The Due Diligence Project's

Privacy in the Digital Age & Human Rights Obligations to Promote Protect and Fulfill Women's Human Rights

Submission to the
Office of the High Commissioner
for Human Rights

April 2018

Privacy in the Digital Age and Human Rights Obligations to Promote Protect and Fulfill Women's Human Rights

1. Introduction 1
2. Situational Context 1
3. Information Communication Technology related Violence against Women 2
    - Privacy 4
    - Harm 5
    - Aggregated Harm 6
    - Consent 6
    - Anonymity 7
4. Actors and Stakeholders 8
    - Primary perpetrators 8
    - Secondary perpetrators 8
    - Data collector 9
    - The State 9
    - Internet intermediaries 11
5. Moving forward 12

Privacy in the Digital Age and Human Rights Obligations to Promote Protect and Fulfill Women's Human Rights

Zarizana Aziz
Due Diligence Project

I. Introduction

The Due Diligence Project[1] (DDP) welcomes the Human Rights Council resolution 34/7 on "The right to privacy in the digital age" to identify and clarify principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard.

The purpose of this contribution is threefold:

- to frame the discussion on privacy beyond the current language and discourse to take into account the specific challenges in the right to privacy in relation to women's human rights and in particular discrimination and violence against women
- to critically examine crucial basic concepts which adds to this understanding; and
- to look at the intersections between privacy and violence against women through the lens of the State Obligation and human rights obligation of business/corporations.

2. Situational Context

Human rights are universal, inalienable, inter-related, inter-dependent and indivisible. International human rights law protects the rights to dignity, equality and freedom of expression and privacy. It also prohibits gender discrimination and gender-based violence against women.

The internet plays an important role in enhancing access to and facilitating the dissemination of information. Freedom of expression (FoE) and access to information are fundamental rights and key enablers to a range of human rights. Information and communication technology (ICT), in particular the internet, has radically transformed the way we interact. In many instances it has become the main form of communication in commercial dealings as well as personal, political and social interaction. It is important that freedom of expression and freedom of information is protected.[2]

As of January 2018, it was estimated that there were 4.021 billion internet users, that is over half of the world's population, and 3.196 billion active social media users.[3] Research in the US indicates that while a gender gap in being online has diminished since 1990, gender gaps in the number of users of the internet and in the frequency of internet use persists with women having significantly fewer uses of the internet than men.[4]

Yet, women's and girls ability to access and utilise the transformative potential of the internet is increasingly under threat by high levels of information and communication technology related violence against women and girls (ICTV). Research in India indicates that 28% of women who had suffered information communication technology related violence against women (ICTV)

[1] The Due Diligence Project (DDP) is a global project that explores and unpacks the international legal principle of 'due diligence' in the context of violence against women. www.duediligenceproject.org
[2] See Human Rights Council resolutions 20/8, 26/13 and 32/13 on "The promotion, protection and enjoyment of human rights on the Internet", which affirm that the same rights that people have offline must also be protected technology related.
[3] *Digital in 2018*, We are Social and Hootsuite. Available at file://wearesocial.com/blog/2018/01/global-digital-report-2018 (last accessed 31 March 2018).
[4] Hiroshi Ono and Madeline Zadovny, *Gender and the Internet*, Social Science Quarterly, 84(1)

intentionally reduced their online presence.[5] Removing violence against women (VAW) from digital platforms has the net effect of promoting and strengthening freedom of expression as it creates an environment that allows more individuals, especially sections of society who face discrimination in other public spaces, to participate in these media.[6]

3. Information and communication technology related violence against women and girls (ICTV)

While the perpetration of ICTV is somewhat new, which itself poses its own challenges, it shares its basis with other forms of violence against women. Although some forms of ICTV require and deserve further exploration, at this juncture the paper will not attempt to exhaustively define ICTV.

Suffice to say that ICTV are acts 'committed, abetted or aggravated' in part or fully by the ICTV[7] and include, amongst others, cyber stalking, bullying, threats, blackmail, sexual harassment, multiple platform harassment and dog piling; assessing or uploading/disseminating intimate photos, videos or audio clips without consent; accessing or disseminating private data without consent; uploading/disseminating altered photos or videos and uploading them to dating, pornography or other kinds of websites; creating fake profiles and other forms of identity theft; mob attacks[8], grooming predation (of children in particular), doxxing (searching and publicizing personal data of another) and exploitation of women and girls.

ICTV shares similarities with other forms of crimes, quasi-crimes and torts such as defamation, extortion (blackmail) and non-consensual disclosure of private data, communications and images; hate speech; and child pornography. Incitement to harm is yet another possible actionable violation. Incitement comprises of both incitement against a group and incitement against an individual. Harm comprises both physical and psychological harm. Sending threatening or offensive material or sharing a persons' private data, and bombarding someone with sexually demeaning emails all constitute violence against women.

As with physical stalking, non-physical stalking can evolve into extreme physical violence. Stalking began receiving recognition after model-actress Rebecca Shaeffer was murdered in 1989 by an obsessed fan who had been stalking her.[9] Since the Shaeffer case, stalking, including cyber stalking, has received somewhat more attention and legal response in California.[10]

---

[5] Japleen Prasricha, *Violence" Online In India: Cybercrimes Against Women & Minorities on Social Media*, Feminism in India. Available at https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf (last accessed 30 March 2018)

[6] Zarizana Abdul Aziz, *Due Diligence and Accountability for Online Violence against Women*. Available at www.duediligenceproject.org and https://www.apc.org/en/pubs/due-diligence-and-accountability-online-violence-against-women.

[7] Women's Legal and Human Rights Bureau, Inc. & Association for Progressive Communications, *From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women* (March 2015), *available at* http://www.genderit.org/sites/default/upload/flow_domestic_legal_remedies.pdf (last accessed 1 February 2018).

[8] For example, the technology related attack of Leslie Jones on twitter and the hacking of her iCloud and cell phone. Twitter later suspended one of the attackers. *See* Katie Rogers, *Leslie Jones, Star of 'Ghostbusters,' Becomes a Target of Technology related Trolls*, the New York Times (July 19, 2016), *available at* http://www.nytimes.com/2016/07/20/movies/leslie-jones-star-of-ghostbusters-becomes-a-target-of-technology related-trolls.html; Nicholas Mojica, *Leslie Jones Hacked: A Timeline of the 'Ghostbusters' Star's Twitter Hate and Technology related Attackers*, International Business Times (August 25, 2016), http://www.ibtimes.com/leslie-jones-hacked-timeline-ghostbusters-stars-twitter-hate-technology related-attackers-2407046.

[9] Associated Press, *The celebrity murder that changed how stalkers are treated,* Page Six (July 14, 2014), http://pagesix.com/2014/07/14/stars-safer-since-actress-1989-murder/ (last accessed 18 February 2018).

[10] Subsequently, California enacted laws criminalizing stalking. Criminal stalking is defined in California as "someone who willfully, maliciously and repeatedly follows or harasses another victim and who makes a credible threat with the intent to place the victim or victim's immediate family in fear of their safety." Continuity of purpose must be established through more than one incident. However, where stalking itself is not a crime, for example in the UK, "offenders get shorter prison sentences that won't make any difference and they go back to stalking". In the UK, a national stalking clinic was opened in London. *See* Lucy Buckland, *World's first*

In Nova Scotia, Canada, the death of 17-year-old student Rehtaeh Parsons, who took her own life after having been subjected to months of harassment and humiliation stemming from the dissemination of a photo of her being allegedly sexually assaulted directly created a public outcry that more was not done.[11]

In October 2013 in New Zealand, the "Roast Busters" sex scandal in which a group of Auckland men allegedly lured young girls into group sex and posted the video of the incidents led to an inquiry into the lack of legal response despite earlier complaints.[12]

In *United States v. Sayer*[13], the perpetrator stalked his ex-wife online, created fictitious Facebook and Myspace pages in her name, disseminated non-consensual intimate media and made Yahoo messenger profiles to invite men to her home, thereby enlisting third parties to harass his ex-wife. The Court, in sentencing, considered the harm to the ex-wife, namely the fear and danger the perpetrator caused through anonymous third parties, the permanent nature of intimate details posted online and his ongoing obsession with her.

In the Irish case of *Teggart v TeleTech UK Limited,* the Court affirmed the dismissal of an employee, finding, amongst others, that the cumulative impact of the obscene Facebook posts about a co-worker, the intention to create a humiliating work environment and the dissemination of the comments among fellow employees justified the dismissal as having been reasonable.[14]

Another form of violation of privacy is the uploading of images of 'beautiful girls" in specific cities and/or disclosure of their personal data (e.g. mobile numbers). In a study in Pakistan, 70% of the surveyed women posited that they were afraid of their pictures being posted online.[15] In the Indian sub-continent, women featured in these postings may suffer harm and could be subjected to further violence, both offline and online irrespective or whether these women were voluntary participants.[16]

An Indian four-year research found that the highest form of ICTV in India was crank calling women to their mobile phones.[17] In India, 40% of respondents assessing a civil society organisation-operated cyber helpline reported that they had been harassed or stalked via messaging applications.[18] This form of ICTV has not received much attention, possibly because it is prevalent only in isolated countries. These crank calls were so bad that women are known to have opted not to have mobile phones.

ICTV is also frequently used to target women whose political opinions and expressions are objectionable to the perpetrators and to silence women's political views.[19] The use of violence to

---

clinic to treat stalkers and prevent violent crimes opens, DailyMail.com (Dec. 8, 2011), http://www.dailymail.co.uk/news/article-2071219/Worlds-clinic-treat-STALKERS-prevent-violent-crime-opens.html#ixzz3fSnXU858 (last accessed 18 February 2018).

[11] *Rape, bullying led to N.S. teen's death, says mom*, CBC News, 9 April 2013. Available at http://www.cbc.ca/news/canada/nova-scotia/rape-bullying-led-to-n-s-teen-s-death-says-mom-1.1370780 (last accessed 8 April 2018).

[12] *IPCA: Police 'let down' Roast Busters' alleged victims*, New Zealand Herald, 19 March 2015. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11419766 (last accessed 31 March 2018).

[13] *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014)

[14] *Teggart v. TeleTech UK Limited*, [2012] NIIT 00704_11IT (Mar. 15, 2012).

[15] *Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan*, Digital Rights Foundation, May, 2017, http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf

[16] DDP expert meeting, 16-17 January 2018, Washington DC.

[17] DDP expert meeting, 16-17 January 2018, Washington DC. Crank calling involves calling someone and hanging up.

[18] *Cyber Harassment One Year Report, December 2017 – November 2018*, Digital Rights Foundation, 2018. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/Helpline-Annual-Report.pdf

[19] See Boo Su-Lyn, *Threatened with rape, G25's Noor Farida now under sedition probe for khalwat criticism*, Malay Mail, 18 December 2015. Available at http://www.themalaymailonline.com/malaysia/article/threatened-with-rape-g25s-noor-farida-now-under-

silence women politically happens both online and offline. The National Democratic Institute studies suggest that female politicians bear a disproportionate brunt of abusive language and threats and estimates that 44 percent of elected female representatives have been threatened in office, including threats of death, rape, beatings and abductions.[20]

With ICTV, it becomes possible to remotely orchestrate concerted attacks on women for expressing their political views. A case in point is the backlash experience by organisers of the Jakarta's Women's March in 2018. Within hours of the successful Jakarta's Women's March to celebrate International Women's Day, the organiser's Instagram site and hashtags were attacked by conservative groups, as were the accounts and images of several high profile participants.[21]

What all these cases have in common was the fact that ICTV was premised on violations of privacy.

- *Privacy*

Violations of women's right to privacy in the digital era constitutes violence against women (VAW). It is an assault on human dignity and as such is both a public wrong and individual harm. Privacy is a protected human right entrenched in, among others, the Universal Declaration of Human Rights.[22]

There are essentially four categories of privacy that is protected at law.[23] Firstly, invasion of privacy means intruding into someone's private affairs under circumstances where a person has a reasonable expectation of privacy. Peeping and snooping are the common terms one would use to describe this kind of invasion. Disclosure of a person's private data without consent is another category of invasion of privacy. This includes revealing 'truths' about another person that is not of public concern. In some cases, for the action to succeed, the public disclosure of the facts in question must be highly offensive to a reasonable person of ordinary sensibilities. In other words, such a test is not applicable for example, where the data consist of a person's phone number, address or bank account details.

Yet a third category of invasion of privacy is appropriation of name or likeness of another person for profit. Profit in this sense means benefit derived from such appropriation, whether financial or otherwise. In this category, a person is deemed to have proprietary rights over her name and likeness and her name and likeness therefor cannot be appropriated without her consent. The final category of invasion of privacy is when a person relates information about another that is misleading, with intent or reckless disregard and which a reasonable person will find offensive. At common law, these are all tortious (non criminal) wrongs for which loss and damage need to be established in order to obtain remedies. For these wrongs to be criminalized, specific legislative penal provisions need to be promulgated.

---

sedition-probe-for-khalwat (Last accessed 28 March 2018); See also David Z Morris, *Bestselling Feminist Author Jessica Valenti Quits Social Media After Rape and Death Threats Directed at Daughter*, Fortune, 31 July 2016. Available at http://fortune.com/2016/07/31/bestselling-feminist-author-jessica-valenti-quits-social-media-after-rape-and-death-threats-directed-at-daughter/ (Last accessed 28 March 2018);

[20] *Violence against Female Politicians*, Foreign Affairs, 11 July 2017. Available at https://www.cfr.org/article/violence-against-female-politicians. (Last accessed 28 March 2018).

[21] Amanda Hodge, *Cyber thugs stir up tirades of hate against Indonesian women demanding equality*, The Australian. 20 March 2018. Available at https://www.theaustralian.com.au/news/world/cyberthugsstiruptiradesofhateagainstindonesianwomendemandingequality/newsstory/7653ffe878c784fb645dea726316ea13

[22] Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[23] See Joey Senat, *Common Law and Privacy Torts* in Waldo, Lynn & Millet, *Engaging Privacy and Information Technology in a Digital Age*, The National Academy Press, Washington DC. Available at https://books.google.com/books?id=1qBVAgAAQBAJ&pg=PT149&lpg=PT149&dq=JOey+senat+2000+privacy+tort&source=bl&ots=1op3YMiJ_f&sig=ffBrnlNJdXqx9kx5p2OBZNebl5I&hl=en&sa=X&ved=0ahUKEwjB_LT9qrXaAhVLJt8KHWObDEgQ6AEIMzAB#v=onepage&q&f=false (last visited 12 April 2018), Chapter 4.2

Everyone has a legitimate expectation that his or her private life would be protected. This expectation, holds that a person's image "constitutes one of the chief attributes of his or her personality, … The right to the protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication thereof …"[24]

Legitimate expectation is applicable even if the person concerned was a public figure. "[E]ven if such a public interest existed, just as there existed a commercial interest for the magazines to publish the photographs and articles, those interests had .. to yield to the applicant's right to the effective protection of her private life".[25]

- *Harm*

To understand the consequence of violations of privacy against women, we must look at its personal aspect as committed by a perpetrator and the harm to the victim as well as the impact of that harm to women given the prevailing demands on women by culture and social norms.

Patriarchy and prevailing interpretations of moral norms, culture and religion place women as the primary bearers of honour and tradition. Transgressions or deemed transgressions of culture by women are viewed as more reprehensible and dealt with by society more severely than those committed by men. These transgressions and deemed transgressions range from women asserting their rights and freedom in relation to sexuality, expression, political participation, marriage and sexual and reproductive health. This renders women more vulnerable and susceptible to "moral" and "cultural" attacks, particularly sexually nuanced attacks.

Because harm can be caused remotely and through third parties, it is necessary to unpack the traditional notion of harm. It is essential that we broaden our understanding of harm to include the manner in which harm can be caused in ICTV violations of privacy. In most instances, ICTV can be gauged by its intent to harm, content, credibility or imminence of harm and context. For example, the Court in *Sayer* took into account the harm caused through the use of ICT namely the fear and danger the perpetrator caused through anonymous third parties and the permanent nature of intimate details posted online.[26]

However, in violations of data, for example the publishing of private or identifying information and images, harm in the traditional sense maybe more difficult to establish. The law needs to expand its narrow understanding of harm often excludes the intangible concepts of privacy, dignity and sexual integrity. These risks are deemed to be part of "the ordinary frustrations and inconveniences that everyone confronts in daily life with or without fraud or negligence".[27] Therefore specific legislation is required for these kinds of violations of privacy.

Where harm is not immediately apparent, malicious intent, may in appropriate circumstance be sufficient to render an act actionable. This includes acts such as doxxing, where personal information and data retrieved by the perpetrator is made public with malicious intent.[28] For these cases, complainants would need to rely on privacy harms (see "Consent" below).

---

[24] ECtHR, *Von Hannover v. Germany* (No. 2), Grand Chamber judgment of 7 February 2012, § 96. This legitimate expectation is grounded in Article 8 (right to respect for private life) of the European Convention on Human Rights and its violation constitutes a violation of human rights.
[25] *Id.*
[26] *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014)
[27] *Id*.
[28] Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints and DNA).

➢ *Aggregated harm*

The internet provides a forum where harm can be inflicted in multiples of hundreds, thousands or even millions who had been wittingly or unwittingly enlisted to participate in and re-perpetrate the violence resulting in an aggregate harm. The target may be an individual, such as when a woman's personal details and intimate photos are made public. Or the target may be women as a class, motivated by gender animus (hate speech based on gender).

In describing the aggregated harm the unauthorized release of her intimate photos caused, a Hollywood actress said,

> "When I first found out it was happening, my security reached out to me. It was happening minute-to-minute — it was almost like a ransom situation where they were releasing new ones every hour or so. And, I don't know, I feel like I got gang-banged by the fucking planet — like, there's not one person in the world that is not capable of seeing these intimate photos of me."[29]

Rehtaeh Parson's mom narrated the trauma her daughter went through from the circulation of the photo of her alleged rape. "She walked into the school and everyone started calling her a slut, … She was never left alone. Her friends turned against her, people harassed her, boys she didn't know started texting her and Facebooking asking her to have sex with them since she had had sex with their friends. It just never stopped." In the meantime, the police told the family that the photographs were not a criminal issue even though Rehtaeh was underage.[30]

➢ *Consent*

A criteria in determining whether a violation has occurred is consent. Consent in relation to violation of privacy is often complicated by the exact act to which the consent, if any, relates. Because of this, defining consent is crucial and must be addressed in any mechanism dealing with violation of privacy. Consent that is specific to an individual, like sharing of intimate photos, cannot be expanded to consent for the data to be shared and disseminated more widely.

Consent may also be conditional and temporal. A German Federal Court ordered a photographer to destroy intimate photos of his ex-lover after their break-up, irrespective of whether he had any intention of sharing them. The Court held the consent to have been withdrawn when their relationship ended as retaining the photos would have granted the photographer 'manipulative power' over his ex-lover.[31]

Focusing on consent recognizes that women have the right to sexual expression, in other words that there is nothing intrinsically unlawful or immoral about expressing oneself sexually through digital images. It is not the taking, but the spreading of these images, videos or other private data without consent that is unlawful or immoral.

What also needs to be remembered is that personal data is no less personal even though it may be available in the public domain. In the digitized world of big data, what is personal and what is public data is blurred. Our personal data is continuously being handled and commoditized by internet intermediaries and other corporations. Such personal data however, is no less personal even though it may be available in the public domain. This further emphasizes that consent for its dissemination is crucial in determining whether a violation of privacy has been committed.

---

[29] Scott Fienberg, *'Awards Chatter' Podcast — Jennifer Lawrence ('Mother!')* The Hollywood Report, 20 November 2017. Available at https://www.hollywoodreporter.com/race/awards-chatter-podcast-jennifer-lawrence-mother-1059777. Accessed 1 February 2018.

[30] http://www.cbc.ca/news/canada/nova-scotia/rape-bullying-led-to-n-s-teen-s-death-says-mom-1.1370780

[31] Sex tape row: German court orders man to destroy naked images, BBC News, 22nd December 2015, http://www.bbc.com/news/world-europe-35159187 (last accessed 1 February 2018).

➢ *Anonymity*

The anonymous nature of the internet may elevate the perception of online disinhibition as, in the online environment, people are less sensitive to the consequences of their actions due to geographical and temporal distance.[32] On the one hand, the relative anonymity made possible by ICT allows women to transgress and challenge cultural norms, especially in relation to sexuality. On the other hand, anonymity and disinhibition effect may motivate the perpetration of ICT related violence.[33] Consequently, understanding the negative or toxic use of the internet is important.

The same anonymity combined with the speed, ease and reach of transmission provides an optimum platform for extortion, particularly as the victim/survivor herself, more than the perpetrator, tends to bear the brunt of societal condemnation if the ICTV involves the uploading of suggestive or sexually explicit images and conversations either maliciously or without the victim's/survivor's consent.

Anonymity is a feature that has to a large extent contributed to the lively and provocative discussions on the internet. There is a false sense that anonymity and accountability are inversely related in that increased anonymity results in decreased accountability.

The internet offers unprecedented capacity for criminals, pranksters, governments and corporations to interfere with the rights to freedom of opinion and expression. For this reason, encryption, anonymity and the concept of security behind them is essential in the face of political censorship as it creates a zone of privacy to protect opinion and belief.[34] The internet, having become a "central global public forum", deserves protection. Further, "such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity."[35]

Protecting the anonymity of users has also facilitated social and political activism particularly in oppressive regimes. Experts have maintained that restrictions on encryption and anonymity tools put the privacy of all internet users at risk.[36] Anonymity is critical for whistle-blowers, human rights defenders and victims of ICTV (both for purposes of reporting and re-entry into ICT spaces post ICTV) and those who oppose current dominant groups or those who are under historical social/cultural/political surveillance because of their identity including black/indigenous/ migrant/women, sex workers, queer people, young women and those identifying as LGBTQIA.

It is simplistic therefore to view anonymity as a threat that needs to be removed under all circumstances. Formulating principles and guidelines that allow the internet to continue to be the central global public forum that defends the right to privacy and is free from government censorship on the one hand, yet ensuring that it is not used as an instrument to commit violations of women's human rights, on the other hand, is critical. Rather than removing anonymity, the solution

---

[32] Computer-mediated communication has given rise to the "disinhibition effect". People may self-disclose or act out more frequently or intensely than they would in person. Researchers have identified six factors that interact with each other in creating the ICT disinhibition effect: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority. John Suler, *Cyber Psychology & Behavior*, July 2004, 7(3): 321-326

[33] Randy M Young & Ors, *Does gender matter in cyberbullying perpetration? An empirical investigation,* Computers in Human Behaviour, 79 (2018)247 – 257 quoting Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206e221. In the online environment, people are less sensitive to the consequences of their actions due to geographical and temporal distance.

[34] *Id*.

[35] *See Report on encryption, anonymity, and the human rights framework,* United Nations Human Rights Office of the High Commissioner, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (last accessed 18 February, 2018).

[36] Kaye, David, (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinon and Expression), U.N. Doc. A/HRC/29/32 (May 22, 2015), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement.

may lie with simultaneous implementation of anonymity protections and accountability mechanisms.[37]

4. Actors and Stakeholders

Any response to violations of privacy must address the following actors and stakeholders. There are five actors and stakeholders involved in violations of privacy. Firstly, the person initiating the violence, namely the author, and/or the person who gathers personal data first uploads the violating material. This is the primary perpetrator. Secondly the person, who purposefully, recklessly or negligently downloads, forwards, or shares the violating material. Thirdly the entity storing the personal data to some degree, tasked with protecting the personal data. Fourthly, the State, who bears the international obligation to eliminate violations of human rights including violence against women. Lastly, the internet intermediaries on whose platforms ICTV is perpetrated.[38]

➢ *Primary perpetrator*

The individual who generates the violating material is clearly the primary perpetrator. However, legal enforcement officers often lack the training, skill or resources to identify perpetrators who employ protocols to shield their identity, thus offering little or no protection for victims/survivors.

The inability of law enforcement and intelligence services to uncloak anonymity or decipher encrypted communications to investigate crimes has raised "legitimate concerns about how bullies and criminals use new technologies to facilitate harassment."[39] Over-regulation on the other hand, can lead to technology related censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression and can put the privacy of all internet users at risk.[40]

➢ *Secondary perpetrators*

Given the ease and speed of transmission, eliminating ICTV which violates privacy includes not only addressing and eliminating the primary violation (by the principal perpetrator) but also the dissemination, whether wittingly or unwittingly, by others (secondary perpetrators). Once posted, the offensive material may generally be accessed by others who may download the material, share it by reposting or by creating a link to the material. These others may then take action to discriminate or commit hostile or violent acts against the victim/survivor, for example by directly communicating with the victim/survivor or related persons.

Little attention and effort is made to hold these secondary perpetrators, who re-transmit the violating material, liable. Data and images that are tweeted and re-tweeted, downloaded and forwarded, liked and shared may involve a great number of individuals and pose an overwhelming challenge to regulators. Further reflection is needed on how to hold re-transmitters responsible for the transmission of violating materials.

Intent, or more specifically, lack of intent, can be an issue with secondary perpetrators. Still, holding persons accountable despite lack of intent is not without basis under the law, such as the concept

---

[37] Wolff, Josephine, *Application-layer design patterns for accountable–anonymous online identities*, Telecommunications Policy 37(2013)748–756.

[38] Internet intermediaries bring together or facilitate transactions between third parties on the internet and ICTs. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties. For purposes of this paper, they include internet or digital access providers, internet service providers, network infrastructure providers, platform providers including social platforms.

[39] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinon and Expression), U.N. Doc. A/HRC/29/32 (May 22, 2015), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement (last accessed 18 February 2018).

[40] *Id*.

of reckless indifference where intent cannot be established. Another example is the established liability of persons repeating slanderous or defamatory statements.[41]

- *Data collector*

With the increasingly massive collection and storage of data by corporations, it is crucial that we re-think privacy. Unauthorized access to and dissemination of data all cause distress, harm and damage. Yet, courts frequently do not recognize harm arising from breaches or theft of data.[42] This is because taking preventive steps to avoid or remedy foreseeable risk of future harm arising from data breaches (as opposed to actual damage or injury) is not generally a cognizable injury. Neither is emotional distress caused by exposure of data. These risks are deemed to be part of "the ordinary frustrations and inconveniences that everyone confronts in daily life with or without fraud or negligence".[43]

That being the case, it is necessary to re-look at the business model that focuses on collection, storage and analysis of massive amounts of personal data. This is particularly critical as often, the data collected by corporations and businesses are disproportionate to what is required for interaction with their customers.

After all, data, today, is the most valuable commodity and its breach not only harms the individual but can have other far reaching consequences. Companies who elect to collect and store massive data, should regard themselves as equivalent to data banks with the concomitant responsibility to protect their customer's personal data.[44] The European Union (EU) is also set to bring into effect the General Data Protection Regulation (GDPR) on 25 May 2018. The changes to be ushered in by the new regulations will dramatically shift control over personal data to the subject and require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure, amongst others.[45] The regulation will also assert extra-territorial jurisdiction as it is applicable to all EU companies as well as international companies that collect or process personal data from subjects residing in the EU.[46]

- *The State*

Merely criminalizing violations of privacy does not provide the remedy required by women. Criminal law should form part of the repertoire of responses to violationd privacy, not its entire response. Experience has shown that women's access to justice should be victim/survivor oriented and comprise a mix of criminal, civil and administrative processes and include prevention of ICTV;

---

[41] "A false statement is not less libelous because it is the repetition of rumor or gossip or of statements or allegations that others have made concerning the matter." Ray v. Citizen-News Co.(1936) 14 Cal.App.2d 6, 8-9.
[42] *In re Hannaford Bros Co. Customer Data Security Breach Litigation*, 2010 ME 93, 4 A.3d 492
[43] *Id*.
[44] Last month, a whistleblower provided details of how the misuse of data by Cambridge Analytica influenced the results of elections and referendums. The company "harvested millions of Facebook profiles of US voters in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box." This is done by profiling "individual US voters, in order to target them with personalized political advertisements". Carole Cadwalladr *and* Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, 17 March 2018. Available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (last accessed 4 April 2018). The latest figures released by Facebook estimate that "87 million users, most of them in the US but at least 1 million in the UK, may have had their information improperly obtained and used by the data mining firm Cambridge Analytica". Nick Statt, The Verge, 4 April 2018. Available at https://www.theverge.com/2018/4/4/17199632/facebook-cambridge-analytica-data-collection-87-million-users-api-developer-restrictions (last accessed 6 April 2018).
[45] Nate Lord, *What is GDPR (General Data Protection Regulation)? Understanding and Complying with GDPR Data Protection Requirements,* Digital Guardian, 23 January 2017. Availabel at https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection (last accessed 6 April 2018). See also *GDPR Key Changes*, https://www.eugdpr.org/key-changes.html (last accessed 6 April 2018).
[46] *Id*.

protection of victims/survivors; prosecution and punishment of perpetrators and provision of redress and reparation for the victims/survivors.

State regulation however, must be conscious of not violating freedom of expression yet at the same time, prioritizing women's access to ICT in a safe environment where perpetrators of ICTV do not enjoy impunity. The State has a positive role in creating an enabling environment for women, as much as men, may enjoy their rights and freedoms, including gender equality, freedom of expression and right to safety and security.

At the same time, the State must be conscious not to over-extend its regulatory powers as this can lead to violations of freedom of expressions including women's freedom expression. Strong democratic structures — including free and fair elections, an independent judiciary and a vibrant civil society — are needed to prevent abuse and to realize more fully the goals of pluralism and equitable access.[47] Crucially, these measures must be developed within the framework of human rights and democratic institutions as well as in consultation with key stakeholders, namely civil society (including women's rights organizations and the academia) and the technical community.

Notable laws on violations of women's privacy include reforms implemented in California after Shaeffer's death. These include laws that make stalking a crime (felony stalking), availability of long term protection orders (up to ten years) for stalking, restrictions on public access to information from driving records in California, and a specialized Los Angeles police unit that works with prosecutors, attorneys and security details to keep stalkers a safe distance away from their target.[48]

The *Intimate Images and Cyber-Protection (Nova Scotia)* creates civil remedies in cases involving cyberbullying and the distribution of images without consent.[49] It defines cyberbullying as an "electronic action that is maliciously intended to cause harm or an action carried out in a reckless manner, with regard to the risk of harm". The Act also established a unit that is tasked with assisting victims through the process of getting online images or posts removed.[50]

The New Zealand *Harmful Digital Communications Act 2017*[51] provides victims/survivors with a quick and efficient means of redress for harm (defined broadly) caused to individuals by ICT (including any text message, writing, photograph, picture or recording). The Act also creates an agency to which victims can turn when they face ICT related abuse; a set of court orders that can be served against internet intermediaries and perpetrators upon referral by the aforementioned agency; new civil and criminal offences; and a 48-hour content takedown process whereby individuals can demand that internet intermediaries remove content they allege is harmful.[52] Internet intermediaries are afforded safe harbor protection from criminal and civil liability if they correctly set up a process for individuals to seek removal of harmful content.

The *Criminal Justice and Courts Act 2015* (England and Wales) created new Sections 33-35 and Schedule 8 which provide a new criminal offence of disclosing private sexual photographs and films without the consent of an individual who appears in them, with intent to cause that individual distress (so called "revenge porn provisions").[53] The law defines revenge porn as "photographs or films which show people engaged in sexual activity or depicted in a sexual way or with their

---

[47] *See for example*, Article XIX, *Camden principles on Freedom of Expression and Equality* (April 2009), *available at* https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf.

[48] Associated Press, *The celebrity murder that changed how stalkers are treated*, Page Six (July 14, 2014), http://pagesix.com/2014/07/14/stars-safer-since-actress-1989-murder/.

[49] https://nslegislature.ca/legc/bills/63rd_1st/3rd_read/b027.htm

[50] The previous law allowed the unit to act on behalf of the victims by pursuing their cases in court.

[51] Public Act 2015 No. 63. Available at http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html (last accessed 31 March 2018).

[52] Nyst at 18-22.

[53] *Criminal Justice and Courts Act 2015*, ss. 33 -35. Available at http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted, http://www.legislation.gov.uk/ukpga/2015/2/section/34/enacted and http://www.legislation.gov.uk/ukpga/2015/2/section/35/enacted. (last accessed 31 March 2018).

genitals exposed, where what is shown would not usually be seen in public". It covers images shared on and offline without the subject's permission and with the intent to cause harm. The section carries a maximum of 2 years imprisonment. In 2015 – 2016, there were three prosecutions of rape pornography and 206 prosecutions commenced of the offence of disclosing private sexual images without consent.[54]

The *Indian Information Technology Act* which criminalises violations of privacy by non-consensual publication and transmission of images of 'private parts' of an individual. See S.66E. Punishment for violation of privacy - Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. [55]

- *Internet intermediaries*

Eliminating ICTV which is premised on violations of privacy requires the intercession of internet intermediaries, including transnational corporations serving the role of internet intermediaries.

As violations of privacy happens not merely on the first upload by the primary perpetrator, but is repeated every time it is liked and shared, re-tweeted, searched and downloaded or forwarded, internet intermediaries are uniquely situated to stop the recurrence of the violence and provide the necessary relief and remedy needed by victims/survivors. It is also more cost effective to seek redress from internet intermediaries than all the re-transmitters (which in fact may not even be logistically possible).

Internet intermediaries have a responsibility to put in place preventive measures and respond to violating materials, especially when they have the capacity to moderate content and have in place measures to flag and report "user generated" content.[56] There are precedents where the courts have been "mindful of the risk of harm posed by content and communications on the internet" and demanded greater vigilance from internet intermediaries.[57]

Because of the internet's capacity to store and communicate staggering amounts of information, internet intermediaries are placed in a unique position.[58] In any event, it is unrealistic to expect the internet to provide a platform for unrestricted free speech. Free speech as we understand it is already mediated by internet intermediaries.[59] Consequently, freedom of expression is increasingly becoming nebulous and dependent on the "protective" measures put in place by the internet intermediaries themselves.

Still, based on a business for profit model, more self-regulatory mechanisms will be put in place where violations would be economically or financially detrimental, for example breach of

---

[54] *Delivering Justice: Violence against women and girls crime report*, 2015 – 2016, Crown Prosecution Service, UK, p. 90. Available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps_vawg_report_2016.pdf

[55] *Information Technology Act 2000*. Available at http://www.lawzonline.com/bareacts/information-technology-act/section66E-information-technology-act.htm (last visited 12 April 2018).

[56] Compare this to the more traditional media such as newspapers. Statements carried in newspapers are vetted and edited, as necessary. Thus the level of control over newspapers is much higher than the control exerted by internet and digital platform providers.

[57] *See* Delfi, § 157. "While acknowledging the "important role" played by the Internet "in enhancing the public's access to news and facilitating the dissemination of information in general". Although Delfi did not involve violence against women, this dicta is persuasive and is applicable to ICTV. *See also* Ahmet Yıldırım, cited above, § 48, and Times Newspapers Ltd, cited above, § 27. The Court reiterates that it is also mindful of the risk of harm posed by content and communications on the Internet (see Editorial Board of Pravoye Delo and Shtekel, cited above, § 63; see also Mosley, cited above, § 130)".

[58] European Court of Human Rights, *Ahmet Yıldırım v. Turkey*, App. No. 3111/10 (2012), § 48, and Times Newspapers Ltd, § 27.

[59] See criticism of Facebook's policy on nudity in Levin, Wong and Harding, *Facebook backs down from 'napalm girl' censorship and reinstates photo*, Guardian, 9 September 2016. Available at https://www.theguardian.com/technology/2016/sep/09/facebook-reinstates-napalm-girl-photo.

intellectual property, which has cost internet ntermediaries millions in damages. A better paradigm which can exist alongside State obligation to eliminate violence against women, is for intermediaries to subscribe to a new business model that holds themselves accountable because of their own human rights responsibilities.[60]

5. Moving forward

For various structural and functional reasons, there is merit in the argument that neither institution, the State and internet intermediaries, should be regulating ICT on their own but that we should consider establishing another mechanism. Furthermore, States attempting to hold perpetrators, re-transmitters and internet intermediaries accountable are faced with a major complication, namely that some of these individuals and entities may be beyond the reach of a State's jurisdiction. Only in rare cases do States assert territorial jurisdiction over matters occurring outside their physical boundaries. Yet, the global nature of the internet has added an urgent need to re-examine the meaning of extra-territoriality.[61]

In considering if an independent third party mechanism is the answer, questions on governing structure, access to information, enforcement procedures and resources will need to be carefully thought out. The mechanism should form part of the national democratic institutional structure capable of providing quick and efficient means of redress.

Still, the ensuing jurisprudence from multiple jurisdictions has resulted in confusing or conflicting court decisions.[62] What is required is an international multi-stakeholder framework that harmonizes and prescribes the factors to be considered for indirect internet intermediary liability and the defenses available against such liability.[63]

Industry actors too can take the initiative to establish an independent mechanism serving several internet intermediaries to review decisions of internet intermediaries regarding user complaints once the initial internal team decides (or fails to decide within a reasonable time) on such complaints. Such mechanism must be transparent and capable of providing quick and efficacious justice sensitive to the needs of ICTV victims/survivors based on human rights principles. In such a diverse ecosystem that is the ICT, these processes must work for all parties concerned and not overly punish small industry actors and stakeholders.

Any mechanisms however must protect the right of women to freedom from violence including violations of privacy with as much passion as right of all to freedom of expression. Pitting one against the other as the starting point can lead to misguided solutions.

---

[60] John Ruggie, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy Framework,"* (UN Human Rights Office of the High Commissioner, 2011). The Guiding Principles were proposed to the United Nations Human Rights Council as part of the 2011 report to the Council by then-UN Special Representative on business & human rights, John Ruggie: *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie,* UN Doc. A/HRC/17/31, Mar. 21, 2011, *available at* http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. *See also* Guidelines for Multinational Enterprises of the Organisation for Economic Co-operation and Development and the Ten Principles of the UN Global Compact, available at https://www.unglobalcompact.org/what-is-gc/mission/principles

[61] States have used different approaches to overcome extra-territoriality e.g. European Union's *General Data Protection Regulation.*

[62] Compare the court decisions of A&M Records Inc v. Napster (9th Cir. 2001) and UMG Recordings Inc. et al. v. Veoh Networks Inc et al. (9th Cir. 2011). Napster was held liable for third party infringing content and Youtube not liable despite a high amount of infringing content existing on both platforms.

[63] *See also* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Note by the Secretariat, U.N. Doc. A/HRC/32/38 (11 May 2016), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement (last accessed 18 February 2018).