note 76, at 913-14; *Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/fs/fs18-cyb.htm (last updated Apr. 2012) [hereinafter *Fact Sheet 18*].

103. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

104. *Id.* § 102, 112 Stat. at 2860-61. WIPO is the United Nations agency that aims to develop a framework for an effective intellectual property system. *What is WIPO?*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/about-wipo/en/ (last visited July 27, 2012).

105. *See, e.g.*, Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified in scattered sections of 18 and 47 U.S.C.); Children's Internet Protection Act, Pub. L. 106-554, 114 Stat. 2763A-335 (2000) (codified at 20 U.S.C. § 9134 (2006) and 47 U.S.C. § 254(h) (2006)).

106. Pub. L. No. 104-104, 110 Stat. 133.

107. *Id.* § 502, 110 Stat. at 133.

108. 521 U.S. 844 (1997).

Internet.[109] In response to *Reno*, Congress enacted the Child Online Protection Act ("COPA"),[110] which was similar to CDA in criminalizing certain online speech, but was drawn more narrowly to restrict only transmissions over the Internet, and applies specifically to commercial speakers and "material that is harmful to minors."[111] In *American Civil Liberties Union v. Ashcroft*,[112] the Third Circuit found that "the ACLU would likely succeed on the merits in establishing that COPA is unconstitutional."[113] The Supreme Court affirmed, declaring that COPA failed to meet the least restrictive means test.[114] Congress enacted other laws after COPA in order to protect minors but those enactments were extremely limited in scope.[115] Most recently, Congress has proposed two new pieces of legislation concerning the regulation of content on the Internet, which specifically address intellectual property infringement.[116] Both the Stop Online Privacy Act ("SOPA")[117] and the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act" or "PIPA")[118] provide methods of fighting online piracy and are aimed at foreign websites that provide copyright infringing material.[119] However, these bills have received a

109. *See id.* at 849, 867, 877 (distinguishing the readiness to regulate radio and broadcast due to the lengthy regulatory history of those mediums, as compared to the lack of regulatory history of the Internet).

110. Pub. L. No. 105-277, 112 Stat. 2681-736 (1998) (codified at 47 U.S.C. § 231 (2006)).

111. *Id.* § 1403, 112 Stat. at 2681-736; BENJAMIN ET AL., *supra* note 76, at 934.

112. 322 F.3d 240 (3d Cir. 2003).

113. *Id.* at 271. The Third Circuit agreed with the District Court that alternatives such as filtering and blocking mechanisms were a less restrictive means of accomplishing the same protection. *Id.* at 265. They also concluded that the statute was overbroad, and placed "significant burdens on Web publishers" with regard to protected speech. *Id.* at 266.

114. Ashcroft v. ACLU, 542 U.S. 656, 668-69, 673 (2004) (discussing the holding and the alternative means evaluated by a government commission). When dealing with a regulation that restricts speech, the Court:

> assumes that certain protected speech may be regulated, and then asks what is the least restrictive alternative that can be used to achieve that goal. . . . The purpose of the test is to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to ensure that legitimate speech is not chilled or punished.

Id. at 665-66.

115. *See id.* at 663. These other laws only addressed the issues of misleading pornographic Internet domain names and the potentiality of a second level Internet domain with content just for children. *Id.*

116. *See* Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011); PROTECT IP Act of 2011, S. 968, 112th Cong. (2011); *see also* August Brown, *SOPA and PIPA: What's Still at Stake for Music?*, POP & HISS: THE L.A. TIMES MUSIC BLOG (Jan. 18, 2012, 4:43 PM), http://latimesblogs.latimes.com/music_blog/2012/01/what-should-online-music-still-expect-from-sopa-and-pipa.html.

117. H.R. 3261.

118. S. 968.

119. H.R. 3261; S. 968; Jared Newman, *SOPA and PIPA: Just the Facts*, PCWORLD (Jan. 17, 2012, 6:00 PM), http://www.pcworld.com/article/248298/sopa_and_pipa_just_the_facts.html.

significant amount of negative attention, and have been delayed for further legislative discussion.[120]

C. Modern Notions of Privacy

American conceptions of privacy have changed as a result of the Internet, and many academics have attempted to explore this shift in privacy standards.[121] Scholarly articles have touched on concerns that range from government access to personal information[122] to expectations of privacy in the public sphere.[123] Some of the more popular issues concern the new social media phenomenon, otherwise known as online social-networking technologies ("OSN"), and the effect those sites will have on this generation and the next, both generally and specifically as it relates to privacy expectations.[124]

Privacy tort law also faces the challenge of adapting to our modern notions of privacy.[125] Perhaps the reason why one definition of privacy has never emerged is because the public's conception of privacy has changed over time.[126] In 1997, a Stanford study conducted by students showed that a majority of Internet users felt "that legislation should be enacted to protect personal privacy."[127] An online identity theft agency conducted another survey of 5000 adult Internet users, and estimated that about 57 million adults "have experienced a phishing attack," and

---

120. Newman, *supra* note 119. Some powerful Internet sites have made their dissatisfaction over SOPA and PIPA known through their websites and collectively blacked out their sites on January 18, 2012 as a way to make the public aware of their fight. Brown, *supra* note 116.

121. *See* Lipton, *supra* note 1, at 948 (providing commentators' perspectives on how to deal with this issue and stating how "[w]idespread unregulated online-privacy incursions can create a general culture of unease where individuals cannot rely on anyone to respect personal boundaries").

122. *See, e.g.*, Solove, *supra* note 33, at 746-48 (discussing privacy rights as they relate to government searches and intrusions).

123. *See, e.g.*, Calvert & Brown, *supra* note 2, at 479-80 (discussing intrusive voyeurism in public places like malls and amusement parks); Kane, *supra* note 42, at 355 (discussing the Google street view public privacy issue); *see also* Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 354 (2011) (discussing the recent phenomenon of "upskirt photography" in public places).

124. *See generally* Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH L. 1001 (2009) (explaining how OSNs present distinct risks, such as reputational risks and identity theft, for the younger generation which uses the Internet for socialization purposes, and how such sites have changed the very nature of interpersonal relationships and social interactions).

125. *See* Abril, *supra* note 19, at 17.

126. *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRACTICE 56, 57-60 (1999) (explaining the evolution of society and how it has affected individual and communal perceptions of privacy).

127. Jonathan Louie et al., *Databases in Cyberspace: Maintaining Individual Privacy Rights: Privacy Statistics*, STAN. U., http://www-cs-faculty.stanford.edu/~eroberts/cs181/projects/databases-in-cyberspace/statistics.html (last visited July 27, 2012).

1.78 million "could have fallen victim to [those] scams."[128] Phishing is an online lure that often comes in the form of spam e-mail or pop-up screens that look trustworthy, but are actually harmful and likely to lead to fraud.[129] It is unclear whether people understand the gravity of privacy concerns arising from the Internet, especially in its Web 2.0 phase, but "[n]early all indications of the severity of the security threat to computer systems . . . indicate a continuously worsening problem."[130]

A little over a decade ago, in anticipation of the changes the Internet would bring, Professor Lawrence Lessig predicted that "the extent of the monitored, and the reach of [the] searchable" would be "fundamentally altered."[131] In his article, Professor Lessig takes the reader back to early America where social life was never private, because of the nature of small communities and busy-bodies.[132] He explains that the balance to this open lifestyle was the self-regulating nature of society, which kept people in check, and the non-permanence of memory, which allowed people to move on more easily.[133] The Internet no longer makes that kind of reality possible, because information is saved and reproduced, and thus not forgotten.[134] In terms of the searchable, Professor Lessig draws on the simplicity of early American life, and the protections afforded by the architecture of property, specifically the physical boundaries that provide a sense of private versus public space—a concept also no longer possible in today's technologically monitored world.[135]

---

128. *Internet ID Theft Statistics Show How Online Identity Theft Works*, GUARD PRIVACY & ONLINE SECURITY, http://www.guard-privacy-and-online-security.com/internet-id-theft-statistics.html (last visited July 27, 2012).

129. *See id.* Phishing e-mail messages and websites are used to steal money. *How to Recognize Phishing Email Messages, Links, or Phone Calls*, MICROSOFT SAFETY & SECURITY CENTER, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx (last visited July 27, 2012). Cybercriminals can install malicious software on a computer, or use "social engineering" to convince Internet users to install malicious software which is then used by the thieves to access and steal personal information from those computers. *Id.* Cybercriminals also find ways to convince Internet users to "hand over [their] personal information under false pretenses." *Id.*

130. STEERING COMM. ON THE USABILITY, SEC., & PRIVACY OF COMPUTER SYS., NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TOWARD BETTER USABILITY, SECURITY, AND PRIVACY OF INFORMATION TECHNOLOGY 2 (2010), *available at* http://books.nap.edu/catalog.php?record_id=12998.

131. Lessig, *supra* note 126, at 56-57.

132. *See id.*

133. *See id.*

134. *See* Citron, *supra* note 58, at 1813 ("While public disclosures of the past were more easily forgotten, memory decay has largely disappeared. Because search engines reproduce information cached online, people cannot depend upon time's passage to alleviate reputational and emotional damage. . . . The Internet thus ensures that damaging personal information is not forgotten . . . .").

135. *See* Lessig, *supra* note 126, at 58. Traditionally privacy was defined by spatial experiences and seclusion in one's dwelling space, and in many ways that concept shaped our ideas of personal

One of the most daunting problems the Internet presents in terms of privacy is purely structural: it is the breakdown in boundaries between public and private space.[136] On the Internet, it is unclear where a user has a reasonable expectation of privacy, and what level of privacy is afforded to them.[137] Physical boundaries generally allow people to better conceptualize what is public and private.[138] For instance, in the real (i.e. not cyber) world, people know that the things they do and keep within the four walls of their home will be protected from the public or government eye, but when they step outside to their front yard their privacy expectations change, and they are aware that others may be observing them.[139] The Internet does not provide a clear mechanism to distinguish private from public space.[140] Personal, secure banking pages are presumed private, while blogs and most other websites are presumed public, but Facebook and other social media websites have settings that are somewhere in-between.[141] As the Internet progresses, varieties of Web pages are born, making it increasingly difficult to manage privacy expectations.[142] This ambiguity causes tension with the traditional line that courts have drawn distinguishing the acquisition of information from a public place versus a place where an individual has a reasonable expectation of privacy.[143]

---

identity. *See* Abril, *supra* note 19, at 11-12.

136. *See* Abril, *supra* note 19, at 12.

137. *See id.*

138. *See* Lessig, *supra* note 126, at 58-59 (describing the privacy protections afforded to one's private home, as compared to public places).

139. *See id.* at 56-58 (describing the natural societal monitoring that an individual expects to face when walking down a public street, in contrast to privacy in one's home).

140. *See* Abril, *supra* note 19, at 12; *see also* Lessig, *supra* note 93, at 505 (explaining how in cyberspace you do not notice "monitoring because such tracking in cyberspace is not similarly visible" as it would be in traditional real space).

141. *Compare* Lipton, *supra* note 1, at 931-32 & n.67 (discussing the level of privacy expected on sites like Facebook or MySpace, as opposed to YouTube or Flickr, and what defines a "closed network" on the Internet), *with* Abril, *supra* note 19, at 18 ("[A]ctivity that is visible to the public eye—whether that eye is human or mechanical—is not actionable under the public disclosure tort."). *See also Fact Sheet 18*, *supra* note 102.

142. *See* Abril, *supra* note 19, at 11 (explaining that "privacy expectations and norms are constantly challenged by technology" and the evolution of the Internet is the latest "threat[] to privacy").

143. *See id.* at 18-20. The Supreme Court first adjusted the framework of privacy violations in 1967 by expanding the protections of the right to privacy to any location where a person maintained a reasonable expectation of privacy in their activities. Marc Jonathan Blitz, Stanley *in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 HASTINGS L.J. 357, 363 (2010) (citing Katz v. United States, 389 U.S. 347, 351-52, 361 (1967)).

III. REGULATORY AND REMEDIAL DEFICIENCIES PLAGUE WEB-RELATED PRIVACY INFRINGEMENT

Innocent victims of crime and privacy infringements are often left with deeper wounds and fewer remedies simply because the offense against them took place on the Internet. The way that our society allows cyberspace to function, with little to no regulation or legal remedial framework, is inconsistent with the way American life works in real space. Unlike cyberspace, in real space criminals and tortfeasors that leave evidence of their indiscretions take the risk of being noticed and brought to justice.[144] Furthermore, in real space, victims have a better opportunity of finding those who have harmed them, either to seek justice or limit the exposure of their private footage or information.[145] The Internet complicates all of these basic crime-fighting and remedial structures. The issue is twofold: criminals and tortfeasors get away with more, and victims who are unable to connect an individual to the offense are left without a remedy—as is the case with attempts to remove the Internet postings of unauthorized nude footage or of other embarrassing private information.[146]

A. Increase in Crime and Privacy Violations

Since the inception of Internet use by the masses, very few laws have been passed to address specific concerns that have emerged from online culture.[147] Some believe that this is because remedies exist for Internet crime through regular legal structures;[148] others believe it is because the Internet is impossible to monitor.[149] One thing is undeniable: the Internet has become a tool for perpetrating both age-old crimes as well as new digital crimes.[150] The secret capture of lewd video footage, otherwise known as video voyeurism, is one type of criminal privacy infringement that has become difficult to control because of an unregulated Internet.[151]

---

144. *See infra* text accompany notes 152-53 (discussing the anonymity shield of the Internet).

145. *See* discussion *infra* accompanying notes 184-92 (concerning the difficulties in tracking and prosecuting online criminals).

146. *See infra* Part III.A–C.

147. *See* BENJAMIN ET AL., *supra* note 76, at 903 (describing how there are few regulations that govern the Internet itself).

148. *See, e.g.*, *id.* at 913.

149. *See, e.g.*, Lessig, *supra* note 93, at 505.

150. *See* Nick Nykodym, Sonny Ariss & Katarina Kurtz, *Computer Addiction and Cyber Crime*, J. LEADERSHIP, ACCOUNTABILITY & ETHICS, http://www.na-businesspress.com/JLAE/nykodym.pdf (last visited July 27, 2012).

151. *See* Calvert & Brown, *supra* note 2, at 476, 523 (defining video voyeurism in the context of the Internet and describing pornography on the Internet as "largely unregulated").

1. Crime on the Internet

Criminals take advantage of the Internet because it is a global system that is fast and unregulated.[152] It also "affords them a kind of anonymity."[153] All types of criminals from hackers to sexual predators and murderers use the Internet as a tool for perpetrating crime.[154] The Internet can expand a criminal's victim pool beyond his or her own geographic area, and can be used as a resource to investigate those victims.[155] A whole new kind of criminal activity specific to the Web has also emerged.[156] The Federal Bureau of Investigation ("FBI") fights "high-tech crimes" such as "cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds."[157] The complex nature of these crimes plus the fact that they utilize the Internet cause prolonged investigations, which often affect the success of obtaining criminal evidence.[158]

2. Privacy and Video Voyeurism

Video voyeurism, the secret videotaping of others, is one of several crimes that has become increasingly difficult to control as a result of the Internet. Although not all voyeurism is illegal, many states have criminalized sexually-based and particularly invasive voyeurism.[159] The Internet has created an underground market for voyeuristic images, leaving lawmakers concerned that more people will seek to make money by providing illegal voyeuristic videos to websites.[160] Video voyeurism has been described as "one particularly pernicious and proliferating variety of Web-based pornography . . . [that] raises serious questions about invasion of privacy and leaves in its wake real adult victims."[161]

---

152. *See Internet Crime Hearings*, *supra* note 98, at 6 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

153. *Id.*

154. Nykodym, Ariss & Kurtz, *supra* note 150.

155. *Id.*

156. *See* FED. BUREAU OF INVESTIGATION, CYBER CRIME, http://www.fbi.gov/about-us/investigate/cyber/cyber/ (last visited July 27, 2012) (describing the Federal Bureau of Investigation ("FBI")'s preparedness to fight Internet-based offenses).

157. *See id.* The FBI's current priorities are: combating widespread and malicious cyber viruses and worms; stopping sexual predators; and addressing intellectual property theft that impacts consumer health and safety. *Id.*

158. *See Internet Crime Hearings*, *supra* note 98, at 2 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary).

159. *See, e.g.*, CONN. GEN. STAT. ANN. § 53a–189a (West 2007) (making voyeurism a felony); LA. REV. STAT. ANN. § 14:283 (2004) (making video voyeurism a sexual offense).

160. *See* Calvert & Brown, *supra* note 2, at 511, 517.

161. *Id.* at 470.

Victims of Web-based video voyeurism are "twice bitten."[162] The initial violation occurs when the voyeur captures the image or video by invading the subject's physical space and his or her "right to be let alone."[163] The second is the subsequent posting of that image or video on the Web, taking away the subject's right "to control the flow of information about themselves."[164] Unfortunately, there continues to be no remedy for controlling those images once they make it to the Internet.[165]

Voyeuristic privacy infringements are particularly bothersome because the private information is disseminated via images.[166] Video images are different from text-based data, and should be treated differently when involving privacy infringement.[167] Instant photo sharing has become a part of our daily lives and a part of our social ecology and discourse.[168] But since its advent, portable camera image capture has also presented unique privacy concerns.[169] Data in video formats is generally more accessible and presents additional problems in terms of the ease of public access, lack of contextual information, increased threat of viral dissemination, added challenges in detecting accuracy, and most notably, the image subject's inability to control who has access to the image once it reaches cyberspace.[170] Online technologies and mobile camera devices create even greater threats to privacy.[171] In a recent article about online privacy, Professor Jacqueline D. Lipton explains: "The fact that individuals can instantly snap a photograph without even thinking to carry a camera, and can then disseminate that image instantaneously and globally at the push of a button, raises significant problems of decontextualization."[172]

---

162. *Id.* at 488.

163. *See id.* (internal quotation marks omitted).

164. *See id.*

165. *See* Lipton, *supra* note 1, at 928-29.

166. *See id.* at 927 (describing how video-based accounts provide more detail, but lack context).

167. *See* Lipton, *supra* note 1, at 926 & n.43 (providing various examples where courts considered the difference between video and text information in the privacy context).

168. *See* Kreimer, *supra* note 123, at 341.

169. *See id.* at 351.

170. Lipton, *supra* note 1, at 928-29.

171. *Id.* at 927.

172. *Id.* Professor Lipton describes "decontextualization" in terms of:

> [c]omparing a video-based account of an event to a text-based account[,] reveal[ing] that the textual account likely provides more relevant and accurate context. The video-based account may capture more information in terms of small background details, but those details will not necessarily provide the more accurate context conveyed by textual accounts. Some courts have begun to recognize the distinction between information in text and video formats in terms of concerns about contextualization.

B. Lack of Regulation

The Internet, as it exists today, does not have an adequate structure for regulating online criminal behavior. The only significant Internet regulation directly implemented is the IP address system, which allows Internet Service Providers ("ISPs") to see where information is being sent and where it is received.[173] However, the IP address technology is not equipped to link an address to a specific individual.[174] While some machines are static and have a permanent address, others are reassigned an address each time a connection with the Internet is established.[175] Furthermore, "software has been developed and commercialized to allow users to . . . continuously change[] their IP addresses," which presents additional problems for a consistent tracking system.[176]

A tracking feature may be most valuable for monitoring online conduct, because the Internet often draws out the worst in people—allowing them to misbehave behind a screen of anonymity.[177] Although authors have a First Amendment right to free anonymous speech,[178] anonymity also tempts people to behave badly as they are less accountable for their conduct.[179] Professor Lessig explores how communal monitoring and the high likelihood that bad behavior in public would be noticed and exposed compelled early Americans to abide by social norms.[180] The Internet is an anomaly within the idea of self-regulation and accountability, because there is no effective regulatory structure, even for public postings.[181]

Online criminals, including criminals who post evidence of their real world crimes online, are difficult to prosecute because of the

---

Id.

173. *See* BENJAMIN ET AL., *supra* note 76, at 910, 913.

174. Lessig, *supra* note 93, at 515.

175. *Id.*

176. Ben Quarmby, *Protection from Online Libel: A Discussion and Comparison of the Legal and Extrajudicial Recourses Available to Individual and Corporate Plaintiffs*, 42 NEW ENG. L. REV. 275, 291 (2008).

177. *See Internet Crime Hearings*, *supra* note 98, at 2 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary); *id.* at 4 (statement of Rep. Lamar Smith, Chairman, H. Comm. on the Judiciary); *id.* at 6 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) (raising the issue of the Internet's cloak of anonymity); SOLOVE, *supra* note 64, at 140 (explaining the dark side to anonymity).

178. Burrell, *supra* note 57, at 726.

179. SOLOVE, *supra* note 64, at 140.

180. Lessig, *supra* note 126, at 57.

181. *See* Lessig, *supra* note 93, at 519-20 (describing how a different Internet architecture could bring about a self-regulated system); *see also id.* at 515-16 (explaining the inadequacy of the current IP address system as a regulating mechanism and making alternative suggestions).

Internet's anonymity.[182] In order for law enforcement or a victim, like Erin Andrews, to proceed with a case or suit, the identity of the online criminal or third party poster must be known.[183] A victim must file an ex parte motion seeking a subpoena, along with an order to show cause providing a reason for identifying the defendant in order to compel the ISP, website operator, or online service provider ("OSP") to disclose the anonymous poster.[184] The government goes through a similar process by seeking a subpoena, court order, or search warrant to obtain data.[185] Some Internet companies, though, forward leads directly to the government.[186] However, both in private and government investigations, searches are often frustrated due to the failure of ISPs to retain information.[187] The greatest drawback of relying on ISPs for identification information is the lack of insurance that sufficient data will be held long enough to assist law enforcement or victims.[188] The Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009 ("Internet SAFETY Act")[189] was introduced to address this electronic retention problem, specifically proposing that ISPs be required to retain identification data for at least two years.[190] This kind of solution, although a good step, does not resolve other issues, such as delays in detecting Internet crime[191] and the imprecise nature of connecting an individual to a specific IP address.[192]

---

182. *See Internet Crime Hearings*, *supra* note 98, at 2 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary) (introducing the subcommittee to the issue by saying that "[t]hese criminals have the luxury of cloaking themselves in the anonymity that the Internet provides, making their apprehension significantly more difficult").

183. *See* Burrell, *supra* note 57, at 727.

184. *Id.*

185. *Internet Crime Hearings*, *supra* note 98, at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

186. *Id.* at 3 (statement of Rep. Bobby Scott, Ranking Member, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary) (explaining how some companies proactively retain and forward information to law enforcement).

187. *Id.* at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) (stating that "critical data has too often been deleted by providers" before law enforcement can obtain access to it).

188. *See Internet Crime Hearings*, *supra* note 98, at 7-8 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

189. H.R. 837, 110th Cong. (2007).

190. *Internet Crime Hearings*, *supra* note 98, at 5 (statement of Rep. Lamar Smith, Chairman, H. Comm. on the Judiciary). Rep. Lamar Smith introduced the Internet SAFETY Act. *Id.*

191. *See id.* at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) ("The problem is exacerbated by the complexity of investigating crimes committed using online means. These crimes are difficult to detect, and they may not be discovered or reported to law enforcement until months and months have gone by.").

192. *See* Lessig, *supra* note 93, at 515 ("Th[e] IP address is unique; only one machine at any one time may have a particular address. . . . But while [the] addresses are unique, there is no

C. Lack of Takedown Measures

Individuals remain completely without control over their personal information when the Internet fails to provide a takedown structure for unlawfully obtained or posted material.[193] The Internet, even in its early phases, presented unique problems of controlling one's personal information.[194] In the present phase of Web 2.0, anyone can publish images or information.[195] Many OSNs, such as Yahoo, Facebook, and YouTube, have terms of use intended to protect online privacy, but Internet users still have virtually no power to legally demand the takedown of an unauthorized image from these sites.[196] When an Internet user's rights have been violated, they can complain to the service provider or website operator, but ultimately it is up to the provider or operator to decide whether to take the image down or to punish the subscriber for his unlawful or unauthorized posting.[197] Generally the complaining party lacks standing to sue under contract law, because they are not a party to the service provider's terms of use.[198] Furthermore, the victim is unable to sue the service provider directly because Section 230 of the Communications Decency Act appears to protect service providers from secondary liability for their subscribers' postings.[199] Existing laws provide virtually no control to Internet users over their own information.[200] Current communication technologies have broken down privacy barriers more than ever before—and perhaps altogether.[201]

IV. REGULATION AND TAKEDOWN LEGISLATION IS THE SOLUTION

A regulatory mechanism is necessary to enforce existing laws on the Internet, and takedown legislation is necessary to preserve privacy rights and remedy current deficiencies in the law. Internet use has changed vastly over the last few decades, and, in turn, the nature of control given to ISPs and OSPs and the legal rules enforced against

---

necessary link between an address and a person.").

193. *See* Burrell, *supra* note 57, at 739-40.

194. *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 486 (2010) (describing "the unprecedented ability of governments and corporations" to gather personal information about individuals in the early days of the Web).

195. *See* Lipton, *supra* note 1, at 927.

196. *See id.* at 936-39; *see also* 47 U.S.C. § 230(c)(1) (2006) ("No 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.").

197. Lipton, *supra* note 1, at 939.

198. *Id.*

199. *Id.* (citing 47 U.S.C. § 230(c)(1)).

200. *See* Lipton, *supra* note 194, at 487.

201. *See id.*

unlawful online users must change as well.[202] Regulatory measures will facilitate tracking down and prosecuting perpetrators, and takedown legislation will ensure that some semblance of individual privacy is preserved.

A. Creating a Better Regulatory Structure

Although regulation raises concerns,[203] the cyber-world has reached a point where some level of monitoring is necessary to stop crime and protect individual rights. Regulation is the key to tracking down Internet criminals and tortfeasors.[204] Policing unlawful or suspicious behavior in public places is what most people expect of government protective forces, and allowing Internet administrators to monitor public discourse and postings online is no different.[205] Linking unlawful content to a particular individual does not constitute a Fourth Amendment search, because open Web pages are analogous to public spaces, and those who choose to visit or post content on such pages should be traceable by ISPs.[206]

Some technology is already in place to track Internet posters, including anonymous users.[207] As mentioned earlier, IP addresses enable ISPs and OSPs to track the flow of information, and ISPs routinely use this technology along with the software component called a "cookie" to keep records of those addresses.[208] When requested, information about a particular IP address user may sometimes be available from ISPs or OSPs through the use of a subpoena.[209] However, this system has proven

202. *See* Burrell, *supra* note 57, at 732-33.

203. *See, e.g.*, *id.* at 749 (stating that the major objection to "traceable anonymity" is that it hinders free speech); Newman, *supra* note 119 (exemplifying the kind of negative response created by new legislation concerning Internet regulation).

204. *See, e.g.*, *Internet Crime Hearings*, *supra* note 98, at 8 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) (describing the importance of a retention requirement so that law enforcement can effectively prosecute crimes over the Internet).

205. *See* Terry v. Ohio, 392 U.S. 1, 23-24 (1968); *see also Internet Crime Hearings*, *supra* note 98, at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) (discussing already existent measures for monitoring the Internet).

206. *See* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (discussing privacy expectations on the Internet, and suggesting that there is a shift in privacy expectations in the digital age); *see also id.* at 957 (Sotomayor, J., concurring) (reflecting on Justice Alito's feelings about the diminution of privacy in the digital age).

207. Burrell, *supra* note 57, at 748.

208. *Id.* (noting that cookie software tracks user identity by communications from the website's server to the user's Internet browser and back again).

209. *See id.* at 727, 748-49; *Internet Crime Hearings*, *supra* note 98, at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

to be inadequate to fight Internet crime and privacy torts in the Web 2.0 world.[210]

A better technology, such as a universal Internet log-on system or some form of identification-based monitoring system, would allow ISPs to directly connect an individual to their activity online.[211] When online criminal activity is detected, the service provider would be able to directly connect an individual to that conduct.[212] User identities would remain private to the public—allowing some anonymity—but ISPs would be able to connect a comment, image, or video to the specific individual who posted it.[213] Thus, when unlawful conduct or postings are detected, this system will increase the speed and accuracy of catching the cyber-criminal.[214] Additionally, this log-on system would provide a framework to limit the flow of certain information to underage users.[215] Protecting minors from inappropriate material on the Internet has been an ongoing battle,[216] which this system may help resolve.[217]

The most important feature of a log-on-type monitoring system is that it puts Internet users on notice, enabling individuals to choose what information they offer about themselves.[218] If the public is candidly made aware that their online conduct is being monitored, a decrease in cybercrime and torts would naturally result from individual self-regulation.[219] Professor Lessig stated that "if . . . technologies of identification were in general use on the Internet, then the *regulability* of behavior in cyberspace would increase."[220]

---

210. *See* Burrell, *supra* note 57, at 749 ("Most information gathered using cookies and IP addresses is anonymous because these do not convey any personal information in their own right.").

211. *See* Lessig, *supra* note 93, at 515-18 (suggesting several types of identification systems that would regulate conduct on the Internet).

212. *See id.* at 516 (suggesting that an identity-based Internet system would allow websites to identify the individual visiting their page).

213. *See, e.g.*, Burrell, *supra* note 57, at 748-49 (providing an explanation for how the current system tracks anonymous online posters).

214. *Cf. Internet Crime Hearings*, *supra* note 98, at 7 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice) (expressing the difficulties of Internet crime detection and investigation, specifically as it relates to collecting evidence).

215. *See, e.g.*, Lessig, *supra* note 93, at 517-19 (describing a hypothetical statute where Internet browsers would block data collection and certain websites when the browser identifies the user as a minor).

216. *See* discussion *supra* Part II.B.2.

217. *See* Lessig, *supra* note 93, at 518-19.

218. *See id.* at 519.

219. *See id.* at 519-20 ("Architectures can enable or disable individual choice by providing (or failing to provide) individuals both with the information they need to make a decision and with the option of executing that decision. . . . Self-regulation, like state-regulation, depends upon architectures of control. Without those architectures, neither form of regulation is possible.").

220. Lessig, *supra* note 93, at 516.

Capturing an electronic footprint on the Internet is no more an infringement on individual privacy than the regular monitoring and data retention that takes place in real space.[221] In the digital age, using the Internet inevitably means giving up some privacy on a daily basis, even when performing everyday mundane tasks.[222] In today's digital world, a person's whereabouts can be monitored based on which cell phone tower is generating their signal, where their credit card is swiped, or which toll collection booth swipes their vehicle's automatic pay pass.[223] It is time that the legal world catches up to the technological world by defining privacy expectations in new digital spaces.[224] Hopefully, by doing so, a clear means of regulating cybercrime and online torts will emerge.[225]

This proposed tracking system will naturally be limited in scope. The idea is to utilize the direct identification feature specifically for suspicious, criminal, or directly identified tortious activity.[226] This means that the latent monitoring system would work continuously, but that the direct identification of any user would only be executed when illegal or suspicious material is identified.[227] Though some networking sites utilize a signature-type mechanism to create accountability,[228] this

---

221. *Cf.* Terry v. Ohio, 392 U.S. 1, 22 (1968). The Court stated:

> One general [governmental] interest is of course that of effective crime prevention and detection; it is this interest which underlies the recognition that a police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes of investigating possibly criminal behavior even though there is no probable cause to make an arrest.

Id.

222. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (discussing the different ways people give up personal information to third parties in the digital age, such as their cell phone numbers to their service providers and the medications they purchase to online retailers).

223. *See id.* at 963 (Alito, J., concurring); Lessig, *supra* note 126, at 60.

224. *See* Lipton, *supra* note 194, at 488.

225. *See* Lipton, *supra* note 1, at 966 (describing "the difficulty of ascertaining appropriate levels of privacy protection in the absence of clearer information about social expectations").

226. *See Internet Crime Hearings*, *supra* note 98, at 5 (statement of Rep. Lamar Smith, Chairman, H. Comm. on the Judiciary) (stating how "[m]ore robust data retention will . . . assist law enforcement investigators on a wide array of criminal activity"); *id.* at 64 (statement of Rep. Debbie Wasserman Schultz) (stating that it "is not about watching or tracking people's behavior online . . . [i]t is about helping law enforcement connect the dots").

227. It is important to distinguish the proposal in this Note from the suggestion made by law enforcement in the Committee meeting—specifically that this proposal does not include tracking content within e-mails and private messages, but only content posted on websites open for searching on the World Wide Web. *See Internet Crime Hearings*, *supra* note 98, at 34-35 (statement of John B. Morris, Jr., General Counsel, Center for Democracy and Technology) (expressing unease with a broad scope tracking system that covers all varieties of online communication).

228. Facebook is an example of one of these networks. *See* Sarah Perez, *The 3 Facebook Settings Every User Should Check Now*, N.Y. TIMES (Jan. 20, 2010), http://www.nytimes.com/external/readwriteweb/2010/01/20/20readwriteweb-the-3-facebook-settings-every-user-should-c-29287.html?em.

regulation would not necessarily require a public signature.[229] Instead, it would simply enable a private footprint to track down individuals who actively and repeatedly abuse the Internet's anonymity, and if necessary identify those individuals for further prosecutorial measures.

B. Imposing Takedown Measures on ISPs

The second part of this proposal calls for Congress to develop a law that requires Internet providers or search engines to remove intrusive and completely unlawful videos or images. Aside from tort inadequacies, the greatest privacy-related limitation on the Internet is the lack of a takedown remedy for infringing postings.[230] Victims of online privacy infringements are generally most concerned about the removal of their images from the Web, and would be more satisfied with a structure that provides that kind of remedial measure.[231] Requiring ISPs to remove infringing material upon notice is neither a great imposition,[232] nor a limitation to the originally intended protections afforded to service providers under Section 230 of the CDA.[233] In fact, it is perhaps the most uncomplicated means of protecting individual privacy, without overhauling the present legal framework governing the Internet.[234]

---

229. *Cf.* Burrell, *supra* note 57, at 748 (explaining that a system already exists for the purpose of monitoring anonymous Internet activity without the need for public signatures).

230. *See* Citron, *supra* note 58, at 1814 (explaining how "the searchable, permanent nature of the Internet ensures that [victims] must grapple with the pain [of their exposure for] years after it occurred"); *see, e.g.*, Pesta, *supra* note 2, at 94 (describing Andrews's struggle to remove an unlawful video from the Internet).

231. *See* Burrell, *supra* note 57, at 746 ("[E]nforceable means of identity protection that require OSPs to take down identity-misappropriating posts would be more effective to remedy online infringement than the current suit-for-damages system."). Interestingly, "most plaintiffs would prefer to simply have the offending posts removed than to get money damages." *Id.* Two examples include Caroline Wimmer's parents, who sought to have unauthorized images of their daughter's corpse removed from Facebook, but did not seek financial restitution. *See* Andrew Beato, *Facebook Sued for Keeping Dead Body Photos*, INTENTIOUS (Mar. 30, 2011), http://intentious.com/2011/03/30/facebook-sued-for-keeping-dead-body-photos. Similarly, Cecilia Barnes worked for months to have a fake sexually explicit profile of herself removed from Yahoo's site, before she finally resorted to filing a lawsuit against the company for breach of promise. Hunter Walker, *Court Rules Yahoo! Can Be Sued for Fake Profile*, SOC. TIMES (May 11, 2009, 3:32 PM), http://socialtimes.com/court-rules-yahoo-can-be-sued-for-fake-profile_b49777.

232. *See* Lipton, *supra* note 1, at 955-56 (describing the similarities between copyright and privacy and how there is an already existing copyright takedown model).

233. *See* Burrell, *supra* note 57, at 722-23 (providing a background on the original purpose of § 230 of the CDA and explaining that publisher liability immunity was not explicitly provided to ISPs).

234. *See* Lipton, *supra* note 1, at 944-45, 961-62 (explaining other more extensive means of protecting privacy on the Internet; specifically, giving individuals property rights to their personal information, or utilizing express and implied contracts of confidentiality, or extended breach of confidence actions).

The takedown structure for copyright infringing material is a perfect example of a removal process that balances the rights of all Internet users.[235] Some scholars suggest that there are incredible similarities between copyright and privacy with respect to video files.[236] Some of the issues that Professor Lipton highlights include the effectiveness of controlling access and use of digitally available information, balancing the rights of the rights-holder and the interests of free speech, determining whether ISPs should face liability for the unauthorized activity of others, identifying wrongdoers in a mostly anonymous online culture, and providing effective remedies for harms caused by the dissemination of protected information.[237] Despite these similarities, the protective regimes available in copyright law remain unavailable for privacy violations and other crimes that make their way to the Internet.[238]

The Online Copyright Infringement Liability Limitation Act ("OCILLA"),[239] which is Title II of the DMCA, can work as a model for a privacy-based takedown provision. OCILLA requires that a service provider remove material from its server upon notice that it is hosting copyrighted material.[240] Service providers are protected from liability so long as the they do not have knowledge of the infringing material on their site, or "upon obtaining such knowledge or awareness, act[] expeditiously to remove, or disable access to, the material."[241] The DMCA lists specific instructions for copyright holders on how to give service providers notice of infringing material on the Internet.[242]

A limited liability notice and takedown law can be effective in removing privacy infringing material as well. Internet users who identify a privacy infringing image or representation of themselves on the Internet should be able to notify the appropriate service provider of the content and have the infringing material removed upon further

---

235. Lipton, *supra* note 1, at 955.

236. *See, e.g.*, *id.* at 955-56.

237. *Id.*

238. *See id.* at 929-30; Pesta, *supra* note 2, at 94 (explaining that Andrews's lawyers had to resort to obtaining a copyright to her video in order to send out cease-and-desist letters to websites to take down the video).

239. 17 U.S.C. § 512(c)(1) (2006).

240. *Id.*

241. *Id.*

242. *Id.* § 512(c)(3)(A). Notice by the Internet user includes: a signature of the owner of the exclusive right allegedly infringed, identification of the work or material claimed to be infringed, contact information of the complaining party, a statement from the complaining party indicating a good faith belief that use of the material is not authorized by the owner, and a statement under penalty of perjury that the notice is accurate and that the individual submitting it is authorized to act on behalf of the exclusive right owner. *Id.*

investigation.[243] Similar to the DMCA's instructions, the user would be required to file a notice claim identifying the image or video and providing their contact information.[244] In addition, they would need to provide a statement under penalty of perjury that self-identifies them as the individual depicted, explaining their good faith belief for why the image was unauthorized, or how it infringes on their privacy expectation, and acknowledging that they are the only legitimate holder to the rights of the image under established privacy law.[245] This information will be adequate to open an investigation and temporarily remove the identified materials.[246] The service provider would then notify the third party Internet user who posted the infringing material, requesting a response within two weeks admitting or denying the claim.[247] If the third party responds by denying the claim, he or she will have to provide an explanation, showing evidence of their authority to post the private image or video.[248] If, however, there is no response or the third party admits to the wrongdoing, the service provider will remove the image permanently.[249] If the image or video appears unlawful in its capture, or depicts criminal activity, then the service provider will be required to convey that information to the appropriate authorities.[250] The complaining party could also commence a lawsuit against the third party user, but may choose not to if satisfied with the removal of the image.[251]

To ensure that ISPs, search engines, websites, and online networks

---

243. *See* Burrell, *supra* note 57, at 747; Lipton, *supra* note 194, at 507-08 & n.197 (citing 17 U.S.C. § 512) (suggesting that a takedown remedy is more appropriate for plaintiffs in privacy infringement suits because their concern is about the embarrassment and psychological harm, and cites the DMCA as an appropriate model).

244. *See* 17 U.S.C. § 512(c)(3).

245. *See id.*

246. *See* Ariel Ronneburger, *Sex, Privacy, and Webpages: Creating a Legal Remedy for Victims of Porn 2.0*., 21 SYRACUSE SCI. & TECH. L. REP. 1, 29 (2009) (providing a similar proposal for removing infringing content with the opportunity for a third party to respond to any untruthful or exaggerated claims).

247. *Cf. id.*

248. *Cf. id.*

249. *Cf. id.*

250. *See Internet Crime Hearings*, *supra* note 98, at 2 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary) (explaining that "[c]urrent law already requires providers to preserve such data upon the request of law enforcement"); *id.* at 3 (statement of Rep. Bobby Scott, Ranking Member, Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary) (stating that "private industry already forwards over 100,000 leads a years to law enforcement").

251. *But see* 17 U.S.C. § 512(g)(2)(C) (2006) (differing from DMCA in that a lawsuit brought by the Internet user is not necessary to permanently remove the infringing material). This makes greater sense in the context of individual privacy infringements, because the claim does not necessarily involve protecting monetary interests.

will remove the unlawful images from the Web, the law must encompass an enforcement mechanism against those that do not comply. Similar to OCILLA, a potential threat of civil and criminal liability will ensure compliance with the takedown laws recommended herein.[252] However, this enforcement mechanism should not be used loosely, as it is not intended to burden OSPs and ISPs, but rather to motivate compliance with takedown requests.[253]

Imposing enforcement-based liability under the privacy takedown legislation will give the statute teeth, without defying Congress's initial purpose for the CDA. The enactment of Section 230 was meant to "encourag[e] ISPs to pursue their own online-content regulation and . . . methods . . . for protecting users [but instead] has become a shield from liability even when ISPs attempt no regulation whatsoever."[254] ISPs have taken advantage of the CDA, in part, because courts have over-read the protection the statute affords.[255] Only a year after the CDA was enacted, in a case involving a misappropriated post on an online message board, the Fourth Circuit "precluded distributor liability despite the lack of any explicit statutory language to support [its] determination."[256] Although this ruling, in *Zeran v. America Online, Inc.*,[257] has been accepted as the "contemporary interpretation of CDA immunity," some believe the Fourth Circuit went beyond Congress's original intent.[258] This is because historically under defamation law, there is a distinction between publisher and distributor liability, and "Section 230 expressly provides immunity to ISPs from liability as a publisher" but does not even mention immunity from distributor liability.[259] Thus, it may be understood that Congress's original intent was likely to immunize ISPs from publisher liability but not eliminate the possibility of holding them liable for passive conveyance of private or defamatory information.[260]

Although a privacy takedown law should be generally permissible, its application will not necessarily cover all cases of privacy

252. *See* 17 U.S.C. § 512(c)(1), (g)(2)(C).

253. *See* Burrell, *supra* note 57, at 747 (explaining that to avoid misuse of takedown liability against ISPs, only a "reasonable standard of care to make efforts to remove the infringing post in a reasonable time after receiving notice" should be applied).

254. *Id.* at 721-22.

255. *See id.* at 722-25.

256. *See id.* at 722-23.

257. 129 F.3d 327 (4th Cir. 1997).

258. *Id.* at 720, 723.

259. *Id.* at 719-20.

260. *See id.* at 713, 720.

infringement.[261] Certain types of images must be defined categorically for requisite takedown.[262] In trying to better classify takedown-worthy images, an initial line can be drawn through the use of criminal procedure laws.[263] For instance, the Fourth Amendment requires that searches and seizures conducted by law enforcement be done only if reasonable, and that searches be granted only upon probable cause.[264] In the context of the Internet, if the image posted was captured from an unlawful vantage point, as defined by Fourth Amendment jurisprudence,[265] and without the subject's knowledge or permission,[266] it would qualify for potential removal.[267]

In limiting this privacy takedown remedy further, some additional distinctions must be established. For instance, most people would agree that there is a difference between pornography or pseudo-voyeurism, where the individual knows they are being watched or photographed, and *verité* voyeurism, where the subject of the image was unaware and did not give permission to be photographed.[268] A takedown remedy would be inappropriate for those individuals who consented to being photographed and knowingly waived their rights to the image.[269] This limitation is important to "ensure[] that the [takedown of images] does not unduly restrict the free flow of [constitutionally protected]

---

261. *See* Calvert & Brown, *supra* note 2, at 504-06, 508 (describing First Amendment protections for certain images).

262. *Cf.* 17 U.S.C. § 101 (2006) (defining copyright infringing materials); *id*. § 512(b)(2)(E) (defining the kind of copyright infringement that is necessary to require a takedown of the image); 18 U.S.C. § 2256(8) (2006) (defining what constitutes child pornography); Lipton, *supra* note 1, at 948 (describing how some commentators believe that privacy harms are better redressed as specific, rather than general, harms).

263. *See* Lessig, *supra* note 126, at 58 (expressing certain limitations provided by the Fourth Amendment).

264. U.S. CONST. amend. IV.

265. *Cf.* Pesta, *supra* note 2, at 94 (indicating it was evident from the footage that Andrews was filmed naked in her hotel room through the peephole of her door); OPRAH, *supra* note 4 (indicating that the footage was evidently taken by a stalker because it was filmed in more than one hotel room).

266. *Cf.* Calvert & Brown, *supra* note 2, at 476 (explaining that *verité voyeurism* is when the target is unaware they are being photographed, and, as such, has not consented to being viewed and videotaped).

267. *Cf.* Burrell, *supra* note 57, at 747 (expressing similar limitations, specifically that ISPs should not be burdened with the "duty to remove simple references to an individual, []or . . . postings that do not . . . giv[e] out sensitive personal information").

268. *See* Calvert & Brown, *supra* note 2, at 476, 485 (defining *verité* and pseudo voyeurism).

269. *See* Levin & Abril, *supra* note 124, at 1011 ("The burden to protect sensitive information is logically placed on the invaded victim before an invasion occurs. Only plaintiffs who have maintained control over their information—by drawing their blinds or not sharing their secrets—can be vindicated."). However, if a third party is unable to show some proof that the photographs were taken with knowledge and consent of the aggrieved party, then they risk having the images removed from the Internet. *See supra* text accompanying notes 253-55.

information."[270] Another distinction is that of the public and private spheres.[271] Although there is no doubt that unauthorized public image capture and its dissemination is a growing issue,[272] as is public video voyeurism,[273] this takedown legislation is not geared to address those problems.[274]

Finally, when applying takedown law, the remedial distinctions for private versus public figures should be the same as their relative treatment under standard tort law. Just as public figures must meet a higher threshold of proof when seeking a remedy for defamation, they will similarly have to meet a higher standard—of clear and convincing evidence—in order to remove images that infringe on their more limited sense of privacy.[275] Celebrities tend to wield more power[276] and are often able to use powerful resources to affect a speedier takedown of private images.[277] On the other hand, because celebrities also attract more attention, their private images may circulate more quickly.[278] All in all, though, celebrities are not excluded from utilizing takedown measures because they too are entitled to have certain private images or footage remain private and off the Internet.[279]

---

270. Levin & Abril, *supra* note 124, at 1011; *see also* Burrell, *supra* note 57, at 747 (conveying concerns about the misuse of safeguard takedown laws).

271. *See* Kane, *supra* note 42, at 350 (discussing the tort of publicity of private facts and the fact that no protection is afforded to observations made in public).

272. *See* Blackman, *supra* note 46, at 313-14 (describing the increase in digital surveillance and its distribution through the Internet).

273. Calvert & Brown, *supra* note 2, at 479-80 (discussing the growing trend of voyeurism in public places like malls).

274. This proposal is intended to extend the effective implementation of already existing privacy torts to Internet intrusions and exposures, and not to necessarily expand the elements or applications of the torts.

275. *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974). The Court stated:

> The *New York Times* standard defines the level of constitutional protection appropriate to the context of defamation of a public person. Those who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention, are properly classed as public figures and those who hold governmental office may recover for injury to reputation only on clear and convincing proof that the defamatory falsehood was made with knowledge of its falsity or with reckless disregard for the truth.

Id.; *see also* SOLOVE, *supra* note 64, at 126.

276. *See Gertz*, 418 U.S. at 344 (distinguishing between public and private individuals, specifically "the likelihood that private individuals will lack effective opportunities for rebuttal, . . . [as] a compelling normative consideration underlying the distinction between public and private . . . plaintiffs").

277. *See, e.g.*, Soltis, *supra* note 11 (reporting that ESPN was able to get many of the Andrews images off of the Internet through public threats).

278. *See, e.g.*, Michael Y. Park, *Erin Andrews Calls Peeping-Tom Video a 'Nightmare'*, PEOPLE (Sept. 1, 2009), http://www.people.com/people/article/0,,20301731,00.html (reporting that Andrews's ordeal continued because of ongoing media coverage).

279. Jamie E. Nordhaus, Note, *Celebrities' Rights to Privacy: How Far Should the Paparazzi Be Allowed to Go?*, 18 REV. LITIG. 286, 288-89 (1999) ("Celebrities are entitled to the same general

C. Legislation Is the Key

As technology becomes a larger part of daily life, Congress must enact legislation that will help define our rights and protect our interests in a new digital world. There was a time when wiretaps had a dangerously intrusive effect on American lives; they devastated what most believed was the essence of privacy, the seclusion of one's home.[280] In response to changing technologies and legal standards, Congress enacted 18 U.S.C. §§ 2510–2522, which helped define the extent to which new technology, such as wiretaps, would affect individual privacy.[281] As a reaction to the complex privacy issues concerning novel present day technologies, Justice Alito recently reiterated Justice Taft's sentiments during the wiretap era: that the effect of advanced technology on individual privacy rights is "a matter better left for Congress."[282]

Although copyright law's takedown provision does not affect private images posted on the Internet,[283] Congress has shown interest in regulating the posting of certain images through other legislation, such as child pornography laws.[284] Some scholars have even suggested that the courts have gone as far as adopting what amounts to a "Child's First Amendment," which permits far greater regulation of speech when it implicates children.[285] Victims of voyeurism, who are exposed publicly without their knowledge or authorization, are like victims of child pornography in that they are vulnerable non-consenting victims of exploitation[286] and are left with a permanent electronic footprint of the crime.[287]

Specifically addressing the issue of unlawful capture of private footage, Congress proposed the Camera Phone Predator Alert Bill in

---

right of privacy that extends to all individuals.").

280. *See* Lessig, *supra* note 126, at 58-59.

281. *See* United States v. Jones, 132 S. Ct. 945, 962-63 (2012) (Alito, J., concurring) (discussing Congress's decision to "not leave it to the courts to develop a body of Fourth Amendment case law governing [the] complex subject" of wiretap).

282. *Id.* at 963.

283. *See* Lipton, *supra* note 1, at 930.

284. *See, e.g.*, Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736 (1998) (codified at 47 U.S.C. § 231 (2006)).

285. Calvert & Brown, *supra* note 2, at 502-03; *cf.* New York v. Ferber, 458 U.S. 747, 776 (1982) ("This special and compelling interest, and the particular vulnerability of children, afford the State the leeway to regulate . . . .").

286. Calvert & Brown, *supra* note 2, at 476, 504. Just as society protects children from unknowing exploitation, the rights of a voyeurism victim, who is also typically unaware of the camera's presence, should trump the audiences' free speech interest in receiving those images. *Id.* at 504.

287. Lipton, *supra* note 1, at 929 n.53 (discussing the problems of Internet permanence).

order to curb video voyeurism through the use of camera phones.[288] This Bill intended to address the rising problems of unauthorized video capture and the further dissemination of that footage.[289] However, the Camera Phone Bill's solution is far too limited in scope, as it deals exclusively with the image-gathering and does "nothing to stem the tide of global online dissemination of a damaging image."[290]

In addition to federal legislation, some states have enacted laws to address Internet crime and specifically video voyeurism. In response to the uncontrolled distribution of personal and damaging images, some states have adopted or amended video voyeurism laws that impose additional penalties for the dissemination of voyeuristic content.[291] In 1999, Louisiana enacted a law that directly confronted video voyeurism, or as it defined it: "[t]he use of any . . . image recording device for the purpose of observing, viewing, photographing, filming, or videotaping a person where that person has not consented to the observing . . . and it is for a lewd or lascivious purpose."[292] The Louisiana law went further by punishing the transfer of an image "by live or recorded telephone message, electronic mail, the Internet or a commercial online service."[293] In the same year, Connecticut enacted a similar law that applies to individuals who distribute—without permission—an image they knew was taken in violation of voyeurism laws.[294] Other states have also passed voyeurism laws, but have faced difficulties shaping those statutes to encompass all voyeuristic conduct within the bounds of contemporary principles of privacy.[295] These legislative measures indicate that lawmakers recognize some of the present day issues, but unfortunately,

---

288. Camera Phone Predator Alert Act, H.R. 414, 111th Cong. § 3(a) (2009) (requiring camera phones to emit a sound when a photograph is taken); Lipton, *supra* note 1, at 923.

289. Lipton, *supra* note 1, at 923-24. There is a general recognition that public postings of private or embarrassing moments can have devastating and long-term effects on chances of employment, education, and health insurance. *Id.* at 924.

290. *Id.* at 923.

291. *See* Calvert & Brown, *supra* note 2, at 521-23 (discussing various state efforts to formulate laws that will address Internet dissemination of voyeuristic images); Lipton, *supra* note 1, at 948-49; *see, e.g.*, CONN. GEN. STAT. ANN. § 53a–189b (West 2007); LA. REV. STAT. ANN. § 14:283 (2004 & Supp. 2012). Congress has addressed the criminal nature of voyeurism, but unlike some state statutes, the federal law does not address the dissemination of those images; *see also* 18 U.S.C. § 1801 (2006) (punishing the intent to capture an image of an individual's private area without their consent in circumstances where the individual has a reasonable expectation of privacy, but failing to address the issue of disseminating that image).

292. LA. REV. STAT. ANN. § 14:283; *see also* Calvert & Brown, *supra* note 2, at 521.

293. LA. REV. STAT. ANN. § 14:283.

294. CONN. GEN. STAT. ANN. § 53a–189b (West 2007); *see also* Calvert & Brown, *supra* note 2, at 523.

295. Calvert & Brown, *supra* note 2, at 524-25, 528, 530-32, 534-35, 538, 540-41 (analyzing Alaska, Florida, Missouri, Ohio, Pennsylvania, and Wisconsin law and the difficulties of capturing all voyeuristic content within the limitation of their state statutes).

none of these laws address the problems faced by individuals who want already posted images to be removed from cyberspace.[296]

D. Not a Constitutional Violation

The two-part recommendation in this Note is intended to provide a thoughtful basis for encouraging legislative action, but the proposed enactments raise some constitutional concerns. Regulation of the Internet will inevitably present Fourth Amendment privacy-type search and seizure problems. Similarly, takedown legislation poses issues for First Amendment restrictions on free speech. Despite these apprehensions, the recommendation proposed will not encroach on either Fourth Amendment or First Amendment rights of Internet users.

1. Fourth Amendment Rights

The regulatory scheme suggested herein is admittedly broad but will be no more intrusive than a lawful Fourth Amendment search and seizure carried out in real space. The Fourth Amendment mandates that searches and seizures conducted by law enforcement be done only if reasonable, and require that warrants be granted only upon probable cause.[297] Through a history of elaborate case law, the Supreme Court has defined the boundaries of a lawful search and seizure.[298] The Fourth Amendment test used today explains that a warrantless search would only violate the Fourth Amendment if conducted in areas where the target of the search had "a subjective expectation of privacy . . . that society accepts as objectively reasonable."[299] As explained earlier, the Internet presents an anomaly to this notion of "reasonable expectation of privacy" because virtually all of what transpires on the Internet—short of a few protected websites—is available to public viewership and leaves no room for an expectation of privacy to those who willingly post or access illegal materials.[300]

The Supreme Court has repeatedly acknowledged that technology affects individual expectations of privacy. In *Kyllo v. United States*,[301]

---

296. *See* Calvert & Brown, *supra* note 2, at 543-44 (summarizing state laws and attempts to address the problem); Lipton, *supra* note 1, at 930 (explaining that takedown law has been enacted for privacy infringement actions).

297. U.S. CONST. amend. IV; Lessig, *supra* note 126, at 58.

298. The Court defined private space and property in several decisions, specifically Katz v. United States, 389 U.S. 347, 351-53 (1967), United States v. Place, 462 U.S. 696, 697-98 (1983), United States v. Karo, 468 U.S. 705, 707, 712-13 (1984), Florida v. Riley, 488 U.S. 445, 447-48, 450 (1989), and Kyllo v. United States, 533 U.S. 27, 29, 33, 40 (2001).

299. California v. Greenwood, 486 U.S. 35, 39 (1988).

300. *See supra* text and accompanying note 137.

301. 533 U.S. 27 (2001).

Justice Scalia expressed that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[302] In *United States v. Jones*,[303] a more recent decision, Justice Alito expressed in his concurrence that "if the public does not welcome the diminution of privacy that new technology entails, they may either reconcile themselves to this development as inevitable" or allow their "concern about new intrusions [to] spur the enactment of legislation to protect against these intrusions."[304]

Fourth Amendment concerns may be particularly controversial in this instance, because regulating the Internet may include monitoring the way an individual surfs the Web within their own home.[305] The Supreme Court and various Circuit Courts have discussed the degree of privacy protection afforded to one's home, and specifically when engaging in illegal behavior there.[306] In *Katz v. United States*,[307] Justice Harlan explained that "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[308] In the same vein, the Supreme Court held in *Stanley v. Georgia*[309] "that . . . obscene movies or books . . . generally . . . constitutionally prohibited or punished when in public . . . are nonetheless *protected* by the First Amendment when read or viewed by a person in [their] own home."[310] However, some Circuit Courts have limited *Stanley* for Fourth Amendment purposes.[311] In *United States v. Whorely*,[312] "the Fourth Circuit stated that obscene materials obtained through e-mail or through an 'interactive computer

---

302. *Id.* at 33-34 (providing a brief history of the changes technology has made on individual expectations of privacy).

303. 132 S. Ct. 945 (2012).

304. *Id.* at 962 (Alito, J., concurring).

305. *See* Lessig, *supra* note 126, at 58 (describing the sanctity of one's home from government searches); *Kyllo*, 533 U.S. at 31. In *Kyllo*, the Court held:

> The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."

Id. (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

306. *See infra* text accompany notes 307-14.

307. 389 U.S. 347 (1967).

308. *See id.* at 361 (Harlan, J., concurring).

309. 394 U.S. 557 (1969).

310. Blitz, *supra* note 143, at 359; *see also Stanley*, 394 U.S. at 565.

311. Blitz, *supra* note 143, at 359-60.

312. 550 F.3d 326 (4th Cir. 2008).

service' are not within the scope of *Stanley v. Georgia*'s protection."[313] Similarly, the Third Circuit also rejected the application of *Stanley* in Internet cases.[314]

All of this suggests that monitoring illegal material or unlawful conduct within easily accessible public websites is lawful within Fourth Amendment parameters.[315] This leads to the conclusion that it would be constitutionally permissible to allow law enforcement to trace posters of illegal materials when the forums on which they post those materials are public.[316] There is no *reasonable* expectation of privacy in posting private materials in a public place.[317]

2. First Amendment Rights

Takedown structures that make certain unlawful material less available for public viewership affect, but do not unconstitutionally abridge, First Amendment freedoms.[318] Freedom of speech is a fundamental right in American society, and the Constitution guarantees that "Congress [will] make no law . . . abridging the freedom of speech."[319] Generally laws that regulate the display of images, which are not classified as unprotected speech (i.e., obscene or child pornographic material), are subject to strict scrutiny.[320] Similarly, speech expressed via the Internet also receives full First Amendment protection.[321] Under the strict scrutiny test, a law must be the "least restrictive means to achieve a compelling government interest."[322]

---

313. Blitz, *supra* note 143, at 360; *see also Whorely*, 550 F.3d at 332-33.

314. Blitz, *supra* note 143, at 360-61 (citing United States v. Extreme Associate, Inc., 431 F.3d 150, 161 (3d Cir. 2005)).

315. *See* Kyllo v. United States, 533 U.S. 27, 32 (2001) (explaining that examining or viewing anything from a public viewpoint—including a portion of a house—is not an unreasonable search within the meaning of the Fourth Amendment, if it constitutes a search at all); *see also supra* text accompanying notes 136-43 (discussing the privacy distinctions of various kinds of websites, and the public nature of some Web pages).

316. *See* Blitz, *supra* note 143, at 362 (concluding that based on post-*Stanley* cases, the privacy of the home, as it relates to First Amendment protections, does not extend any further than the physical space—in other words it does not extend to the virtual spaces on the Internet, which are considered outside of the home).

317. *See* Katz v. United States, 389 U.S. 347, 361-62 (1967) (Harlan, J., concurring) (explaining what constitutes a *reasonable* expectation of privacy).

318. Lipton, *supra* note 1, at 949 (discussing privacy on the Internet and the conflict of First Amendment speech protections).

319. U.S. CONST. amend. I; SOLOVE, *supra* note 64, at 125. "[T]he Supreme Court currently resolves free-speech cases by balancing speech against opposing interests." *Id.* at 128.

320. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

321. *See* Reno v. ACLU, 521 U.S. 844, 868-70 (1997).

322. SOLOVE, *supra* note 64, at 128.

However, not all forms of speech are protected equally and some varieties of speech receive less protection.[323] For example, the Supreme Court gives less protection to commercial speech.[324] The Supreme Court, despite First Amendment concerns, has also limited protection for speech related to public disclosure tort suits.[325] "In one case, the Supreme Court concluded that . . . [i]t is speech on 'matters of public concern' that is 'at the heart of the First Amendment's protection' . . . [and thus,] speech of private concern should be given much less protection than speech of public concern."[326]

The Supreme Court's discussion on balancing privacy and free speech indicates that speech concerning private matters should be given less protection than speech of public concern.[327] To further support the Court's sentiment, the justices in *Griswold* declared a fundamental right in making choices about one's private life without public exposure or scrutiny.[328] The interests of protecting the privacy of victims and shielding children from voyeuristic sexual images are certainly important, if not compelling.[329] Thus, a narrowly tailored law providing for the takedown of unauthorized private images will likely pass the lesser scrutiny test afforded to such material.[330] In reviewing any such privacy takedown law, the Court will hopefully recognize that unauthorized private publications are direct violations of both the right to (1) protect sensitive information from disclosure, and (2) make independent personal choices.[331]

V. CONCLUSION

Although there are many barriers to protecting individual dignity and privacy on the Internet, there are also many reasons why the public should demand this initiative be a priority.[332] Basic regulation of the

---

323. *Id.*

324. *Id.* at 128.

325. *Id.* at 129.

326. *Id.* (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758-59 (1985)).

327. *Id.* at 128-29.

328. Griswold v. Connecticut, 381 U.S. 479, 494 (1965) (Goldberg, J., concurring).

329. *See* Reno v. ACLU, 521 U.S. 844, 849 (1997) (expressing that there is "legitimacy and importance [in] the congressional goal of protecting children from harmful materials"); *Griswold*, 381 U.S. at 494 (Goldberg, J., concurring) (finding "the right of privacy [to be] a fundamental personal right, emanating from the totality of the constitutional scheme under which we live" (internal quotation marks omitted)).

330. *See* SOLOVE, *supra* note 64, at 128-29 (citing *Dun & Bradstreet, Inc.*, 472 U.S. at 758-59) (holding that speech of private concern should be given less protection).

331. *See supra* text and accompanying notes 34-35.

332. *See* SOLOVE, *supra* note 64, at 129-32 (explaining "why free speech is valuable" by

Internet will allow law enforcement to find those individuals who choose to abuse its use.[333] As Professor Lessig put it: "[w]e must make a choice about life in cyberspace—about whether the values embedded there will be the values we want."[334] This does not mean we should prohibit the availability of lawful, albeit lascivious or distasteful, content on the Internet. Instead, it means we should take a hard stance about punishing those who disseminate material that is not lawful, and offensive to our sense of dignity and privacy.

The two-part solution is the key. Regulation is an important part of the solution in curbing cybercrime. As the Internet increasingly becomes a part of Americans' daily lives, more regulation will be required to ensure a safe cyber community. However, no cyber-law can be effective without means for enforcement. Creating an Internet architecture that will allow law enforcement to identify criminals is merely the first step towards a safer online community. The proposed privacy-based takedown legislation is meant to expand the available remedies for legally actionable online privacy violations. In other words, this legislation is not meant to expand privacy rights, but rather provide better remedies for those who have actionable claims.[335] There is no reason why an intrusive or unlawfully obtained image should continue to be available on the Internet for further dissemination.

Victims like Erin Andrews deserve "to be let alone" and to find peace with the crimes that have befallen them. Andrews is the face of a fight for privacy in a modern day culture that allows entrepreneurs to make money off of another's defenseless sorrow.[336] Andrews had a right to her privacy within the confines of her hotel room,[337] but without the fortunate coincidence of a suspicious lead that led police to her

---

reason of principles like individual autonomy, democracy, and the marketplace of ideas). *See contra* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 489, 491 (1975) (deciding that sometimes freedom of speech takes precedence over the right to privacy).

333. *Internet Crime Hearings*, *supra* note 98, at 6-8 (statement of Jason Weinstein, Deputy Assistant Att'y Gen., U.S. Department of Justice).

334. Lessig, *supra* note 93, at 548.

335. *See* RESTATEMENT (SECOND) OF TORTS § 652A–E (2000) (laying out the elements necessary to fulfill each privacy tort); s*ee also* Lessig, *supra* note 93, at 508 (expressing that the law regulates some cyber conduct more efficiently than others).

336. Calvert & Brown, *supra* note 2, at 480-83 (describing the incredibly lucrative online industry of pornography, which enjoys a significant viewership of voyeurism).

337. *See* 18 U.S.C. § 1801 (2006) ("Whoever . . . has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined . . . or imprisoned."); RESTATEMENT (SECOND) OF TORTS § 652B ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

stalker,[338] and without the tremendous influence of ESPN, she may have never received justice, or been able to remove her video from the Internet.[339]

There are no illusions about the difficulties in trying to implement an effective regulatory structure for the Internet or a successful privacy takedown system.[340] The complexities of reforming an elaborate Internet structure or creating an efficient report and takedown system present a number of concerns.[341] The hope is to establish a legal framework for making such regulatory and privacy-based takedown systems possible and allowing Congress and the Courts to tease out these problems along the way.

*Maayan Y. Vodovis**

338. *See* Pesta, *supra* note 2, at 94; *see also 2½ Years*, *supra* note 53 (explaining TMZ's role in the investigation of Andrews's stalker).

339. *See* Soltis, *supra* note 11 (reporting that EPSN played a major role in removing traces of the video from the Internet).

340. *See Internet Crime Hearings*, *supra* note 98, at 34-35 (expressing concerns over implementing a full tracking system); Lipton, *supra* note 1, at 949 (expressing concerns over how to logistically protect privacy on the Internet).

341. *See* Lipton, *supra* note 1, at 954 (expressing concern over the effectiveness of a regulatory framework in light of the global scale of the Internet); *supra* Part IV.D.

* J.D. candidate, 2012; Hofstra University School of Law. This Note is dedicated to my family and entire support system of friends and colleagues. Despite my intermittent absence, my family and friends have been a source of incredible support. Thank you for your constant care, love, and patience. Specific thanks go to my mother for her encouragement and unceasing support throughout my life and the last few years of law school, and to my sister for her attention and friendship when I needed her most. My sincerest gratitude goes to Rob Lattin, who has provided love, security, and laughter to my life, and without whom these last three years would have been far more difficult. I would also like to acknowledge the editors of the *Hofstra Law Review* for their help throughout the writing and editing process of this Note, especially Katie Porter, Chris Leo, Stephen Piraino, Simone Hicks, Allana Grinshteyn, Rebecca Sklar, and Dave Gerardi. I also extend my gratitude to Professor Akilah Folami for her guidance throughout the Note-writing process, including her thoughtful substantive and editorial suggestions.