The New Porn Platform:

Standards Gaps in 'Revenge Porn' Policy and Protection

Jilanne Doom

Georgetown University

CCTP 644 Global Standards: What's at Stake?

In a time of rapid technological advancement and the social networked society, the current legal standards put in place to protect our personal information and online data are becoming increasingly archaic. Even more dangerous for our privacy is the rate at which these standards are able to evolve, which is often far too slow or not at all. A rising threat to privacy due to the law's inability to keep pace with technology, especially for young digital natives, is intimate private made public content, better known as 'revenge porn.'

Revenge porn is the term encompassing all types of distribution of private, intimate digital content such as nude images or videos. The threat of this type of distribution has existed for some time; however, the practice began garnering media attention in 2010 with the launch of an amateur pornography site named IsAnyoneUp.com. The site catapulted the practice to extreme levels because it created a platform, accessible to anyone with Internet access, where users can submit not only private images, but also identifiable and contact information (Garfield 2011). Though the site was shut down in 2012, hundreds of replacement sites have appeared in its stead.

Where previously, distribution of intimate images was possible among contact channels like mass emailing or Facebook shares, this content can now reach the masses with even greater ease – and with very little legal protection for those it affects.

For the purpose of this paper, the definition of 'revenge porn' material will be reassessed and split into different terms. This specification is necessary in reference to this type of content because not all instances of intimate data leaks or distribution are carried out in a vengeful manner. Some surface in the form of mass data leaks involving a large number of people with whom the presumed hacker has no personal connection. In this instance, the term 'private made public content' will be used. It is also important to identify this content by its intimate nature in reference to privacy laws. Privacy laws contain protections for many types of ownership, including both online data and offline possessions and space. When referencing the missing privacy standards in these cases, the term 'intimate data' will be used to encompass digital property of an intimate nature, such as nude photographs or videos. The term 'revenge porn' will remain in cases concerning the distribution of intimate data with a vindictive nature and, because it is the most widely accepted term, it will also be used to represent the general practice.

In response to the increasing popularity of revenge porn, a small number of states have enacted legislation to provide some protections to those depicted in the images or videos. However, there is no federal law for online privacy protecting victims of revenge porn (Nelson 2014). Even more troubling, the few state laws that are in place rarely contain proactive standards protecting this data from being distributed in the first place. Most of these new laws are merely reactionary, only doling punishment after the damage has been done. An argument worth raising to this point is the importance of an adaptable

legal framework that could theoretically change as technology advances. This new set of standards will be discussed in the sense of economist Brian Arthur's concept of modularity.

In addition to the lack of legal standards providing protection, another missing standard that could curb the amount of intimate content available for distribution is Internet and social networking education for young people. Millennials – the generation of young adults who have grown up in the technology boom – have staked their identities in online communication and networks (Najdowski & Hildegrand 2014). The standards for sharing personal information with one another via online networks has become commonplace, and many people lack the understanding of just how much of our personally identifiable information is available on the web. This lack of education about a vital aspect of our lives coupled with the sheer distributive power of the Internet creates a breeding ground for hackers and ex-lovers alike to share intimate content never intended for the public.

Currently, a number of players are at work to change the legal standards and potentially the legal framework to protect people from privacy leaks in a technologically advancing environment. However, an even larger network possesses the capabilities to create and distribute revenge porn – namely, anyone with Internet access. Organizations like the Cyber Civil Rights Initiative (CCRI) and several state legislatures are working on advocacy and drafting or passing new legislation. One powerful tool working against these groups' efforts is the constitutionally protected freedom of speech. Another roadblock to these protections occurs when the victim creates these images or videos themselves (Najdowski & Hildegrand 2014). The complex web of players involved in

both the creation of this content and those working to halt or protect the practice is highly complex.

This paper looks to identify the multifaceted issues related to the practice of revenge porn and pinpoint the missing legal standards for protection and the educational standards for prevention. Part I of the discussion begins with an explanation of the practice of revenge porn, and how that very definition conflicts with the language of current privacy law. Federal and certain state laws will be dissected to pinpoint the exact standards gaps where revenge porn cases can fall through.

Following the analysis of legal standards, Part II moves toward the work being done to change the legal framework and how a series of social and political standards curb these efforts. More specifically, these social standards include the shifting of our identity standards toward the sharing and social networking culture, are causing people to become more apt to trust and share intimate content with others (Toogood 2014). Politically, these roadblocks include certain rights that revenge porn legislation could infringe upon. Similarly, taking a legal stand against the practice could cause heightened self-censorship by Internet companies and users (Nelson 2014).

In Part III, the legal gaps and social and political standards will be used to examine a series of case studies that each exemplify a different aspect of the missing standards in revenge porn cases. The first of these cases is the recent leak of nude photos of over 100 celebrities. This case represents the sheer power of technology and the ability of those able to navigate it to compromise the intimate or merely private data of large groups of people or, namely, anyone who uses the Internet. The second case study is that of the first revenge porn instance in New York State in which the perpetrator tweeted

nude photos of an ex-girlfriend. This case raises the issue of consent when the images were given to the perpetrator but in a private manner. It also provides substantial evidence of the many standards gaps in current revenge porn laws. The final case study looks at the social issues raised at the fore of this practice through the lens of the former Internet site IsAnyoneUp.com mentioned earlier.

Part IV argues for a different approach to preventing revenge porn, that media literacy and online safety education are a viable alternative to current ineffective legal attempts. Research shows that, like standards for revenge porn, policy and educational standards for teaching Internet safety in the classroom has developed entirely too slowly to address risky online practices of young people (Choulat 2010). Therefore, educators and parents alike must take a different approach to teaching children the importance of Internet safety. If effective and accessible curricula for parents and teachers can be developed, it could create a safer environment for young people to utilize online networking without putting themselves at risk to becoming a victim of revenge porn.

Literature Review

At this time, a limited amount of scholarly research exists regarding the practice of revenge porn and the privacy law limitations of intimate data. Though online privacy concerns have existed for decades as the free flow of information through communication channels continues to multiply, the practice of distributing intimate data for the purposes of revenge, popularity or monetary gains is rather new. A key reference article for this paper is Danielle Citron and Mary Anne Franks' *Criminalizing Revenge Porn*. This paper from the Wake Forest Law Review takes an historical approach by examining privacy

law that covers topics like identity theft and disclosure of individually identifiable information and applies it to the development of legislation for criminalizing revenge porn. Another important point this piece makes is how copyright law can be leveraged as an advantage against the argument that those who take the intimate photos themselves are responsible for the content disclosure (Citron & Franks 2014).

As a first step toward this potential legislation, Franks, the Vice President of CCRI, also authored a "Guide for Legislators" for approaching the subject of revenge porn from a policy standpoint. The guide provides the essential elements for a new standard and a model of a state law, along with relevant statistics and case studies (Franks 2014). This model could provide potential fillers for the current standards gaps.

In the discussion of inadequate privacy policy and the development of new frameworks to address distribution of intimate data, the concept of modularity could provide an innovative approach to reshaping the legal system to fit the tumultuous interconnected society in which we live. This concept, described by Arthur in *The Nature of Technology*, breaks down a system into sub-parts that have the ability to be rearranged as circumstances or needs change (Arthur 2009). Modularity is no stranger in many fields, as it has become an integral concept in creating the evolving technology of our time. So why not integrate that into the legal system, which has proven too slow to adapt to this technology? This discussion could reshape privacy law to imitate the rapidly evolving technological environment in which it lives. The concept of modularity will be applied in a theoretical sense, with admitted flaws, to propose a new way to approach revenge porn legislation. Another reference for this restructuring discussion will be Adam Thierer's piece from the *Harvard Journal of Law and Public Policy* that stresses a multi-

layer approach to upholding and creating online privacy standards. Thierer suggests the "3-E" approach, which combines education, empowerment and enforcement (Thierer 2013).

In the analysis of social and political challenges to combating revenge porn, David Grewal's leverage points, which he identifies in *Network Power: The Social Dynamics of Globalization,* will provide unique evidence as to why this practice remains so prevalent despite general public disdain. Grewal identifies three leverage points of the Internet that result in its infinite power as a network: compatibility, malleability and availability. These points will be discussed in reference to how revenge porn has risen to popularity and how the Internet will allow the practice to further blur our online privacy rights and comprise intimate data.

Two others pieces that will provide an interesting view of changing social standards that impact how much we share online are a sit-down interview with IsAnyoneUp.com founder Hunter Moore and an academic blog from *The Telegraph.* The Moore interview discusses the business of revenge porn and why making a profit from it is a viable source of income due to the current culture of "over-sharing" (Garfield 2011). The academic blog by Dr. Laura Toogood discusses the dangers young people face when they are not aware of the consequences of how much they share online. Children and their parents alike not only face physical danger, such as online predators, but also emotional distress (Toogood 2014). The journal article from the *American Psychological Association* "The criminalization of 'revenge porn'" discusses how legislators must also take into account the psychological impacts revenge porn has on victims when creating new standards (Najdowski & Hildegrand 2014).

An important view of political standards blocking the way for new privacy standards is examined in a *MIT Technology Review* academic blog by Vivek Wadhwa. "Laws and Ethics Can't Keep Pace with Technology" gives current examples of other legal instances where technological capabilities are creating gaps in policies. Wadhwa argues that the political process is far too slow and regulated for laws to ever keep pace with advancing technology (Wadhwa 2014).

These legal, political and social standard gaps will then be made evident in three recent case studies. The first of which is the highly publicized "Celebgate" instance that compromised the private images of over 100 celebrities stolen from Apple's iCloud in August 2014 (Kedmey 2014). Jennifer Lawrence, the most outspoken celebrity regarding the break, has demanded heightened punishment and revision of the law to address the case, but concrete revision in policy standards have yet to be reached (Ehrenfreund 2014). At the current time, the iCloud hacker(s) has not been discovered. Through a series of news articles from outlets such as *TIME* and *The Washington Post,* this case will be detailed and compared to the current federal privacy standards.

The second case study involves a clear-cut example of the original sense of revenge porn. A New York man was arrested for distributing nude photos of an ex-girlfriend on his Twitter account in a vengeful manner. Ian Barber, the man on trial, was charged on three counts but was acquitted of all charges when the judge found his actions fell through the legal gaps. This was New York's first case involving revenge porn (Yaniv 2014). This case, also detailed from media reports and legal analysis of New York state law, will provide concrete examples of the many standards gaps and the lack of progress that has been made despite the public's awareness of the gaps.

The third case study will focus on a specific web platform for distribution of revenge porn material. This analysis will be a deeper look at the site IsAnyoneUp.com mentioned earlier and its now celebrity-status creator, Hunter Moore (Garfield 2011). Because of missing legal standards, the site was never closed down due to its insidious nature; instead, it remained online for two years before being removed for employing a hacker who stole many of the photos being posted (Dodero 2012). The study also provides an interesting but sobering view of the identity standards of the Internet generation and how they could be creating a more vulnerable online environment for young people. Media reports, an analysis of an interview with Moore, and the *American Psychology Association* journal article will be used in this case study.

In the discussion on Internet safety education in Part IV, the primary resource for the current policy and education standards is information technology specialist Tracey Choulat's "Teacher Education and Internet Safety." Choulat sets a foundation for Internet safety curriculum and the importance of educators and parents to introduce these concepts to young adults despite lagging educational and policy standards that have yet to be implemented (Choulat 2013). A report from the Wilson Center and Paul Vallas highlights the lack of STEM educational standards in US schools, which could be a factor in young people's lack of understanding of technology systems and social network power (Vallas & Pankovits). Thierer's "3-E" approach will also be integrated into the discussion as education being the first aspect to changing our online privacy landscape (Thierer 2013).

Part I

As acknowledged, revenge porn in all its forms is becoming a more pervasive problem as technology continues to advance, people continue to share rather than protect, and our legal standards remain stagnant. This section will identify the legal landscape of revenge porn legislation, specifically the language of state laws, the lack thereof at the federal level and the standards gaps in which revenge porn creators and distributors can slip through in the legal system.

Among the first states to enact revenge porn-specific policy, California recently sentenced one year in prison in its first revenge porn guilty verdict. California and others like Virginia and Utah have seen actual progress in cracking down on perpetrators because of effective definitions in the legal language. The California state law "prohibits someone from posting nude photographs online for the purpose of causing emotional harm" while further detailing what emotional harm encompasses (Rocha 2014). Where many states falter in their language, allowing loopholes, is merely identifying revenge porn as "nonconsensual pornography" but not including mention of intent. Another intent issue is that of intimate data stolen and distributed for monetary gain; there is no explicit intent to the harm the individual personally, just benefit from their likeness (Stuart 2014). And often in these cases, the actual perpetrator of stolen data is difficult to trace because of Internet anonymity.

While state legislators seem to be realizing the issue but not always hitting the target, it is in the federal standards that Americans are most vulnerable. As mentioned, currently no federal standard definition or legal framework for revenge porn exists. Because of the issue's amorphous and disputable nature, coming to a nationwide consensus has proven quite difficult, allowing individual states to come to their own legal

standards. This avenue is acceptable, but only until cases where a single geographic location is untraceable. Blog forums and revenge porn platform sites present this issue because they are available to users nationwide, not to mention globally. When a victim's intimate data lands on one of these platforms with often-anonymous posters, where can the victim turn for justice? The answer is not simply toward the website host, which will be discussed further in the third case study of this paper. Lack of a federal standard is becoming a dire problem for these victims as the practice becomes more and more common.

Of the multitude of standards gaps evident in an array of criminal statutes used to charge revenge porn perpetrators, it is important to focus on two brought to the fore by Citron and Franks for the *Wake Forest Law Review.* First, revenge porn legislation must include a component addressing harassment, however, "criminal harassment and stalking laws only apply to defendants who engage in repeated harassing acts" (Citron & Franks 2014). Many of these components address that emotional harm must be a result of continued harassment, but nearly every instance of revenge porn examples will show that just one post, distributed online to the masses, causes emotional distress. Nevertheless, the law concludes that one act is permissible and not considered legal harassment. The second major gap lies in whom the harassment is directed toward. Most revenge porn law states that abuse must be directed toward the victim, however, most case of revenge porn include the dissemination of intimate data to the masses for embarrassment purposes rather than directed toward the victim (Citron & Franks 2014). This gap speaks directly to the issue that the legal standard is not in fully understanding of the concept of the

practice. This gap will manifest itself in the second case study of this paper detailing the New York man acquitted due to "insubstantial evidence" (Yaniv 2014).

Several avenues exist for lawmakers to make changes to better reflect the gaps in policy, but one must consider an alternate framework from the "one silver bullet" approach the majority of US legal standards take (Thierer 2013). As technology advances, so too should our approach at protecting individuals in the tumultuous and often muddy environment. Franks and the CCRI have developed a robust recommended legal framework and have actually advised many states in drafting their own revenge porn policies. Among the most important points on their recommended standards for revenge porn policy are "clearly set out elements of the offense," a very explicit list of what are the exceptions, and a deliberate focus on not confusing intent with motive (Franks 2014).

Another – admittedly abstract – attempt at reshaping the revenge porn landscape includes the concept of modularity as applied to law. As mentioned earlier, the silver bullet approach is useful in clearer applications of the law. Revenge porn does not fall into that category. A modular approach, in the legal sense of the technological concept described by Brian Arthur, means taking different elements of the law and combining them as seen fit for each individual case, but still placing them under an umbrella charge of revenge porn creation or distribution (Arthur 2009). To give this approach more context, say a perpetrator finds a nude photo in his ex-girlfriend's property, creates a tweet and sends the nude image to his Twitter followers with the intent to cause her emotional distress. He could be charged with one count each of revenge porn creation and revenge porn distribution, modular charges that would incorporate the different levels

of revenge porn activities and motivations with the elements of his crime. Under creation, he is guilty of nonconsensual use of pornography, copyright infringement and possession of stolen property. Under distribution, many of these same actions also apply, but his motivations could include the motive to cause emotional distress and potentially slander, but not monetary gain for copyright or stolen material. Clearly this approach needs further refinement, but it could present a new way in which many types of technology or privacy crimes are approached, eliminating the archaic one-application, silver bullet approach.

Part II

As revenge porn becomes a more recognized form of harassment and online victimization, several activist groups and notable individuals have sprung to take action in changing legislation. The aforementioned CCRI and its proposed legislative framework along with celebrity pressure like that of "Celebgate" victim Jennifer Lawrence have forced state lawmakers to take a serious look at revenge porn standard reforms. As of now, just 12 states have passed legislation specifically aimed at revenge porn, but many others appear to be soon to follow.

Other types of platform standards in society weigh heavily on these legislative reforms, including social identity standards, fundamental network standards and American political standards. Growing up in a technologically innovative time while simultaneously engaging in the Internet as the pioneers of social networking, the millennial generation has shaped what can now be referred to as the "sharing culture." No other time in history have such a vast number of individuals been so personally

connected, in both the sense of availability of information on one another and their willingness to share their personal information with the masses. Consequently, this sharing culture has reshaped the identity standards upheld by the population, increasingly the younger the Internet user. As users become more apt to share personal information via online platforms, they often become more unaware of the dangers and consequences this presents. Dr. Laura Toogood of Digitalis explains this trend: "While many children are oblivious to privacy controls, or under pressure to ignore them, others are aware of how to take advantage of unprotected accounts and use this as a bullying tactic" (Toogood 2014). Toogood says online dangers, like the potential to fall victim to revenge porn or even physical harm, are becoming more and more prevalent while simultaneously becoming more easily disguised, creating an online environment ripe for creating Internet privacy victims (Toogood 2014; Najdowski & Hildegrand 2014). This presents a great roadblock for legislators and activists: How are lawmakers supposed to change the language to protect users who are often the ones, even unknowingly, placing themselves at risk?

Even the very fundamental structure of the Internet competes with the US's rigid legal framework. In David Grewal's analysis of networks in *Network Power,* he discusses three leverage points that together determine the power of a network. These three points, availability, compatibility and malleability, combined with the Internet's colossal user base make it the most powerful and widely used network on the globe (Grewal 2008). With these points in mind, one can clearly see a framework for how private content travels online and impacts millions of users faster and more efficiently than every before.

The Internet provides an open platform for its nearly 3 billion users to search or come into contact with content from a vast number of sources on an infinite number of topics. Its *availability* is striking. Aside from certain censors, such as government, educational, etc., Internet content has the potential to reach users from all corners of the globe, especially if it comes into contact with other mass communication platforms like television. Also, when the content is of a widely interesting topic to Internet users or of a taboo nature, like conflict, celebrities or pornography, the availability aspect is duplicated, due also to its relevancy factor. Therefore, the more people are sharing and posting the content, in this case revenge porn and intimate data, the more available it becomes to users.

While the network's inner framework is a clear example of how billions of different types of pages, documents and interfaces can work across one another seemingly seamlessly, it is the outer framework of communication technologies that relates to revenge porn dissemination. In terms of *compatibility,* Internet content can be accessed, shared and used by people from many types of devices and be formatted for sharing effectively. Leaked YouTube videos can be shown on television programming; leaked photos can be saved onto someone's smartphone and texted to a group of friends. The compatibility aspect makes Internet content infinitely shareable.

Arguably the most beneficial to its success as a platform and at distributing private-made-public content is the Internet's *malleability*. Grewal states that there is a malleability sweet spot that networks must have in order to remain open to revision but retain their measurable standards and network power (Grewal 2008). The Internet as a

whole has managed to retain its network framework while still allowing site and content creators to transform its interworking parts to suit specific needs. For example, revenge porn site creators such as Hunter Moore with IsAnyoneUp.com have built their own platforms to allow users to upload their own content and develop the site to their specifications, and the stability of the Internet framework standards support the channels by which this content is shared from hub to user and vice versa. Additionally, these creators have embraced site facilitator standards to not only manage these pages, but also protect themselves from lawsuits.

Finally, the political history and framework of American society faces great challenges today in many issues similar to the ethics-versus-freedoms battle evident in revenge porn regulation. The Founding Fathers set a political standard that "must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times" (*Thomas Jefferson*, Wadhwa 2014). However, as Stanford technology fellow Vivek Wadhwa poses, if the human mind cannot keep pace with the technology we are creating, how can our laws, which are shaped by the people? One political standard applicable to revenge porn is the freedom of speech. Critics argue this type of legislation infringes on this freedom, both that of the distributor and the creator (Najdowski & Hildegrand 2014). Essentially, if one wants to share pornographic images for whatever reason, they should not be penalized because of the few who take part in the practice with malicious intent. Furthermore, if one wants to create intimate data for their own personal use, the law should not discourage them.

Part III

The following case studies provide examples of three distinct shapes revenge porn can take: single instance mass leaks of private-made-public content; classic revenge porn distribution by an ex-lover; and an open Internet platform where users participate for a variety of motivating factors.

1. “Celebgate”

In August 2014, an unknown hacker or group of hackers broke through Apple’s security walls in the iCloud data storage service and distributed private photographs found inside the accounts of over 100 celebrities or public figures by taking advantage of a password guessing hole (Vaughn-Nichols 2014). While many of these images were considered harmless to the appearance of those portrayed, some were authentic nude or suggestive photographs. Of the group victimized by the hack, two of the most well known and negatively affected were actress Jennifer Lawrence and model Kate Upton. Since the security breach and lack of progress in punishing those responsible, Lawrence has called for serious updates to the online privacy legal landscape.

However, because of the lack of a federal legal statute addressing revenge porn, those responsible for “Celebgate” will likely never receive full punishment for the damage they caused. Lawrence’s camp has announced a full investigation and to prosecute any member of the online community who distributes the photographs, but that is likely the extent of action. Leaks such as these involve thousands, potentially millions of players, many of which are painstakingly traced. Even if Lawrence’s and other celebrities’ lawyers take the time to track each of these distributors and websites, the

highest extent of the law they could prosecute these individuals is copyright infringement – a tool many agree is not ideal (Ehrenfreund 2014; Kedmey 2014). Furthermore, if the original hackers are caught, they could receive stiff punishments, especially due to lawsuits from Apple, but no law currently stands at the federal level that would specifically address the emotional distress and stolen intimate property of those whose cloud accounts were compromised.

2. New York's first revenge porn case

Until recently, no legislation explicitly targeted toward revenge porn existed in New York, which resulted in an acquittal in the state's first revenge porn case. In July 2013, Brooklyn resident Ian Barber shared nude photos of his former girlfriend to the woman's sister and employer, as well as his personal Twitter account. However, because of three clear gaps found between the law and the charges filed against him, the judge dismissed the case in February 2014. Even after the court determined permission was never granted to expose the photos online – the defendant claimed otherwise – the judge concluded "current laws are insufficient to sustain the allegations" (Yaniv 2014).

Barber was charged with three misdemeanors: one count each of aggravated harassment, dissemination of unlawful surveillance and public display of offensive sexual material. Unfortunately for the victim, in each charge, a loophole existed. For harassment to stick, some type of communication must be sent to the victim whereas Barber sent the images to her family and colleagues. For unlawful surveillance, images must have been obtained illegally whereas Barber was sent the photos in confidence before the relationship ended. Finally, as arguably the most outdated law in this case, for offensive

sexual material, nudity in the photo is not the only stipulation. The image must be posted for public display, which New York law does not consider Twitter because it is a subscription service (Yaniv 2014). Therefore, not only does New York law view Twitter as a private space, despite the facts it is free, highly accessible and widely used, it also presents clear standards gaps for revenge porn distributors to slip through.

It is important to mention that, as of August 2014, the governor of New York closed one legal loophole that could impact future revenge porn victims in the state. The former unlawful surveillance law stated that a person could not "broadcast images of another person engaged in sexual activity with the person's consent" but the law "required that certain body parts be identifiable." The new law removes that caveat, making any broadcast sex act without those depicted permission illegal (Weaver 2014). However, the law makes no mention of the standards gaps exploited in the original case study.

3. IsAnyoneUp.com

The third case study exemplifies revenge porn in its arguably most malicious form. Before the site was removed from the web in 2012, IsAnyoneUp.com operated as a platform allowing users to upload content, specifically nude or suggestive images of themselves or others, and distribute it across the site or the web, often including identifiable or contact information. While the site remained under close watch by authorities and continued to gain bad press for its detestable intent, it found refuge in a legal clause that would allow it to continue operations for its two and a half years on the web. Title V or Section 230 of the Communications Decency Act of 1996 states: "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." This legal standard, along with a three-prong test, allowed the site's founder and administrator, Hunter Moore, to escape many legal battles from outraged women, and sometimes men, who found their images on the site (Garfield 2011). Even when these revenge porn victims sought justice through claiming copyright or any other legal avenue, they could not attack the site because it was the individual user who was held legally responsible for the uploads. Therefore, even though the site's content might violate a plethora of moral and legal standards, the often-anonymous online user was the only perpetrator who could be found at fault.

However, in 2012, IsAnyoneUp.com was shut down because it had finally been found in violation of legal standards that could be brought against its administrators. After a string of strange Gmail password hacks that each coincidentally led to the victim's photos posted on the revenge porn site, the scam was eventually traced back to a hacker named Charles Evans under the guise of "Gary Jones" who had been receiving payments from Moore to break into email accounts, steal incriminated images and post them to the site anonymously. Both Moore and Evans now face 15 federal charges each, including conspiracy, unauthorized access to a protected computer to obtain information and aggravated identity theft (Stuart 2014; Dodero 2012). The troubling issue with these charges is that none of them involve the actual intent of the actions: to distribute pornographic images of non-consenting individuals. By our current legal standards, stealing the images and doing so for a profit are punishable but not the intent to distribute other people's intimate data.

Though the Moore case presents a clear example of where legal standards gaps exist and are exploited, it also brings to light how today's Internet and sharing culture are reshaping our identity standards. The earlier discussion presented mainly through Dr. Toogood's analysis on the dangers children face in the online environment examines these gaps. Additionally, in an *On the Media* discussion, Moore gives a sobering view of the reality of this culture and how the Internet is a ripe environment for revenge porn: "I give a stage for people to put that content on the Web. But it's 2011. I mean, people – they're putting their lives on Facebook and Twitter and – and then they expect to send these private intimate photos to random people that they're meeting online that they don't know, and they expect it to not be on the Internet?" Moore claimed not to be hurting anyone, just facilitating a space for them to hurt themselves while he makes a profit of it (Garfield 2011). Essentially, his logic is nearly correct, leaving maneuvering space for those who had no knowledge of images being taken or those who are incorrectly identified. Lawmakers, standard setters, are once again plagued with the question of how to legally help people when they are not helping themselves.

Part IV

So far, the discussion on the issue and prevention of revenge porn has circulated around the legal landscape. However, many experts on the subject of online security and privacy argue that the justice system is not the best avenue for combating the issue; the answer lies in the education system. With the combination of advancing technology and the user's increasing comfort with the technology, the user is becoming more vulnerable to potential threats they often do not know exist - the iCloud breach, for example. Instead

of relying on the law to prevent and serve justice to creators and distributors of revenge porn, educational technology experts like Tracey Choulat agree that a viable alternative is preventative educational measures. By introducing online safety practices and training in the classroom during a young person's formative years, we can create a more responsible online citizenry (Choulat 2010).

The need for educational programming in schools is seen as the first of three targets in the "3-E" solution to online privacy and safety. Privacy expert Adam Thierer recognizes the legal system's inherent inability to adapt to a standard that addresses online privacy concerns, like revenge porn, and concludes that new strategies must be devised: "This conclusion does not mean that privacy is unimportant or that society is entirely powerless to address it through legal or regulatory means. It does, however, mean that individuals who are highly sensitive about their online privacy will likely need to devise new strategies to shield it as the law will not likely play as great a role due to both normative and practical constraints" (Thierer 2013). The second and third E's of the "3-E" solution include user *empowerment* and *enforcement* of existing legal standards, but this section focuses mainly on the first E, *education.* Thierer proposes this solution as a viable new direction also because of another unclear standard for the general population: a standard definition of privacy. Online privacy and appropriate regulation is a highly disputed issue for the majority of Internet users in the United States (Thierer 2013). Therefore, educating people how they can maintain their own standard of privacy online instead of painstakingly trying to create a legal standard is the best solution for all.

While some online safety regulations exist in schools, they serve as policing mechanisms rather than educational tools. The majority of safety mechanisms in place in

most American high schools include firewalls that merely prevent potentially harmful content from view or download. Firewalls on school servers block many kinds of content from pornographic images to virus-carrying software. While these firewalls were put in place for noble reasons, they do nothing to actually educate students why they exist. Choulat argues this places a large burden on students and their parents when students return home where often these same online protections do not exist (Choulat 2010). By educating students about *why* certain sites and content are blocked, how firewall software filters for harmful material, and how students can begin to navigate the interweb responsibly, young people will have a deeper understanding of the Internet environment and the many privacy concerns and harms it harbors if used irresponsibly. But first, this kind of curricula must find its way into high school educational standards.

A recent report from the Wilson Center on the 21st century challenges for American classrooms concluded startling results in regards to STEM education. “The outdated curriculum in most schools carves out little time to teach the skills in the crucial STEM areas necessary for the most competitive 21st century jobs” (Vallas & Pankovits). While the report based much of its research on the importance of updated curricula for the future of the job market, these same results can be applied to the importance of STEM education on Internet safety. If students are not being allotted time in the classroom to learn technology and Internet basics, they will continue to utilize these fascinating tools with increased ignorance to their negative side-effects.

Admittedly, very little research is available to prove the effectiveness of online safety education, but this is often cited as part of the bigger problem. Very few extended programs on youth cyber-security exist, therefore, little evidence on these programs’ or

curricula's actual effectiveness exists. While some schools may offer one-time seminars or online training videos, these tactics have a much lesser chance of creating a lasting effect than if cyber safety was molded into the curriculum.

Recent research does show, however, that "students with greater knowledge of internet privacy and security issues were more likely to protect private information and the groups most able to impact students' online activities were parents, educators and their peers (Choulat 2013; Chai, Bagchi-Sen, Morrell, Rao & Upadhyaya 2009). Therefore, implementing new education standards for online safety into middle and high school classrooms – a time they are most impressionable and simultaneously acquiring technological skills, surrounded by educators and peers – can protect Internet users from the threat of revenge porn rather than rely on the outdated standards of the justice system.

Conclusion

Though it has taken much time and countless examples to finally bring the issue to light in the United States, revenge porn in all its forms as well as the implications of Internet safety for current and future generations are becoming priority issues for activists and policymakers alike. This paper touched on many of the standards at play in this complex network, including legal standards, identity and social standards, political standards and technological standards, but deeper understanding of each aspect is necessary to create a more legally protected environment against revenge porn. Simply put, our legal system is falling drastically behind in its effort to keep pace with technology and the globalized society. That is not to say technological advancement and network expansion are hindrances to Americans' safety, but they should not be viewed

lightly. Privacy issues like revenge porn will continue to pervade society, no doubt spawning more 21st century issues in their wake. It is up to lawmakers and activists now to recognize this, then address it with fresh eyes and innovative methods to rework the country's legal standards and framework to better protect our future generations.

References

Arthur, W. Brian. *The Nature of Technology: What It Is and How It Evolves.* New York: Free Press. August 2009. Print

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H., & Upadhyaya, S. "Internet and online information privacy: An exploratory study of preteens and early teens." 2009.

Choulat, Tracey. "Teacher Education and Internet Safety." *College of Education, University of Florida.* 29 March 2010. Available at: http://www.academia.edu/2901022/Teacher_Education_and_Internet_Safety

Citron, Danielle K., and Mary Anne Franks. "Criminalizing Revenge Porn." *Wake Forest Law Review.* Vol. 49, No. 345. 19 May 2014. Available at: http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2424&context=fac_pubs

Distribution of Intimate Images. UT – HB 71. 60th Cong. (2014). <http://le.utah.gov/~2014/bills/static/HB0071.html>

Dodero, Camille. "'Gary Jones' Wants Your Nudes." *The Village Voice.* 16 May 2012. <http://www.villagevoice.com/2012-05-16/news/hacker-is-anyone-up-hunter-moore-fbi/2/>

Ehrenfreund, Max. "The legal system hasn't adapted to what Jennifer Lawrence calls a 'sex crime.'" *The Washington Post.* 8 October 2014. <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/10/08/the-legal-system-hasnt-adapted-to-what-jennifer-lawrence-calls-a-sex-crime/>

Franks, Mary Anne. "Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators." *End Revenge Porn.* 25 July 2014. Available at: http://www.endrevengeporn.org/guide-to-legislation/

Garfield, Bob. "Revenge Porn's Latest Frontier." *On the Media.* 2 December 2011. <http://www.onthemedia.org/story/173718-revenge-porns-latest-frontier/transcript/>

Grewal, David Singh. *Network Power: The Social Dynamics of Globalization*. New Haven: Yale University Press. 1 October 2008. Print.

Kedmey, Dan. "Hackers Leak Explicit Photos of More Than 100 Celebrities." *TIME.* 1 September 2014. <http://time.com/3246562/hackers-jennifer-lawrence-cloud-data/>

Law, Victoria. "Will revenge porn laws actually stop revenge porn?" *The Daily Dot.* 22 October 2014. http://www.dailydot.com/opinion/revenge-porn-laws-jennifer-lawrence-celebgate/?tw=dd

Najdowski, Cynthia J., and Meagen M. Hildegrand. "The criminalization of 'revenge porn.'" *American Psychological Association, Judicial Notebook.* Vol. 45, No. 1. January 2014. Available at: http://www.apa.org/monitor/2014/01/jn.aspx

Nelson, Steven. "Federal 'Revenge Porn' Will Seek to Shrivel Booming Internet Fad." *US News & World Report*. 26 March 2014. <http://www.usnews.com/news/articles/2014/03/26/federal-revenge-porn-bill-will-seek-to-shrivel-booming-internet-fad>

National Conference of State Legislatures. "State 'Revenge Porn' Legislation." *National Conference of State Legislatures.* 2014. <http://www.ncsl.org/research/telecommunications-and-information-technology/state-revenge-porn-legislation.aspx>

Oren, Yaniv. "Judge dismisses case against Brooklyn man who shared nude photos of girlfriend on his Twitter account." *New York Daily News.* 19 February 2014. <http://www.nydailynews.com/new-york/brooklyn/revenge-porn-case-put-bed-article-1.1620648>

Price, Michelle L. "Lawmakers approve bills on STEM education, 'revenge porn' during final hours." *Associated Press.* 14 March 2014. <http://www.ksl.com/?sid=29056269&nid=210&s_cid=rss-extlink>

Rocha, Veronica. "'Revenge porn' law: Ex-boyfriend who posted nude photos gets jail time." *Los Angeles Times.* 1 December 2014. <http://www.latimes.com/local/lanow/la-me-ln-la-man-jail-revenge-porn-law-20141201-story.html>

Stuart, Tessa. "Hunter Moore, Revenge Porn Profiteer, Arrested by the FBI." *The Village Voice*. 23 January 2014. <http://blogs.villagevoice.com/runninscared/2014/01/hunter_moore_charles_evens.php>

Thierer, Adam D. "The Pursuit of Privacy in a World Where Information Control is Failing." *Harvard Journal of Law and Public Policy.* Vol. 36, No. 2. March 2013. Available at SSRN: http://ssrn.com/abstract=2234680

Toogood, Laura. "Of course children are revenge porn victims – they value popularity over privacy." *The Telegraph.* 1 October 2014. <http://www.telegraph.co.uk/women/womens-life/11133165/Children-are-revenge-porn-victims-because-they-value-popularity-over-privacy.html>

Vallas, Paul, and Tressa Pankovits. "Making a Success of Every School: Meeting the Challenges of the 21st Century." *The Woodrow Wilson International Center for Scholars.*

Vaughn-Nichols, Steven J. "After alleged iCloud breach, here's how to secure your personal cloud." *ZDNet.* 1 September 2014. <http://www.zdnet.com/article/after-alleged-icloud-breach-heres-how-to-secure-your-personal-cloud/>

Wadhwa, Vivek. "Laws and Ethics Can't Keep Pace with Technology." *Massachusetts Institute of Technology: Technology Review.* 15 April 2014. <http://www.technologyreview.com/view/526401/laws-and-ethics-cant-keep-pace-with-technology/>

The author also referenced her own previous works in the writing of this paper:

Doom, Jilanne. "Arthur's Modularity and Internet Privacy Laws." *CCTP 644 Global Standards*. <https://blogs.commons.georgetown.edu/cctp-644-fall2014/2014/10/29/arthurs-modularity-and-internet-privacy-laws/>

Doom, Jilanne. "Leveraging Revenging Porn." *CCTP 644 Global Standards.* <https://blogs.commons.georgetown.edu/cctp-644-fall2014/2014/10/29/leveraging-revenge-porn/>