Gendered Terrorism in the Digital Age: Global Attempts to Combat Technology Facilitated Violence Against Women

By

Emily Kathleen Norton

Submitted to
Central European University
School of Public Policy

in partial fulfilment for the degree of Master of Arts in Public Policy

Supervisor: Cameran Ashraf

Budapest, Hungary

2018

Author's Declaration

I, the undersigned Emily Kathleen Norton, hereby declare that I am the sole author of this thesis. To the best of my knowledge this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted as part of the requirements of any other academic degree or non-degree program, in English or in any other language.

This is a true copy of the thesis, including final revisions.

Date: 14 June 2018

Name: Emily Norton

Signature: _____

Abstract

The advent of the internet and the proliferation of new technologies have created exceptional opportunities for women, however, emerging technologies have also created new mediums through which women can be targeted for harassment, violence, and abuse. This thesis argues that technology facilitated violence against women (TFVAW) *is* violence, and that despite international legal obligations, the international community has not taken adequate steps to protect women in online spaces. The first chapter presents TFVAW as violence and outlines the relevant international law pertaining to the eradication of violence against women. Second, this thesis uses case study analysis to evaluate the Democratic Republic of the Congo, the Islamic Republic of Pakistan, and the Kingdom of Sweden on their legislative efforts to combat TFVAW. Finally, this thesis analyzes the efforts made in the cases selected and, using a new typology for forms of TFVAW, calls for an international declaration that violence facilitated by technology, in both its pure and hybrid forms, constitutes real and prosecutable violence.

CEU eTD Collection

Acknowledgements

I would like to express my sincere gratitude to my supervisor Cameran Ashraf for his continuous feedback and support, as well as Borsca Farago and Andrea Krizsan whose guidance and suggestions were instrumental to my final product. I would like to thank my partner, Yates Jordan, for reading countless drafts and providing moral support throughout this process.

Thank you to all of the women in my life for your constant encouragement and inspiration.

CEU eTD Collection

Table of Contents

CEU eTD Collection

List of Tables

List of Abbreviations

CEDAW - UN Committee on the Elimination of All Forms of Discrimination Against Women

DRC - Democratic Republic of the Congo

GPS - Global Positioning System

IPV - Intimate Partner Violence

NGO - non-governmental organization

TFVAW - Technology facilitated violence against women

UN - United Nations

US - United States

USD - United States Dollar

VAW - Violence against Women

Introduction

For women across the world, the last half century has been a mix of incomparable progress and frustrating stagnation. The rights of women have been recognized at unparalleled rates; ending intimate partner violence (IPV) has risen to an international priority, and rape has been recognized both as an epidemic on college campuses and a crime against humanity when used as an act of war (ICTY 2011). In spite of widespread workplace harassment and abuse, women are entering the workforce and rising to top positions in for-profit and nonprofit sectors alike. Despite these advancements, the prevalence and scope of violence against women (VAW) is staggering. UN Women estimates that 35% of women worldwide have experienced physical or sexual violence in their lifetime (UN Women 2016). While sexual harassment and gender-based violence are experienced differently depending on the national and regional context, violence against women is always a symptom of a larger system of gender inequality and coercive control.

Violence against women is not a new phenomenon. It took place for hundreds of years prior to its recognition by individual states and instruments of global governance. Despite the myriad of international legal obligations that states have to prevent, prosecute, and eliminate forms of discrimination against women, women continue to experience violence in a variety of distinct ways. New and emerging technologies have exacerbated some of these harms, providing new mediums through which women can be targeted for harassment, violence, and abuse. Technology facilitated violence against women (TFVAW) refers to an assortment of behaviors and actions where digital technologies are used to facilitate virtual or in-person harms and inflicts very tangible psychological, economic, and physical consequences that prevent women from engaging as equal members of society (Henry and Powell 2016, 195). Violence facilitated by technology is not a separate form of inequality, but is rather an extension of a centuries-old tradition of (mainly) men using fear and violence to control women.

This thesis argues that TFVAW *is* violence against women, and that despite existing international legal obligations, states have not taken adequate steps to protect women in online spaces. The first chapter will provide a conceptual background and literature review explaining the roots of violence against women, existing international legal obligations, and the role technology plays in perpetuating VAW. The conceptual background develops the backbone for this thesis, arguing that technology facilitated violence against women *is* violence. The second chapter presents the case study analysis methodology and addresses the various limitations of this method. The third chapter evaluates existing legislative efforts taken to combat TFVAW in the Democratic Republic of the Congo, the Islamic Republic of Pakistan, and the Kingdom of Sweden. The fourth and final chapter analyzes the common trends identified in the cases selected and develops a new typology for legislating against TFVAW. This typology makes a clear distinction between hybrid and pure forms of TFVAW and will benefit policy-makers as they attempt to create truly comprehensive legislation to combat TFVAW. This thesis concludes by calling for an international declaration that violence facilitated by technology, in both its pure and hybrid forms, constitutes real and prosecutable violence.

CEU eTD Collection

Chapter 1: Literature Review and Conceptual Background

The literature review and conceptual background of this thesis work to build a bridge between two concepts. The first two sections provide insights into the roots of violence against women (VAW) and outline existing international law that compels states to act to eradicate VAW in all its forms. The final section argues that violence facilitated by technology is no less violent than if the abuse had taken place entirely in an offline environment. Perpetrators of TFVAW are not performing an alternate identity in cyberspace when they harass, stalk or threaten women, but rather use their own thoughts, beliefs, and feelings to carry out targeted attacks. This chapter concludes that given that TFVAW *is* violence, states have an international legal obligation to take positive measures to eliminate it.

1.1 Violence Against Women: Identifying its Roots

Violence against women encompasses a number of distinct acts from harassment, rape and intimate partner violence, to honor killings and feminicides. What all of these acts have in common, however, is that they are the result of societally reinforced gender norms that undergird a system of gender inequality. Feminist scholars, Dobash and Dobash, argue that VAW is both a symptom of gender inequality and a tool for female subordination (Dobash and Dobash 1992, 2). Gender norms are historically rooted in the concept of the public-private divide. As noted by Elizabeth Schneider in her 1994 article "The Violence of Privacy", the female identity revolves around her role in the "private" or domestic sphere, whereas the male identity is created through his actions in the "public" domain (Schneider 1994, 36). These separate spheres have been instrumental to the construction of gender norms and were used for generations to provide justification for the absence of state intervention in family disputes (Schneider 1994, 36). Legal systems, particularly in the United States and Europe, avoided intervention in family affairs, claiming their lack of jurisdiction over "private" matters. Supported

by government indifference, the use of violence by men in intimate partner relationships was a perfectly acceptable performance of one's role as head of the household.

The long established gender hierarchy relegated women to the private sphere, allowing the State to ignore, and thereby implicitly condone, the use of violence by men in intimate partner relationships (Bustelo et al. 2007, 144). In open defiance of the familial black box, however, the State maintained its authority to legislate and intervene in other elements of familial life, namely with regard to family planning and abortions (Schneider 1994, 38). The selective use of the "private" sphere restriction by the State was, in practice, a convenient tool for maintaining female subordination in society.

Violence against women is universal; it is not bound to one nationality, class, education, or race (Engle 2009, 1). Gendered violence creates a common social dependency that can be seen both within a family unit and as a part of the broader societal landscape (Engle 2009, 1). While global prevalence of violence against women is alarmingly high, there is no doubt that certain population's experience violence at sharply different rates and in starkly different fashions. Even within the same national context women with intersecting identities, e.g. women of color, LGBTQI+[1] women, and women with disabilities, experience violence differently (Crenshaw 1989, 152). The concept of intersectionality, coined by Kimberle Crenshaw in 1991, asserts that women with intersecting identities experience discrimination in a manner that is synergistic rather than additive. This means that one does not experience sexism and racism separately, but rather the combination of these two identities creates a distinct and amplified form of discrimination (Crenshaw 1989, 152).

A growing body of feminist literature, championed by Michael P. Johnson, posits that there are four main forms of IPV, intimate terrorism, violent resistance, situational couple violence, and mutual violent control (Johnson 2008, 25). The most severe form of IPV, as described by Johnson, is intimate terrorism. The majority of women who are forced to leave

[1]LGBTQI+ - Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, other identities and orientations

CEU eTD Collection

their homes and seek refuge in shelters fall within this category (Johnson 2008, 6). Intimate terrorism is embedded in a larger concept of coercive control, which utilizes fear and violence, among other tactics, to maintain tight control over women's lives (Leone, Johnson, and Cohan 2007, 427).

Intimate terrorism, while perhaps rooted in patriarchal views of gender norms and societal acceptance of violence against women, puts control and fear at the center of the interpersonal dynamic. While the term intimate terrorism tends to be used within the context of an intimate partnership, the concept of coercive control can be extrapolated outward to apply to societal patterns of violence against women. Using this framework, violence against women is not the result of a specific violation of traditional gender roles, but is rather men's use of threats and violence as a way to maintain control over women more generally (Johnson 2008, 26). Male supremacists, a category of men that is heavily represented on digital platforms, cling to tactics of coercive control in an attempt to push women out of areas of public discourse (Chokshi 2018).

1.2 Combating Violence against Women: International Law and State obligations

It took women's rights activists from all over the world decades to convince institutions of global governance that violence against women is a human rights issue rather than a private family matter. In 1992, the *United Nations Committee on the Elimination of All Forms of Discrimination Against Women* (CEDAW) affirmed in General Recommendation 19 that violence against women is a form of discrimination (CEDAW 1992). Recommendation 19 defines gender-based violence as "violence that is directed against a woman because she is a woman or that affects women disproportionately" and notes that this violence "seriously inhibits women's ability to enjoy rights and freedoms on a basis of equality with men" (CEDAW 1992).

One year later, in 1993, the *UN Declaration on the Elimination of Violence Against Women* declared that "violence against women constitutes a violation of the rights and fundamental freedoms of women", and acknowledges the root of this violence as "a manifestation of

CEU eTD Collection

historically unequal power relations between men and women" (UNGA 1993). The Declaration further calls on states to eliminate violence against women in all its forms (UNGA 1993). Later that same year the *Vienna Declaration and Programme of Action* adopted by the World Conference on Human Rights recognized the eradication of both private and public forms of violence against women as a human rights obligation (World Conference on Human Rights 1993). In 1994, the Commission on Human Rights appointed a Special Rapporteur on Violence Against Women, its Causes and Consequences, and in 1995 the UN Conference on Women, hosted in Beijing, promoted violence against women as a critical area of concern (OHCHR 2014).

A principle of positive state obligations to prevent, prosecute, and punish violence against women had been established by 1995, and various regional and international bodies took this obligation seriously. Despite international legal obligations binding many states, ensuring compliance became a prominent issue. Feminist scholars continue to highlight the perpetuation of violence against women in weak states where the government is unable or unwilling to protect women within its borders (Bustelo et al. 2007, 145).

This "Failing State" frame was underlined in a 2001 decision by the Inter-American Commission on Human Rights in the case of *Maria da Penha v. Brazil (Maria da Penha v. Brazil 2001)*. The Commission found that "the failure [of Brazil] to prosecute and convict the perpetrator of [intimate partner violence]...is an indication that the State condones the violence" (Maria da Penha v. Brazil 2001). This case was a turning point for state responsibility; culpability for violence against women was no longer isolated to individual perpetrators. States that knowingly allow violent acts to occur, or fail to combat conditions that perpetuate such violence, will be held accountable. In furtherance of this obligation, in 2017 the CEDAW Committee published General Recommendation 35, asserting that "the prohibition of gender-based violence against women has evolved into a principle of customary international law", and is legally binding for all states regardless of their ratification of international treaties (CEDAW 2017).

CEU eTD Collection

1.3 Technology Facilitated Violence: the Dissolution of a Feminist Internet

The 1990s brought forth a wave of techno-utopian thinkers who coined themselves cyberfeminists (Evans 2014). Cyberfeminists saw emerging technologies, namely the internet, as opportunities to break down barriers and create a digital realm void of inequality. These women were fully aware that the culture emanating from digital spaces would likely reflect the same gendered power dynamics as the offline world, but they hoped the internet could be a new tool to challenge inequality and a place for global female collaboration (Evans 2014). The modern day internet is a miraculous space for people of all genders, sexualities, races, and religions to communicate, voice their opinions, network and make money, however it is far from the inclusive utopia of which the cyberfeminists dreamed. Much to the chagrin of the techno-utopian movement, the internet has evolved into a medium that perpetuates existing sexism and often amplifies it under the guise of anonymous free speech (Filipovic 2007, 297).

A new form of violence against women, one that is again deeply entrenched in traditional gender roles and elements of coercive control, has blossomed and flourished in online spaces where perpetrators can hide behind masks of anonymity. Technology facilitated violence against women is an umbrella description for many of the different forms of abuse women experience while interacting with emerging technologies. Cyberviolence manifests itself in many ways; common forms include hacking, impersonation, stalking and surveillance, harassment, recruitment of women and girls for exploitation, as well as malicious distribution of images and videos without the consent of one or more of the parties involved (Henry and Powell 2016, 196). Women are specifically targeted for these forms of violence because they are women, and they face serious economic, psychological, and physical consequences as a result (Deibert et al. 2017, 2).

As is true with many forms of sexual violence and harassment offline, women face technology facilitated violence at disproportionate rates to men. United States volunteer organization Working to Halt Online Abuse found that roughly three quarters of U.S. victims of

cyberstalking and harassment are women (Hess 2014). The Guardian conducted an analysis in 2016 that reviewed 70 million of the comments posted on its articles and message boards, isolating the ones that were blocked or removed for being "abusive or disruptive" (Jane 2017, 46). Of the authors who received the most threats and abusive remarks, 80% were women (Jane 2017, 47). In 2017, Amnesty International conducted a survey of women in eight countries: the United States of America, the United Kingdom, Spain, New Zealand, Italy, Poland, Sweden and Denmark (Amnesty International 2017). The report found that not only are women targeted more often than men for online abuse, women who have experienced technology facilitated violence make up one fourth of all women on the internet (Amnesty International 2017).

Women who are targeted by technology facilitated violence are often perceived as experiencing a mere inconvenience, or a form of abuse that is somehow less real than offline violence. Markos Moulitsas, the owner of progressive blog Daily Kos argued in 2007 that women who complain about TFVAW are overreacting, that "if [women] can't handle a little heat in their email inbox, then really, they should try another line of work" (Filipovic 2007, 301). In the same vein, there are constant efforts made to undermine women who speak out against TFVAW. Examples of these kinds of remarks include "women who put their pictures online cannot complain when they are harassed", "women should be grateful for the positive attention", "women who speak out just want attention", and "the women who object to having their privacy violated are trying to shut down First Amendment Rights" (Filipovic 2007, 297). Women who report threats to police are frequently met with "boys will be boys", "It's no big deal. It's just online talk. Nobody's coming to get you", or the all too common "go home [and] turn off your computer" (Citron 2014, 88) Women who experience TFVAW are certainly not overreacting, and they are definitely not asking for it.

While it is true that men are also victims of online abuse, the attacks directed at men tend to be specifically related to their behavior, political views, or beliefs. Women, however, are constantly the focus of comments of a sexual or violent nature. Journalist Amanda Hess

documented examples of the kind of hate speech that is directed towards women online: "Happy to say we live in the same state. I'm looking you up, and when I find you, im going to rape you and remove your head", "i hope someone slits your throat and cums down your gob", "I just want to rape her with a traffic cone", all of which are representative of similar remarks directed at women on a daily basis (Hess 2014). This constant barrage of disgusting and aggressive language not only has the potential to frighten women, but also to undermine their feeling of belonging in areas of public discourse. Feminist author, Jill Filipovic concludes in her article "Blogging While Female: How Internet Misogyny Parallels 'Real-World' Harassment" that online harassment is intended to remind women that despite their accomplishments or qualifications their "primary purpose is decorative" (Filipovic 2007, 303). Not only are women not worth listening to, but women who engage in online spaces will be punished (Filipovic 2007, 303).

Technology facilitated violence against women can have extreme psychological consequences for victims of abuse. The same Amnesty International survey that determined one out of every four women online experiences cyberviolence, noted that 66% of women polled stated feeling apprehension when thinking about using the internet as a result of online harassment (Amnesty International 2017). Of those who had experienced abuse, 32% reported that they changed the way they express themselves online because of cyberviolence (Amnesty International 2017). Feminist scholar, Emma A. Jane, corroborates this finding in her article "Feminist flight and fight responses to gendered cyberhate", where she notes that restricting internet use and one's engagement with technology is a common response by women who experience cyberviolence (Jane 2017, 50). While not every woman responds to cyberattacks by altering their online expression, one thing is clear: technology facilitated violence is having a silencing effect on women in aggregate.

In addition to the above-mentioned psychological effects, TFVAW can result in serious economic consequences for women as well (Hess 2014; Filipovic 2007; Jane 2017; Citron 2014). Direct costs to women include job loss and irreversible damage to one's professional reputation.

Danielle Citron documents in her book *Hate Crimes in Cyberspace* stories of women who suffer periods of unemployment after particularly bad instances of cyber-harassment and cyberstalking (Citron 2014, 3). One woman was targeted by anonymous internet trolls who posted false accusations about past sexual misconduct, irresponsible financial management, and violent tendencies (Citron 2014, 3). Still others had their phone numbers and home addresses leaked online alongside fake advertisements for sexual acts, or disparaging emails sent to their employers (Citron 2014, 3). Legal fees to prosecute perpetrators and counseling fees to address the psychological effects of abuse can add up to thousands of dollars.

Women also face considerable opportunity costs because of online abuse. Lower productivity as a result of wading through abusive emails and comments, as well as a loss of billable hours spent communicating with police, lawyers, or mental health professionals. Finally, and perhaps the least discussed consequence is the missing market of women, who, due to fear, exhaustion or spent emotional capital, refuse to engage with the internet as a form of professional or personal development (Jane 2017, 50).

The physical side effects of TFVAW are the most frequently discussed. Cyberviolence is not isolated to the digital realm, it often takes a hybrid form and manifests into physical presentations of violence. Whether this is an online threat of death or sexual assault that is actualized, or the use of a global positioning system (GPS) tracker to stalk an ex-partner, women who engage with emerging technologies are at risk of far more than a nastily worded email. Given that many threats of sexual and physical violence are made from anonymous users, it is almost impossible to know if the post is coming from across the world, down the street, or the man sitting in the neighboring cubicle.

In 2012, Michael A. Johnson created numerous fake online profiles and ads impersonating his ex-wife. One ad, titled "Rape Me and My Daughters" posted alongside his ex-wife's address, combined with other ads soliciting sex, caused 50 strangers to show up at her home (Jane 2017, 47). One man tried to break in, and another attempted to undress her

daughter. Johnson was convicted of stalking, and sent to prison, however these types of incidents represent the terrifying hybrid threat that digital technologies pose to women. Emerging technologies also pose a threat from women already experiencing intimate partner violence or intimate terrorism more specifically. The rise of new mobile applications that track a user's location or replicate one's screen on another device provide ample opportunities for men to maintain coercive control over the lives of their partners.

Table 1 below discusses six forms of technology facilitated violence against women and gives examples of ways in which they are experienced. This list was formed and adapted in part from existing empirical research (Henry and Powell 2016) to create an extensive categorical understanding of technology facilitated VAW. Given the extraordinarily diverse manner in which women experience abuse through emerging technologies, Table 1 is unlikely to be exhaustive. What is certain, however, is that all the acts listed below are forms of violence.

Table 1: Forms of Technology Facilitated Violence Against Women[2]

Category	Definition	Examples
Technology facilitated harassment	Unwelcome verbal and visual comments and remarks that insult, degrade, harm or distress the recipient. Technology facilitated harassment takes place via a number of mediums: chat rooms, forums, through email or social media, messaging applications etc.	Hate speech, unwanted sexual attention/comments/remarks, online sexual coercion, virtual rape, online sexual solicitation, false accusations, reputation harming lies/comments
Technology facilitated stalking and surveillance	The use of technology to monitor or surveil a person without their consent or to facilitate behaviors that are unwanted, repetitive, intrusive, threatening, and harassing. These actions cause fear for one's safety or of bodily harm and can be perpetrated by a lone individual or a mob.	Surveillance, tracking, threats of: sexual violence, assault, or murder.
Image based sexual exploitation	The sharing of sexually explicit images or videos without the consent of the individuals represented within. Additionally, the sending of sexually explicit images without the consent of the individual receiving the image.	Revenge porn, non-consensual sexting
Technology facilitated physical offenses	The use of technology to lure individuals into violent situations, or to identify their location for the same ends.	Assault, rape, recruitment/trafficking, murder/honor crimes
Technology facilitated identity exploitation	The use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring, altering, or modifying personal information; to assume the identity of an individual; or to release personal information about an individual without their consent.	Hacking, doxxing, impersonation, social engineering
Intragroup hate speech and incitement	Online groups that perpetuate harmful gender expectations and encourage the use of violence against women (online and offline).	Incels, male supremacy groups

CEU eTD Collection

[2] Note: Concepts in Table 1 were adapted from Nicola Henry and Anastasia Powell's 2016 article "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research" (Henry and Powell 2016)

Violence against women is an old phenomenon that has been used for centuries to control women through fear and violence. This intimate terrorism spreads beyond intimate partner relationships and represents a broader challenge to women's engagement as equal members of society. With the advent of the internet and emerging technologies, men from all over the world can use fear and threats of violence as a mechanism to coerce and control women in an attempt to force them out of spaces of public discourse. Forms of technology facilitated violence disproportionately harm women, are directed at women *because* they are women, and have real psychological, economic, and physical consequences. Given that TFVAW clearly fits within the parameters of violence against women as described by CEDAW in 1992, the eradication of this violence is a human rights obligation assigned to states, with roots in international law. After explaining the selected methodology, the remainder of this thesis is devoted to evaluating three case studies, the Democratic Republic of the Congo, the Islamic Republic of Pakistan, and the Kingdom of Sweden, to identify the barriers to eliminating TFVAW globally.

CEU eTD Collection

Chapter 2: Methodology and Limitations

This thesis utilizes three case studies to provide a global perspective on the range of legislative efforts states have taken to prevent and prosecute technology facilitated violence against women. The aim of this case study analysis is to answer the research question: why are states failing to uphold their international legal obligations to combat TFVAW? The three case studies were selected due to their diverse nature: the Democratic Republic of the Congo (DRC), the Islamic Republic of Pakistan, and the Kingdom of Sweden. Case studies, rather than surveys or interviews, were chosen to fill an existing gap in research. Various international organizations and research institutions have published research regarding the various types of TFVAW, including the European Union (European Institute for Gender Equality 2017b), Amnesty International (Amnesty International 2017), and Citizen Lab (Deibert et al. 2017). Furthermore, journalists and advocacy organizations alike have reported extensively on individual stories of online harassment, stalking and hate speech (Nagarajan 2016; Amnesty International 2017; Hess 2014; Filipovic 2007; Citron 2014; Jane 2017).

In addition to studying the types and forms of abuse, some small-scale attempts have been made to establish the prevalence of various forms of online abuse by conducting surveys in selected countries (Amnesty International 2017; European Institute for Gender Equality 2017b; Digital Rights Foundation 2017a). While the aforementioned studies are crucial to increasing global understanding of the magnitude of the problem of technology facilitated violence, more data is desperately needed. Unfortunately, a global survey, or even single country survey that holds up to scientific standards is beyond the scope of this thesis. This thesis, therefore, while acknowledging existing contributions to the field, seeks to evaluate the actions taken by states to combat TFVAW and explain some key barriers to upholding their international legal obligations. Reporting the existence of the problem is of paramount importance, however evaluating global efforts is crucial to identifying next steps in policy response and understanding existing gaps in

CEU eTD Collection

legislation.

By employing a diverse case-selection strategy, this thesis seeks to provide a representative analysis of global efforts to combat technology facilitated violence against women (Gerring 2008, 650). In pursuance of a diverse and representative analysis, this thesis selected two extreme values that represent the high and low levels of legislative efforts to combat TFVAW, as well as one mid-level value, that represents a breakpoint along the continuum (Gerring 2008, 651). While this thesis seeks to collect data on a diverse range of case studies, the wide array of input factors limits this analysis from attempting to develop a universal causal claim. Instead, this thesis aims to establish a robust overview of the threats facing women online and to evaluate the larger global effort to uphold international law and to protect women using emerging technologies. The cases will be evaluated based on the prevalence, relevance, and effectiveness of legislative efforts to combat TFVAW where they exist.

The limitations of the diverse case approach are rooted in the general lack of comprehensive global data on rates of TFVAW. As such, it is impossible to accurately select cases that are perfectly dispersed along the continuum of either prevalence of online violence or the success of legislative efforts. The cases selected for in-depth analysis were done with the goal of representing the full variation of global country contexts and achieving a minimal level of representativeness. However, due to the lack of global data the three selected cases may not perfectly reflect the exact distribution present in the wider population (Gerring 2008, 647).

A final limitation of the case study methodology is the lack of data and general information relating to technology facilitated violence against women in the Democratic Republic of the Congo specifically. While compiling research for the DRC proved to be quite challenging, the lack of information serves to underline the importance of including the DRC in this thesis. The DRC, a country with considerable gender equality and abuse problems, has taken no steps towards documenting or eliminating TFVAW. This case study represents numerous other countries around the world, where the problem of TFVAW, though prominent, is poorly

CEU eTD Collection

documented and not treated as a priority.

CEU eTD Collection

Chapter 3: Case Studies

The three countries selected for evaluation were chosen using diverse case-selection strategy (Gerring 2008, 650). As part of the analysis, each case will be reviewed concerning the prevalence of TFVAW, the relevance of the existing legislative efforts to combat TFVAW, and the effectiveness of those efforts where they exist. The cases were not selected irrespective of their relationship with offline violence against women, but rather due to their location on a spectrum of diverse attempts made to combat TFVAW, which incorporates offline efforts. The range starts with the Democratic Republic of the Congo, which has passed no legislation pertaining to TFVAW, to the Islamic Republic of Pakistan, which has numerous laws with inconsistent implementation (Bytes for All 2014, 5), and finally to the Kingdom of Sweden, which uses existing laws to varying degrees of success (NCCP 2015, 16). Upon completion of the evaluation, the Analysis portion of this thesis will discuss common challenges and what the shortcomings mean for the larger global system to combat TFVAW.

3.1 The Democratic Republic of the Congo

3.1.1 Prevalence of TFVAW

It is impossible to evaluate the Democratic Republic of the Congo (DRC) regarding technology facilitated violence against women without first addressing the egregious level of violence against women offline that takes place within the country. The DRC has repeatedly found itself ranked among the world's most dangerous countries in which to be a woman, due in no small part to the ongoing intrastate conflict that has been marred by exorbitant rates of sexual and gender based violence (United Kingdom Home Office 2017, 15). A study conducted in 2011 by *the American Journal of Public Health* found that over a twelve-month period in the DRC, 48 women were raped every hour (Peterman, Palermo, and Bredenkamp 2011, 1064).

To date, there is no nation-wide data on the prevalence of technology facilitated violence against women in the DRC, however interviews conducted by NGO, Take Back the Tech, show

CEU eTD Collection

that problems with digital surveillance and malicious distribution of images and videos are becoming more prominent (APC 2016, 5). Take Back the Tech interviewed 40 victims of TFVAW and noted several key themes regarding the violence they reported. Of the anecdotal evidence collected, Take Back the Tech found that 25% of women indicated that their partners monitor mobile text messages and incoming calls on their devices (Fascendini and Fialova 2011, 23). Due to the greater access to technology experienced by men in the DRC, male partners often open SIM cards or email addresses on behalf of their spouse or partner. In several instances of intimate partner violence, men repeatedly assaulted, and in one case killed, their female partners after reading messages or viewing call logs on their devices (Fascendini and Fialova 2011, 23).

A second trend in the TFVAW observed by Take Back the Tech was the use of email account control in intimate partner violence, which was present in some form in 15% of the cases documented (Fascendini and Fialova 2011, 23). In these cases, men maintained the password details for their partners' accounts without their knowledge or consent and monitored their activity (Fascendini and Fialova 2011, 23). A third form of violence observed was image-based exploitation, including the distribution of both nude images, and videos of a sexual nature, without the consent of their partners. This accounted for 17.5% of the TFVAW documented by Take Back the Tech (Fascendini and Fialova 2011, 25). Finally, some women, particularly those who were more politically engaged, also faced harassment over blogs and message forums. The blog on which most women reported receiving hate speech was hosted in France, outside the jurisdiction of Congolese law enforcement (Nyst 2014, 5). These global cases of online harassment illustrate the challenges of tackling issues on the internet.

The 40 women interviewed by Take Back the Tech were victims of an array of violent acts facilitated by technology. Some instances resulted in severe physical abuse, while others suffered psychological and economic harms from violations to their freedom and dignity. A number of women reported a mixture of the three. All of these women, however, struggled to

CEU eTD Collection

find legal recourse, due to the lack of recognition of TFVAW as violence and the preferential treatment awarded to men in marital relationships. These concerns will be discussed in the following subsections of this case study.

While Take Back the Tech provided a thorough introduction to TFVAW in the Democratic Republic of the Congo, there was a general lack of empirical evidence for this case study. The dearth of empirical data on TFVAW in the DRC is particularly telling of the attitude towards TFVAW within the country. The alarming level of VAW in the DRC, combined with the personal stories compiled by Take Back the Tech, seem to indicate that technology does indeed facilitate violence against women in the DRC. Unfortunately, however, the government has yet to acknowledge TFVAW as a significant problem worthy of legislative action. The DRC is not alone in its lack of data regarding TFVAW. This case study aptly represents a number of similar contexts globally, where women clearly experience TFVAW, but do not receive protection from any formal legal institutions.

3.1.2 Relevance of Existing Laws

There are no distinct laws in the DRC that provide women with protection from technology facilitated violence, in fact the number of laws directed towards eliminating gender-based violence in general are few and far between. The 2006 Constitution declares in Article 14 that "The public authorities shall ensure the elimination of all forms of discrimination against women and guarantee the protection of women's rights" and in Article 15 that "sexual violence committed against any person in order to destabilize or to break up a family or to bring about the disappearance of an entire people shall constitute a crime against humanity and be punishable under the law" (Art. 14&15 *Const.*DRC).

In addition to its constitutional provisions, the DRC amended its Penal Code (No. 06/018) and Penal Procedure Code (No. 06/019) in 2006, both of which criminalize and provide prosecutorial procedure for various forms of sexual violence, including rape, sexual slavery, sexual harassment, forced pregnancy, forced marriage, sexual mutilation, the deliberate

CEU eTD Collection

transmission of sexually transmitted diseases among other acts (United Kingdom Home Office 2017, 12; *DRC Penal Code* 2006, §06/018, §06/019). However, the DRC does not have any legislation that specifically recognizes intimate partner violence, or provides any legal recourse for such acts should they occur (United Kingdom Home Office 2017, 7). Furthermore, the DRC Family Code also recognizes men as the head of the household, requiring women to obey them, making prosecuting intimate partner abuse, technology facilitated or otherwise, exceedingly difficult (*Family Code* 1987, §444).

3.1.3 Effectiveness of the Existing Legal Framework

The existing laws that were written to combat violence against women in the DRC have not proven to be particularly effective, and they have been exceedingly poor at eliminating technology facilitated abuse. Given that the laws against gendered violence do not take emerging technologies into consideration, women who are abused in this manner are facing an uphill battle if they attempt to prosecute their abuser, particularly if the identity of the perpetrator is unknown, or if the perpetrator does not live in the same region as the victim. If the DRC had a growing societal acceptance or existing legal precedent for using laws pertaining to offline harassment and assault in the context of technology-facilitated abuse, the lack of specific laws may be less problematic. However, given the legally reinforced gender hierarchy, prosecuting TFVAW is fraught with challenges.

While bringing a criminal case against a digital abuser in the DRC is exceedingly difficult, there are options for women to pursue civil claims against perpetrators of TFVAW in an attempt to gain financial compensation for the harms inflicted. The DRC Penal Code has a statute that states, "Any person who causes harm to another is obligated to provide reparation for the act" (APC 2016, 6). Unfortunately, the onus for proving "harm" falls on the victim. In order to provide a solid argument that the consequences of online abuse are tangible and concrete, victims must frequently pay an attorney to argue their case before the judge, a step that requires significant capital. The average annual income for an individual in the DRC is 400 USD,

CEU eTD Collection

however a study conducted by Congolese NGO Si Jeunesse Savait, indicates that the cost of undertaking a criminal proceeding is around 1920 USD (APC 2016, 7). This is a serious impediment for pressing charges in any circumstance; however, women have a distinctly difficult time prosecuting men in a legal context where men are given preferential treatment.

3.2 The Islamic Republic of Pakistan

3.2.1 Prevalence of TFVAW

Violence against women in Pakistan is a chronic societal problem that seeps into all social spheres. Rooted in deeply entrenched societal gender norms, women in Pakistan experience intimate partner violence, sexual abuse, harassment, acid attacks, forced marriages and honor killings, among other forms of violence, at extremely high rates (United Kingdom Home Office 2016, 5). While underreporting remains a significant challenge to accurate analysis, over 10,000 cases of violence against women were reported in 2014 (United Kingdom Home Office 2016, 6). Over the course of 2014, four women were raped per day, 1,000 honor killings took place, and 232 incidents of acid attacks against women were reported (United Kingdom Home Office 2016, 6). Additional reports indicate that 85% of women experience intimate partner violence including physical, sexual, or psychological violence (United Kingdom Home Office 2016, 23).

According to the harassment helpline operated by the Digital Rights Foundation, a Pakistani NGO that engages with human rights and digital governance, cyber-harassment in Pakistan is overwhelming experienced by women (Digital Rights Foundation 2017b, 3). A 2017 report, "Measuring Pakistani Women's Experiences of Online Violence", found that 40% of female participants acknowledged having been stalked or harassed using messaging apps (Digital Rights Foundation 2017a, 36). Existing estimates on the prevalence of TFVAW are instrumental to understanding the magnitude of the problem in Pakistan; however, more data is needed to put

CEU eTD Collection

together a full picture. Much of what is known about technology facilitated violence in the country has been gathered from individual case studies.

In the past decade there have been several high profile cases of honor killings in Pakistan. These murders were perpetrated as a direct result of women's online presence or engagement with emerging technologies. In the 2010 Kohistan case, a video clip of four young Pakistani women laughing and dancing in the presence of three men was shared online, resulting in the honor killing of all four women. The community elders claimed that the women had brought dishonor to their families (Digital Rights Foundation 2017a, 5). In 2015, Pakistani activist Sabeen Mahmud took to the internet to promote emerging technologies as tools for mobilization against gender based violence. Mahmud received repeated threats of sexual assault and death as a result of her continued activism. In April 2015 she was fatally shot while driving home from a conference (de Pencier 2017). In 2016, social-media star, Qandeel Baloch was murdered by her brother Waseem Azeem. In a statement justifying his actions he explained that by Baloch was "bringing dishonor to the family" with her actions online (Khan 2016).

These instances of technology facilitated honor killings are very powerful declarations that women are not allowed to participate in online discourse in Pakistan. In both cases, the internet served a dual function, as both the location of the women's public engagement, as well as a platform for the incitement of violence. While the victims in these cases were not killed by mobs, numerous threats and statements were made encouraging the initiation of violent acts against them prior to their deaths.

3.2.2 Relevance of Existing Laws

Pakistan, unlike the Democratic Republic of the Congo, has numerous laws that overlap and engage with the concept of technology facilitated violence against women. The existing laws have taken aim at cyberviolence from different angles, some of which target electronic crimes directly, while others aim to absorb online acts into offline laws. Both forms have had varying degrees of success. The most powerful law on the books in Pakistan is the *Prevention of Electronic*

CEU eTD Collection

Crimes Act (PECA) of 2016, however its predecessors made attempts to provide recourse to general forms of cyberviolence as well (*The Prevention of Electronic Crimes Act* 2016).

Prior to PECA, a number of older laws were applied to combat forms of cyber-harassment in Pakistan. Sections 509 and 499 of the *Pakistan Penal Code* address harassment and defamation respectively, and were written in a sufficiently broad manner to be applied to actions that take place online (Digital Rights Foundation 2017b, 6; *Pakistan Penal Code* 1860, §499, §509). Even further back in Pakistan's legislative history is the 1885 *Telegraph Act* which monitors harassment communicated by any "apparatus, equipment or plant used for transmitting, emitting, making or receiving signs, signals writing, speech, sound or intelligence of any nature", mandating a sentence of imprisonment up to three years or an equal fine (Bytes for All 2013, 3; *The Telegraph Act* 1885, §3.1). While the *Telegraph Act* may claim to cover some aspects of electronic communication, it is severely outdated and has not been adapted to fit the nuanced nature of cyberviolence.

For cases of technology facilitated violence that took place prior to 2016, Pakistani citizens can make use of the 2002 *Electronic Transactions Ordinance* (ETO) which promulgated the crimes of "violation of privacy of information" and "damage to information system[s]" (Bytes for All 2013, 5; *Electronic Transactions Ordinance* 2002, §36, §37). Under the ETO individuals can be sentenced to a term of up to seven years or a fine not exceeding one million rupees (roughly 8,500 USD) , or both (*Electronic Transactions Ordinance* 2002, §37.3). The ETO was originally written to facilitate electronic transactions and generally bolster Pakistan's e-commerce, however its 2007 counterpart the *Electronic Crimes Ordinance* further outlined crimes such as illegal data access, data damage, electronic fraud and forgery, spamming, spoofing, cyberstalking and cyber-terrorism, among others (*Electronic Crimes Ordinance* 2007). Criticized as a tool to stamp out political opposition, the *Electronic Crimes Ordinance* lapsed in 2009; under the ordinance perpetrators could be punished with a sentence ranging from two years in prison to death (Bytes for All 2014, 4).

CEU eTD Collection

In an effort to tackle forms of offline violence against women, the Pakistani province of Punjab passed the 2016 *Punjab Protection of Women against Violence Act*, which includes "cybercrime[s]" in its definition of violence, along with intimate partner violence, sexual violence, psychological abuse, economic abuse, and stalking (*The Punjab Protection of Women Against Violence Act* 2016, §2(r)(1)). While including cybercrime as a form of violence signals a promising shift in how violence is perceived in Pakistan, excluding both the gendered nature of such forms of violence, as well as the numerous distinct acts that could potentially fall within the umbrella category of "cybercrime", diminishes the overall effectiveness of the Act (Digital Rights Foundation 2017b, 6).

All of these laws considered however, the 2016 *Prevention of Electronic Crimes Act* is the most adept at addressing TFVAW, however it has been widely criticized by members of Pakistani civil society as an attempt to silence opposition voices (Digital Rights Foundation 2017b, 7). Despite the warranted criticism of the Act, PECA includes several relevant sections that protect women online. Section 20 includes elements that address forms of online harassment including acts that negatively affect the reputation of an individual (Digital Rights Foundation 2017b, 8; *The Prevention of Electronic Crimes Act* 2016, §20). Section 21 prohibits the malicious distribution of sexually explicit images or video without the consent of the parties involved (Digital Rights Foundation 2017b, 8; *The Prevention of Electronic Crimes Act* 2016, §21). Section 24 addresses cyberstalking, however with legally ambiguous wording that would make it challenging to use to prosecute a perpetrator (*The Prevention of Electronic Crimes Act* 2016, §24). For example in order to be officially considered "stalking" victims must make a "clear indication of disinterest" to their stalker (Digital Rights Foundation 2017b, 9).

CEU eTD Collection

3.2.3 Effectiveness of the Existing Legal Framework

While there is no comprehensive data on the rates of prosecution for perpetrators of technology facilitated violence against women in Pakistan, a number of individual case studies have been completed that provide insight into the legal process. Pakistani NGO, Bytes for All,

interviewed women who reported experiences of technology facilitated violence to law enforcement (Bytes for All 2014, 5). Of the women who did report, all of them documented hybrid forms of violence, or violence that was both digital and physical in nature.

Pakistan has an impressive number of legal mechanisms that could provide these women with recourse for cyberviolence; however, these laws are far from accessible to the average woman. Bytes for All found that of the women who reported technology facilitated violence, many struggled to get law enforcement to recognize or acknowledge the full depth of the crimes committed, particularly those of a digital nature. While police were willing to document crimes of rape, assault, or abuse, they were reluctant to charge men with crimes such as "violation of privacy, dissemination of obscene and injurious material, blackmail and attempted extortion, and damage and harm to the survivor's reputation" (Bytes for All 2013, 5). Although many of the women attempted to communicate such charges to law enforcement, these crimes did not make their way into the final police reports on which legal proceedings are initiated (Bytes for All 2013, 5).

While some of the women found the police officers were aware of the legal provisions, still others found police in more rural locations had no knowledge of the legislation that created some of the crimes perpetrated against them (Bytes for All 2014, 6). Furthermore, police who do file reports on behalf of women often find themselves heavily pressured by people within the community to lessen or drop the charges (Bytes for All 2013, 6).

Beyond the local difficulties, women have also reported challenges due to the anonymity of users online. Even if a police officer was willing to bring charges against an individual for cyberviolence, identifying that individual is impossible without adequate resources or technical prowess. Some law enforcement officers in Pakistan cite their inability to get large technology companies such as Facebook and Twitter to release the identities of individuals, furthermore on Twitter once a post has been flagged as offensive it is removed, deleting the evidence unless the police file a request with the company (Bytes for All 2014, 8). Women also found themselves

CEU eTD Collection

falling into a jurisdictional gap, where the government of Pakistan did not have the authority to adjudicate crimes of a global nature. When a website that was being used to incite violence or harass an individual was hosted in a different country, the Pakistani authorities noted that without a bilateral treaty with the relevant country, there was simply nothing they could do (Bytes for All 2014, 6). Given the general societal acceptance of violence against women in Pakistan, it is not overly surprising that law enforcement were less than eager to go above and beyond to assist women experiencing abuse online. These additional hurdles facing women when they report abuse allow men to act with impunity regardless of the enacted legislation.

3.3 The Kingdom of Sweden

3.3.1 Prevalence of TFVAW

Technology facilitated violence against women is not isolated to geographic spaces that are deemed dangerous environments for women. The Kingdom of Sweden is consistently ranked towards the top of the gender equality index and recently was named the most gender equal country in the European Union (European Institute for Gender Equality 2017a, 7). Despite Sweden's impressive levels of gender equality, a 2016 study published in *Social Science and Medicine* notes that the country has surprisingly high levels of IPV. The rate of intimate partner violence in Sweden is 28%, six percentage points higher than the average for the European Union (Gracia and Merlo 2016, 27). A possible explanation for the inconsistency offered by the report is that countries with higher levels of gender equality see higher levels of acceptability and disclosure. This argument is reflected in the so-called "Nordic Paradox", with Denmark and Finland reporting rates of IPV of 32% and 30% respectively (Gracia and Merlo 2016, 28). What this likely reveals is that the rates of intimate partner violence are far higher than global estimates indicate.

In line with these high rates of IPV in Sweden, technology facilitated violence against women is also prevalent at similar levels. A 2017 study conducted by Amnesty International

CEU eTD Collection

reported that 30% of the women polled in Sweden stated they had experienced online abuse or harassment, and 80% of those polled agreed that technology facilitated abuse is common (Amnesty International 2017). Perhaps the most well known case of TFVAW in Sweden took place in 2012 at a secondary school near Gothenburg, Sweden. Two teenage girls started an Instagram account titled "Sluts of Gothenburg" that posted 200 photographs of local teenagers alongside allegations about their sexual history (Lyons et al. 2016). The girls were found guilty of defamation in 2013 and were required to pay 15,000 Swedish krona to each of the 38 victims, sentenced to community service, and juvenile detention (Lyons et al. 2016). This case highlights a common trend in Europe and the United States, where instances of cyber-bullying of minors and TFVAW overlap and often require similar treatment by the law.

3.3.2 Relevance of Existing Laws

There is no specific piece of legislation that works to combat technology facilitated violence against women in Sweden. Rather than writing new laws that are specific to online forms of violence, Sweden uses a comprehensive set of existing laws that cover offline harms to prosecute online actions. The Swedish Penal Code, or *Brottsbalk*, includes a wide variety of crimes that work to combat cyberviolence including unlawful prosecution, stalking, defamation and rape (*Brottsbalk* 1962). In 1998, the Swedish government introduced the *Act on Violence Against Women*, which introduced a new offense "gross violation of a woman's integrity" (Bill 1997/98 55). Gross violation of a woman's integrity provides a mechanism for women to prosecute individuals who commit repeated crimes of a violent or sexual nature (*Brottsbalk* 1962, §4: 4a). Each offense is assessed cumulatively; the maximum sentence for this crime is six years in prison (*Brottsbalk* 1962, §4: 4a). In 2011, the penal code was updated again to include unlawful persecution, which added harassment and stalking to the list of prosecutable offenses (*Brottsbalk* 1962, §4: 4a).

In January 2017, the *National Strategy to Prevent and Combat Men's Violence Against Women* came into force. The National Strategy will take place over a ten-year period, and includes

CEU eTD Collection

provisions for more effective crime-fighting, incorporating data collection and efforts to prevent online threats and abuse (European Parliament 2018, 16). These legislative efforts have had varying degrees of success, which will be discussed in the next section.

3.3.3 Effectiveness of the Existing Legal Framework

The effectiveness of Sweden's laws regarding technology facilitated violence against women is a particularly fascinating case study. While Sweden has no official laws that are specific to cyberviolence, the country has a particularly strong record of using existing laws to prosecute individuals for cybercrimes. In December 2017, Sweden became the first country to successfully try and convict someone for virtual rape, or rape over the internet. A court found that a man who blackmailed children in the U.S., Canada, and Britain into performing acts of a sexual nature in front of a webcam, was guilty of rape and child pornography, sentencing him to ten years in prison and over $130,000 in damages to the victims (Cole 2017). This was a landmark trial and one that will hopefully set a precedent for cyber related offenses globally.

Despite this notable success, a 2015 study published by the Swedish Council for Crime Prevention (NCCP) found that of all types of abusive behavior online, only 4% resulted in prosecution (NCCP 2015, 10; Lyons et al. 2016). The reasoning for the low level of prosecution was twofold; many of the incidents did not constitute criminal offenses, and for those that did reach the level of unlawful persecution or defamation, victims had significant problems identifying their abuser and submitting sufficient evidence to prosecute (NCCP 2015, 87).

This report noted that convicting individuals for image based sexual exploitation, such as "revenge porn" is uniquely challenging in Sweden. Given that the naked body is not considered a derogatory image, merely uploading a nude image or a video of a sexual nature does not constitute defamation (NCCP 2015, 16). The context within which an individual uploads the image or video, including any accompanying text, tends to be more important than the media itself (NCCP 2015, 16). However, the greatest impediment to prosecution was the inability to identify anonymous perpetrators without the help of service providers or internet intermediaries

CEU eTD Collection

such as Facebook, Instagram, Twitter, and YouTube (NCCP 2015, 91). Of the cases closed, 44% were due to insufficient evidence or inability to identify the aggressor (NCCP 2015, 91). While Sweden has a comprehensive set of laws to protect women, they are seemingly inadequate to provide full protection to women online. If Sweden wishes to maintain its status as a leader in gender equality, the government may need to work to fill the gaps in its legal system.

CEU eTD Collection

Chapter 4: Analysis

The three case studies used in this thesis were selected because of their diversity, however they are important for their similarities and the common gaps they identify in the global effort to combat technology facilitated violence against women. While the Democratic Republic of the Congo, Pakistan, and Sweden, each provide a distinct and non-replicable cultural context, there are a number of common threads that yield insights for policy-makers and advocates. The analysis portion of this thesis will look at some of the key areas of global concern, followed by the creation of a typology for TFVAW to assist policy-makers in eliminating gaps in legislation. Finally, the thesis will conclude by calling on international community to formally declare that cyberviolence is a form of violence against women. This would constitute one of many important steps towards eradicating TFVAW.

4.1 Gendered Terrorism: Global Areas of Concern

Existing literature and anecdotal evidence serve as a reminder that technology facilitated violence against women is entrenched in offline inequality. TFVAW is a targeted form of discrimination that is perpetrated with the intent of exercising control over female voices, both in areas of public discourse and in private spaces. This use of fear to give rise to a political outcome is gendered terrorism in cyberspace and it should not be met with impunity. Taking clear and decisive action against TFVAW, however, is not free of challenges. Of the many barriers identified, five are particularly troublesome: anonymity, globalization, insufficient data collection, gender-sensitive training, and the legal preference given to forms of violence with physical consequences. These challenges are well exemplified in the case studies of the DRC, Pakistan and Sweden, but are also prevalent in other country contexts around the world. The first four will be discussed briefly in this section; however, the final barrier will be addressed in section 4.2.

CEU eTD Collection

The ability for attackers to shroud their identity and remain anonymous is perhaps the largest barrier to eradicating TFVAW. Without the expenditure of extensive resources, expertise, and capital, identifying an anonymous abuser is often impossible. The prevalence of online abuse makes exerting this level of effort for each instance unsustainable. Furthermore, large scale political efforts to eliminate anonymity online clash with the very important democratic pillar of free speech. There is no easy answer to this problem and it is one that this thesis does not have the time to address comprehensively. As such, anonymity and its relation to TFVAW is identified as an extremely important area of future research.

In addition to anonymity online, the globalization of the internet creates jurisdictional barriers for governments attempting to identify perpetrators or remove harmful content. When an activist in Pakistan writes on a blog hosted in France, without a bilateral treaty, Pakistani authorities are unable to remedy the abuse. A global effort to improve international cooperation is necessary. A first step towards such a framework could be the creation of a simple, but universally accepted procedure for submitting requests to foreign governments or internet intermediaries. These requests could be for the removal of content, or the preservation of evidence. However, a more comprehensive framework may be more appropriate. A multi-stakeholder partnership working to balance the preservation of free speech with the elimination of TFVAW, while idealistic, would likely be the most effective. Future research regarding anonymity and its relation to TFVAW would be critical to the implementation of any kind of global framework to ensure that governments are not able to misuse these procedures to promote censorship or surveillance.

A third theme that was prominent in all three case studies was the lack of data, not only at a global level, but at a country level as well. If the prevalence of TFVAW is not measured, it will remain difficult to evaluate progress. This thesis implores governments, research institutes, civil society, and international organizations to measure the prevalence of TFVAW in all its forms. UN Women, as the leading international organization on gender equality and female

CEU eTD Collection

empowerment would be well placed to organize a global data collection effort. While this may take years to operationalize, a large part of understanding the scope of a global problem is measuring its prevalence and mapping its consequences.

Finally, gender-sensitive training is crucial for law enforcement, policy-makers, and judicial officials. There must be a normative shift towards recognizing that TFVAW *is* violence, and must be taken seriously. Law enforcement officers should be adequately trained in identifying cybercrimes and know how to handle a cyber-investigation. Without confidence in police, women will be less likely to report violence perpetrated against them. In an attempt to protect themselves, women should make use of encryption, anonymity, and digital security tools. Ideally, the onus for eliminating VAW would not be placed on women, and this thesis is not suggesting that women are in any way complicit in the violence directed at them. However, women are unlikely to get a global reprieve from TFVAW anytime soon. As such there are a number of simple ways women can protect their data and their personal information online to make it slightly more difficult for aggressors to violate their privacy (Deibert et al. 2017, 7). Civil society organizations should invest in training and capacity building for their own staff, and for female communities globally.

The international community has already identified violence against women as a form of discrimination, and has vowed to eradicate it in all of its forms (CEDAW 2017). The typology provided in the next section seeks to identify the forms of TFVAW that are being ignored and implicitly condoned by states, thereby providing policy-makers with a way to identify the gaps in their own legislation.

CEU eTD Collection

4.2 Technology Facilitated Violence Against Women: a New Typology

Existing literature on TFVAW focuses on defining acts of cyberviolence and interviewing women about their experiences. While specific acts of TFVAW and their definitions have been considered in Table 1 of this thesis, it is important to recognize that all acts of

cyberviolence can take both a hybrid and a pure form. This thesis therefore finds a pattern not in the acts of TFVAW that have been successfully written into legislation, but rather in the forms of TFVAW (hybrid or pure) that are acknowledged or ignored by states globally. In order to provide policy-makers and advocates with a tool set to distinguish between various forms of violence, this thesis offers up a new typology explored in Table 2 below.

Table 2: Defining the TFVAW Typology

Hybrid-known: The use of technology by a known assailant to stalk, abuse, kill, or otherwise harm a victim. Most commonly utilized by past or current spouses/partners to terrorize or control the behavior of another individual. Consequences of such actions are identifiable due to their physical nature, however there can be additional economic and psychological side effects.
Hybrid-unknown: The use of technology by an unknown or anonymous individual(s) to carry out or incite violence. This is often used as a weapon to harm or silence female political activists, journalist, and public figures. Consequences of such actions are identifiable due to their physical nature, however there can be additional economic and psychological side effects.
Pure-known: The use of technology by a known assailant to harass or threaten a victim. Most commonly utilized by past or current spouses/partners to terrorize or control the behavior of another individual. Consequences of such attacks are economic and psychological. These attacks do not cross the digital divide.
Pure-unknown: The use of technology by an unknown or anonymous individual(s) to harass or threaten a victim. This is often used as a weapon to harm or silence female political activists, journalist, and public figures. Consequences of such attacks are economic and psychological. These attacks do not cross the digital divide.

The purpose of the TFVAW typology is to identify patterns in protection from TFVAW, and conversely, areas in which women are left vulnerable. Building off of the above typology, Table 3 below provides a visual representation for crafting policy interventions, helping policy-makers to identify where responses are lacking or are too passive. The case studies explored in this thesis have shown that existing laws give more credence to hybrid-known and hybrid-unknown TFVAW, represented in the top two quadrants of Table 3. Because instances of hybrid cyberviolence result in physical impacts, ones that resemble traditional "real world" violence, those impacts are generally protected by existing laws on harassment, stalking and assault. The

CEU eTD Collection

main gaps in legislation in the DRC, Pakistan and Sweden, are found in the bottom two quadrants of Table 3, where pure forms of cyberviolence are outlined.

Table 3: Using the TFVAW Typology

	Known Perpetrator	**Unknown Perpetrator**
Hybrid	Known perpetrator; Commonly directed at ex-spouse or partner; Physical consequences	Unknown or anonymous perpetrator; Commonly directed at activists, journalists, public figures; Physical consequences
Pure	Known perpetrator; Commonly directed an ex-spouse or partner; Psychological, economic consequences	Unknown or anonymous perpetrator; Commonly directed at activists, journalists, public figures; Psychological, economic consequences

While Sweden has had several remarkable instances where pure forms of cyberviolence were successfully prosecuted, these cases are outnumbered by individuals who are unable to gain legal recourse due to the lack of tangible consequences or admissible evidence. Among forms of pure cyberviolence, cases where the perpetrator was unknown or anonymous were almost impossible to prosecute given the existing legal frameworks available to victims. The reasoning behind this varies depending on the country context, but is typically rooted in issues of anonymity, the general stigma placed on mental health, and the stubborn belief that pure cyberviolence is not actual violence. As such, this typology helps policy-makers recognize that while hybrid forms of TFVAW are covered by existing laws, forms of pure cyberviolence are not being adequately addressed.

Non-consensual pornography or "revenge porn" is one area of pure cyberviolence that has begun to gain some traction globally, mainly as the result of high profile hacking directed at international celebrities. However, many "revenge porn" laws require the perpetrator to have

CEU eTD Collection

known or intended the distribution of the image to cause "serious emotional distress" (*Cal. 647(j)(4) PC* 2013). This sets a high legal threshold for victims that acts as a barrier to successful convictions. Even in Pakistan where the 2016 *Prevention of Electronic Crimes Act* theoretically provides protection for acts that "negatively affect one's reputation", the law is rarely accepted and poorly enforced (Bytes for All 2014, 8). Sweden has the opposite problem, where merely posting a nude photo or a video of a sexual nature, is not considered derogatory and cannot therefore be considered defamation (NCCP 2015, 16). As such, the context within which the media is shared matters more than the content itself.

The distinction between hybrid and pure forms of cyberviolence is important because it identifies a key gap in global legislation. Countries worldwide, particularly the DRC, Pakistan, and Sweden have failed to adequately protect women from pure cyberviolence. Policy-makers should craft their proposals for intervention with reference to the TFVAW to ensure pure cyberviolence is equally acknowledged. As noted section 4.1 there are distinct obstacles that prevent policy-makers from intervening in areas of pure cyberviolence, however the idea that pure TFVAW is not *real* violence should not be one of them. The following section calls for a global recognition of TFVAW to ensure that states are fully compliant with international law, and can promptly take steps to fill the gaps in existing legislation.

4.3 A Call to Action: Technology Facilitated Violence Against Women *is* Violence

Women's lives are under constant siege from known and unknown attackers through the use of digital technologies. Accepting these actions as violence against women (VAW) is paramount to the success of the international framework to eradicate VAW, technology facilitated, or otherwise. The case study analyses show that acts of TFVAW that produce psychological and economic consequences are still not accepted globally as violent, abusive, actions. The typology developed in the previous section supports this conclusion and provides a framework for policy-makers to ensure their country is providing comprehensive protection to

CEU eTD Collection

women online. By engaging with legislation that punishes forms of hybrid cyberviolence states have fulfilled only part of their legal obligations to combat VAW; they must go one step further and engage with policy solutions that address pure forms of cyberviolence against women as well.

By officially recognizing TFVAW as a form of VAW, the international community would be taking a symbolic and legally binding step towards gender equality. With this declaration states will be bound by the CEDAW Convention and customary international law to take positive measures to eradicate TFVAW in all its forms, including those that take place entirely in the digital realm (CEDAW 1992). Eliminating TFVAW will not be an easy task; issues of anonymity, jurisdiction, and free speech are bound to cause a variety of legal hurdles. It is crucial that attempts to combat TFVAW do not unwittingly provide opportunities for oppressive regimes to repress free speech under the guise of protecting women. Creating a framework that acts on the severity of TFVAW without unduly violating the integrity of individual user data or user privacy will require extensive cooperation and intellectual capital. However, as the world continues to grow ever more connected, the international community must speak loudly and with one voice to declare that women are welcome on the internet and that aggressors cannot act with impunity in cyberspace.

CEU eTD Collection

Conclusion

Combating violence against women has been an international priority since the 1970s; however, the forms of violence facing women have evolved with the rapid growth of the internet and the proliferation of digital technologies. New and emerging technologies have brought a wide array of positive opportunities to women; however, they have also created new platforms for targeted discrimination and abuse. The various forms of TFVAW, including harassment, stalking, image based exploitation, identity exploitation, physical offenses, and the incitement of violence, are rooted in the same offline inequalities as traditional forms of VAW.

The case studies analyzed within this thesis, the DRC, Pakistan, and Sweden, were chosen using diverse case-selection strategy with the purpose of providing a representative analysis of global legislative efforts to combat TFVAW (Gerring 2008, 650). The case studies show that while states continue to take crucial steps towards eliminating forms of TFVAW, these attempts fall short of a comprehensive effort "to eliminate all forms of violence against women" (CEDAW 1992). Where legislative attempts have been made, they tend to be most successful in prosecuting hybrid forms of TFVAW. Hybrid forms of cyberviolence, unlike pure forms of cyberviolence, exhibit physical consequences of the abuse. While homage has been paid to pure forms of cyberviolence, through PECA in Pakistan (*The Prevention of Electronic Crimes Act* 2016) and one-off cases in Sweden (Cole 2017; Lyons et al. 2016), successful prosecutions of pure cyberviolence are far from everyday occurrences. Pure forms of cyberviolence, particularly when they are perpetrated by unknown or anonymous individuals, are not met with the same level of legal recourse as crimes of a hybrid nature.

Given this bifurcated response to TFVAW, it is crucial that the international community recognize all acts of TFVAW as a form of violence against women. Accepting TFVAW as violence is not merely an exercise in semantics; recognizing TFVAW as a form of violence against women confers very specific legal obligations onto the international community as a

CEU eTD Collection

whole. While acknowledging cyberviolence as violence will not act as a silver bullet to miraculously solve the ever-growing problem of TFVAW, it is the first step towards a necessary normative shift. Given the prominence of the internet and its instrumental role in the lives of women globally, it is time for states to engage with TFVAW. If the global community is ever to create true and lasting gender equality, half of its population cannot be barred from utilizing a key platform for empowerment.

CEU eTD Collection

Reference List

Act on Violence against Women. Sweden. 1998. http://evaw-global-database.unwomen.org/en/countries/europe/sweden/1998/act-on-violence-against-women--government-bill-1997-98-55.

Amnesty International. 2017. "Unsocial Media: The Real Toll of Online Abuse against Women." *Medium*, November 20, 2017. https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

APC. 2016. "End violence:Women's Rights and Safety Online Democratic Republic of Congo Country Report." Association for Progressive Communications. https://www.genderit.org/sites/default/upload/drc_country_report.pdf.

Brottsbalk. 1962. https://lagen.nu/1962:700.

Bustelo, Maria, Andromachi Hadiyanni, Fray Kamoutsi, and Andrea Krizsan. 2007. "Domestic Violence: A Public Matter." In *Multiple Meanings of Gender Equality: A Critical Frame Analysis of Gender Policies in Europe*, edited by Mieke Verloo, 141–84. Central European University Press.

Bytes for All. 2013. "Cyberspace and Violence Against Women: A Review of Existing Legislation in Pakistan." Association for Progressive Communications. https://content.bytesforall.pk/sites/default/files/BaselineStudies.pdf.

———. 2014. "Technology Driven Violence Against Women: Pakistan Country Report 2014." Association for Progressive Communication. https://www.genderit.org/sites/default/upload/tech_driven_violence_against_women1.pdf.

Cal. 647(j)(4) PC. 2013. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=647.&lawCode=PEN.

CEDAW. 1992. "General Recommendation No. 19: Violence against Women." *UN Committee on the Elimination of All Forms of Discrimination Against Women*. http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm.

———. 2017. "General Recommendation No. 35: On Gender-Based Violence against Women, Updating General Recommendation No.19." *UN Committee on the Elimination of All Forms of Discrimination Against Women*. http://www.ohchr.org/EN/HRBodies/CEDAW/Pages/Recommendations.aspx.

Chokshi, Niraj. 2018. "What Is an Incel? A Term Used by the Toronto Van Attack Suspect, Explained." *The New York Times*, April 24, 2018. https://www.nytimes.com/2018/04/24/world/canada/incel-reddit-meaning-rebellion.html.

Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Harvard University Press.

Cole, Samantha. 2017. "In a First, a Man Is Charged for Rape Over the Internet." Motherboard. December 1, 2017. https://motherboard.vice.com/en_us/article/pazyn7/in-a-first-a-man-is-charged-for-rape-over-the-internet.

Const. DRC. 2006.

CEU eTD Collection

https://www.constituteproject.org/constitution/Democratic_Republic_of_the_Congo_2011.pdf?lang=en.

Crenshaw, K. 1989. "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics." *The University of Chicago Legal Forum*, no. 140: 139–67.

Deibert, Ronald J., Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto, and Amitpal Singh. 2017. "Submission of the Citizen Lab to the United Nations Special Rapporteur on Violence against Women, Its Causes and Consequences." University of Toronto Citizen Lab.

Digital Rights Foundation. 2017a. "Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan." https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

———. 2017b. "Online Violence Against Women in Pakistan: Submission to UNSR on Violence against Women." https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/UNSR-Submission-by-DRF.pdf.

Dobash, R. Emerson, and Russell P. Dobash. 1992. *Women, Violence and Social Change*. New York, NY: Routledge.

DRC Penal Code. 2006.

Electronic Crimes Ordinance. 2007. *LXXII*. http://www.pakistanlaw.com/electronic_prevention_ord.pdf.

Electronic Transactions Ordinance. 2002. http://www.pakistanlaw.com/eto.pdf.

Engle, Sally Merry. 2009. *Gender Violence: A Cultural Perspective*. Wiley-Blackwell.

European Institute for Gender Equality. 2017a. "Gender Equality Index 2017: Measuring Gender Equality in the European Union 2005-2015." http://eige.europa.eu/rdc/eige-publications/gender-equality-index-2017-measuring-gender-equality-european-union-2005-2015-report.

———. 2017b. "Cyber Violence against Women and Girls." http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls.

European Parliament. 2018. "Exploring Best Practices in Combatting Violence Against Women: Sweden." http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/604958/IPOL_IDA(2018)604958_EN.pdf.

Evans, Claire L. 2014. "We Are the Future Cunt': CyberFeminism in the 90s." *Vice: Motherboard*, November 20, 2014. https://motherboard.vice.com/en_us/article/4x37gb/we-are-the-future-cunt-cyberfeminism-in-the-90s.

Family Code. Democratic Republic of the Congo. 1987. https://landwise.resourceequity.org/records/1604.

Fascendini, Flavia, and Katerina Fialova. 2011. "Voices from Digital Spaces: Technology Related Violence against Women." Association for Progressive Communications; Women's

CEU eTD Collection

Networking Support Program. http://library.pcw.gov.ph/sites/default/files/voices%20from%20digital%20spaces-technology%20related%20VAW.pdf.

Filipovic, Jill. 2007. "Blogging While Female: How Internet Misogyny Parallels 'Real-World' Harassment." *Yale Journal of Law and Feminism* 19 (1:10): 295–303.

Gerring, John. 2008. "Case Selection for Case-Study Analysis: Qualitative and Quantitative Techniques." In *The Oxford Handbook of Political Methodology*, edited by Janet M. Box-Steffensmeier, Henry E. Brady, and David Collier, 645–84. Oxford University Press.

Gracia, Enrique, and Juan Merlo. 2016. "Intimate Partner Violence against Women and the Nordic Paradox." *Social Science & Medicine* 157 (May): 27–30.

Henry, Nicola, and Anastasia Powell. 2016. "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research." *Trauma, Violence & Abuse* 19 (2). SAGE Publications: 195–208.

Hess, Amanda. 2014. "Why Women Aren't Welcome on the Internet." *Pacific Standard*, January 6, 2014. https://psmag.com/social-justice/women-arent-welcome-internet-72170.

ICTY. 2011. "Landmark Cases." *International Criminal Tribunal for the Former Yugoslavia*, 2011. http://www.icty.org/en/features/crimes-sexual-violence/landmark-cases.

Jane, Emma A. 2017. "Feminist Flight and Fight Responses to Gendered Cyberhate." In *Gender, Technology and Violence*, edited by Marie Segrave and Laura Vitis, 31:45–61. Routledge Studies in Crime and Society. Taylor & Francis.

Johnson, Michael P. 2008. *A Typology of Domestic Violence: Intimate Terrorism, Violent Resistance, and Situational Couple Violence*. Edited by Claire Renzetti. The Northeastern Series on Gender, Crime, and Law. University Press of New England.

Khan, Saira. 2016. "The Outrageous 'Honor Killing' of a Pakistani Social-Media Star." *The New Yorker*, July 19, 2016. https://www.newyorker.com/news/news-desk/the-outrageous-honor-killing-of-a-pakistani-social-media-star.

Leone, Janel M., Michael P. Johnson, and Catherine L. Cohan. 2007. "Victim Help Seeking: Differences Between Intimate Terrorism and Situational Couple Violence." *Family Relations* 56 (5): 427–39.

Lyons, Kate, Tom Phillips, Shaun Walker, Jon Henley, Paul Farrell, and Megan Carpentier. 2016. "Online Abuse: How Different Countries Deal with It." *The Guardian*, April 12, 2016. http://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it.

Marcus, Isabel. 1994. "Reframing 'Domestic Violence': Terrorism in the Home." In *The Public Nature of Private Violence*, edited by Martha Albertson Fineman and Roxanne Mykitiuk, 11–35. New York, NY: Routledge.

Maria da Penha v. Brazil. 2001, 54/01. Inter-American Commission on Human Rights.

Nagarajan, Chitra. 2016. "What Does a Feminist Internet Look Like?" *The Guardian*, September 12, 2016. http://www.theguardian.com/commentisfree/2016/sep/12/feminist-internet-empowering-online-harassment.

CEU eTD Collection

NCCP. 2015. "Police-Reported Threats and Violations against Individuals via the Internet." Swedish National Council for Crime Prevention. https://www.bra.se/publikationer/arkiv/publikationer/2015-02-02-polisanmalda-hot-och-krankningar-mot-enskilda-personer-via-internet.html.

Nyst, Carly. 2014. "End Violence: Women's Rights and Safety Online Internet Intermediaries and Violence Against Women Online." *Association for Progressive Communications (APC)*, 1–32.

OHCHR. 2014. "Violence against Women." United Nations Office of the High Commissioner for Human Rights. June 18, 2014. http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/VAW.aspx.

Pakistan Penal Code. 1860. http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html.

Pencier, Nicholas de. 2017. *Black Code*. Canada: Mercury Films.

Peterman, Amber, Tia Palermo, and Caryn Bredenkamp. 2011. "Estimates and Determinants of Sexual Violence against Women in the Democratic Republic of Congo." *American Journal of Public Health* 101 (6): 1060–67.

Schneider, Elizabeth M. 1994. "The Violence of Privacy." In *The Public Nature of Private Violence*, edited by Martha Albertson Fineman and Roxanne Mykitiuk, 36–58. New York, NY: Routledge.

The Prevention of Electronic Crimes Act. Pakistan. 2016. http://www.na.gov.pk/uploads/documents/1470910659_707.pdf.

The Punjab Protection of Women Against Violence Act. Pakistan. 2016. *Act XVI*. http://punjablaws.gov.pk/laws/2634.html.

The Telegraph Act. 1885. http://www.fia.gov.pk/en/law/Offences/26.pdf.

UNGA. 1993. "Declaration on the Elimination of Violence Against Women." *UN General Assembly*. http://www.un.org/documents/ga/res/48/a48r104.htm.

United Kingdom Home Office. 2016. "Country Information and Guidance Pakistan: Women Fearing Gender-Based Harm or Violence." http://www.refworld.org/pdfid/56c420f34.pdf.

———. 2017. "Country Policy and Information Note Democratic Republic of Congo (DRC): Women Fearing Gender-Based Harm or Violence."

UN Women. 2016. "Global Database on Violence Against Women." March 5, 2016. http://evaw-global-database.unwomen.org/en.

World Conference on Human Rights. 1993. "Vienna Declaration and Programme of Action." http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx.

CEU eTD Collection