

GLOBAL INFORMATION SOCIETY WATCH 2015

Sexual rights and the internet



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

Global Information Society Watch 2015

Sexual rights and the internet

Steering committee

Anriette Esterhuysen (APC)

Will Janssen (Hivos)

Coordinating committee

Monique Doppert (Hivos)

Valeria Betancourt (APC)

Mallory Knodel (APC)

Jac sm Kee (APC)

Nadine Moawad (APC)

Project coordinator

Roxana Bassi (APC)

Editor

Alan Finlay

Assistant editor, publication production

Lori Nordstrom (APC)

Proofreading

Valerie Dee

Stephanie Wildes

Graphic design

Monocromo

info@monocromo.com.uy

Phone: +598 2400 1685

Cover illustration

Matias Bervejillo

Financial support provided by

Humanist Institute for Cooperation with Developing Countries (Hivos)

Hivos

APC and Hivos would like to thank the Swedish International Development Cooperation Agency (Sida) for its support for Global Information Society Watch 2015.



Published by APC and Hivos
2015

Printed in USA

Creative Commons Attribution 3.0 Licence
(creativecommons.org/licenses/by-nc-nd/3.0/)
Some rights reserved.

ISBN 978-92-95102-41-5
APC-201510-CIPP-R-EN-P-232

Problematizing the dominant discourse around children, youth and the internet

Mitali Thakor

Massachusetts Institute of Technology
www.mitalithakor.com

Introduction

This report is framed as a challenge to the dominant discourse on children online – a discourse that characterises children in online spaces as vulnerable victims rather than people with agency and risk-management capacity. The current discourse on child victimisation draws from 21st century human trafficking policy, which has generally taken an enforcement- and prosecution-driven approach to problems of exploitation. Global agendas against child exploitation have predominantly replicated anti-trafficking discourse, making assumptions about violence, risk and vulnerability online.

In this report, I will describe the dominant discourse on children online as one of victimisation, and then describe three common digital methods being used against child exploitation: text detection, image detection, and online sting operations. I argue that the discourse of victimisation does not actually uphold victim *rights*, and that in fact many predominant anti-exploitation methods threaten the privacy rights and sexuality rights of young people. Rights to privacy are in jeopardy as the dominant anti-exploitation approach relies on state enforcement and policing, following in the footsteps of older surveillance techniques by monitoring citizens' internet behaviour and increasing government regulation of online traffic. Additionally, the sexuality rights of young people, while perhaps a controversial subject, are also fundamentally threatened by a dominant discourse that positions all children as victims and does not recognise the sexual agency of young people. Under the supposed goal of safety, many anti-exploitation measures by states have veered toward censorship, limiting young people's access to all forms of sexual content online, including sexual identity, sexuality and reproductive health resources.

Recognising that problems of violence, sexual exploitation, misogyny and harassment online are very real, I conclude by imagining what a more

feminist and sustainable approach to address these issues might look like. Dominant anti-exploitation efforts centralise technocratic expertise in the hands of states and large technology companies. I suggest an alternative approach that uses participatory ethnographic research and youth input to influence technology design that honours young people's lived experiences and supports their already ongoing practices of risk management.

The dominant discourse of victimisation

Who gets to be a victim? Are children automatically assumed to be victims by dominant legislative agendas? Which children, and where? Such questions help us understand and critique the current global discourse on child exploitation and victimisation, which takes its cues from the soaring rise in attention to “trafficking” in the past few decades. Much of the language and ideology of the current anti-trafficking movement is rooted in the drafting process for what would become the UN protocol on human trafficking. Human trafficking is defined under the 2000 United Nations Office on Drugs and Crime (UNODC) Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children as “the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception (...),” and expressly prohibits the trafficking of children for the purposes of commercial sexual exploitation.¹ Feminist scholars² have noted that the protocol drafting process brought together

1 United Nations General Assembly. (2000). Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime. UN Doc. A/55/383 at 25. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12-a&chapter=18&lang=en%7Ctitle=UNTC%7Cwork=un.org-title=UNTC-work=un.org

2 See, for example, Soderlund, G. (2005). Running from the rescuers: New U.S. crusades against sex trafficking and the rhetoric of abolition. *NWSA Journal*, 17(3), 64-87; Musto, J. (2009). What's in a name? Conflations and contradictions in contemporary U.S. discourses of human trafficking. *Women's Studies International Forum*, 32, 281-287; Bernstein, E. (2007). The Sexual Politics of the “New Abolitionism”. *Differences: Journal of Feminist Cultural Studies*, 18(3), 128-151.

a peculiar constellation of religious advocates, anti-prostitution feminist activists, bureaucrats, and law enforcement; the rubrics under which they found common agreement have resonance for current child exploitation policy. It is telling that the UN protocol on trafficking, one that had been suggested and discussed for years in various UN agencies, was eventually pushed through by the agency handling transnational drugs and crime control.

Perhaps the most striking point for agreement between these disparate advocacy groups is a shared ideology of punishment for trafficking as a crime. Bernstein³ argues that, in constructing legislation for the criminalisation of trafficking, a conservative Christian sense of penalty and retribution met a second-wave feminist aim to prosecute perpetrators of sexual violence and exploitation of women and girls. This shared ideology of “carceral feminism” advocates for state- and law enforcement-based solutions for addressing crimes of interpersonal violence and exploitation, and glosses over how many marginalised people are in fact often subjected to violence at the hands of the state itself, through structures of policing, environmental law, and economic policy. This point on structural violence and state violence is replicated, I argue, with online policies as well.

Many countries have used the protocol to model their own laws on trafficking, forced migration, labour exploitation and sexual exploitation, including vague definitions of “trafficking victim”, consent and migration. The United States’ (US) domestic commitment, especially, to carceral paradigms of justice has expanded into similar policies abroad with state-based interventions into cases of trafficking, through practices of what Bernstein calls “militarized humanitarianism” – the US financing of enforcement-heavy policing and raids of brothels, settlements and urban spaces where cases of exploitation and trafficking have been purported. This point is perhaps best exemplified by the US State Department’s Trafficking In Persons Report, a country-by-country ranking of the US’s assessment of governmental efforts to prevent and prosecute trafficking. As Pardis Mahdavi notes, lower rankings correspond to sanctions or reductions in foreign aid.⁴ Additionally, “anti-trafficking” has become a hugely marketable and profitable

awareness campaign for numerous activist groups, which use the images and metaphor of “modern-day slavery” to generate millions of dollars in foreign aid and donations. I argue, along with other feminist scholars,⁵ that this new “abolitionist” movement has become another rationale for the neo-imperialist rescue of people in the global South, especially those identified as “prostitutes”, replicating a pattern of humanitarian intervention that has frequently been critiqued by post-colonial activists. The UN protocol title, for example, explicitly calls attention to “Especially Women and Children”, a phrasing that feminist activists have criticised as contributing to the assumption of the feminising of victimhood and the masculinising of rescue. Agustín⁶ suggests that the specific focus on sex trafficking (as opposed to, for example, issues of education, poverty or environmental justice) in global South countries has produced its own veritable “rescue industry” of professionalised humanitarians, journalists, bureaucrats and corporate representatives seeking to stake their claim on anti-trafficking turf. Children’s charities, especially, many of which have been working on issues of youth education, nutrition, sexual health and child labour for decades, have begun switching their primary focus to trafficking and exploitation as a signal of their commitment to this latest humanitarian agenda.

Digital strategies against child exploitation

Additionally, most trafficking and exploitation policies do not explicitly deal with technology, and in this current moment software development far outpaces legislative policy. Abuses online have their parallels online, and children’s advocacy organisations have taken to digital methods for finding and preventing child exploitation, including digital forensics, biometric software, and image detection technologies. In recent years, an unprecedented level of alliances have been forged between technology companies, researchers, activists and law enforcement strategising to detect cyber crime and to collect digital data as evidence. In addition, we have seen a rise in cross-border police partnerships, as virtual crimes often implicate multiple countries or anonymous locations in law enforcement attempts to locate victims, abusers and downloaders alike.

3 Bernstein, E. (2010). Militarized Humanitarianism Meets Carceral Feminism: The Politics of Sex, Rights, and Freedom in Contemporary Anti-Trafficking Campaigns. *Signs: Journal of Women in Culture and Society*, 36(1), 45-71.

4 Mahdavi, P. (2011). *Gridlock: Labor, Migration, and Human Trafficking in Dubai*. Stanford: Stanford University Press.

5 See, for example, Kempadoo, K., & Doezema, J. (1998). *Global Sex Workers: Rights, Resistance, and Redefinition*. New York: Psychology Press; Desyllas, M. C. (2007). A Critique of the Global Trafficking Discourse and U.S. Policy. *Journal of Sociology and Social Welfare*, 34(4), 57-79.

6 Augustin, L. (2007). *Sex at the Margins: Migration, Labour Markets and the Rescue Industry*. London: Zed Books.

Three strategies for countering trafficking and exploitation online that I would like to highlight are:

- *Text and financial transaction detection:* Data mining algorithms are designed and used in criminal investigations to rapidly search large databases. Text analysis can assist with analysing language patterns in online advertisements, for example to detect advertisements suggesting the offer of sexual services by under-age minors. Text detection can also assist police working with social media companies on existing investigations, to trawl through data for key phrases, dates and locations; and with financial transaction analysis, detecting potentially fraudulent transactions, as well as other indicators that may serve as evidence for prosecutions.
- *Image and video detection:* Image analysis – the detection, filtering, categorisation and recognition of digital photos – is a common tool in conducting anti-exploitation cases. Digital forensics tools automate the process of searching through photo data collected from computers and hard drives confiscated by police during investigations. Interpol manages the International Child Sexual Exploitation image database,⁷ which can be used for image-matching with photos of missing children, victims, abusers and geographic locales. Other technologies can determine if images have been digitally altered or tampered with – for instance, converting an innocent image of a child edited into sexually explicit content. Image analysis can also identify images from surveillance systems.
- *Digital sting operations:* In the US, as well as other countries, undercover law enforcement “stings” have long been used to entrap potential child exploiters. However, in many parts of the world, stings are unlawful, and the data produced by sting operations are considered null evidence in courts. Recently, NGO Terre Des Hommes, based in the Netherlands, took the unprecedented step of designing a photo-realistic video avatar of a child to conduct video chats with potential exploiters on chat room sites. Dubbing the operation “Project Sweetie”,⁸ the NGO claimed that over six

months they collected the names and emails of 1,000 people who solicited the avatar. The campaign has been controversially received, with some lauding it as the innovative next step in preventing sexual exploitation of young people, and others raising alarms over privacy infringement issues.

Rights to privacy

My concern with these digital methods’ infringements on privacy rights echoes the protests by groups like the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation,⁹ on the grounds of protecting free speech online and protecting online identities. Many of the innovative techniques that law enforcement must use for thorough digital investigations involve biometric surveillance and identification techniques on proprietary websites. Personal privacy online can be absolutely critical for political dissidents and lesbian, gay, bisexual, transgender and queer (LGBTQ) activists, for example, seeking anonymity to avoid discrimination, harassment or punishment from repressive governments. These groups may see the denial of privacy as a form of political control, and use encrypted websites and email and other dark-web technologies for their own personal safety.

In addition, current digital strategies echo the dominant discourse on victimisation by failing to acknowledge and uphold children’s rights. Many have argued that the UN Convention on the Rights of the Child applies to the internet space: children “shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds.”¹⁰ Unfortunately, in the name of child safety, internet governance legislation and advocates in many countries have chosen to move in the direction of censoring children’s access to social media. While online censorship models vary between countries (e.g. the censorship of “adult pornography” websites where illegal), sometimes censorship may veer too far and limit children’s access to educational and communication sites.

7 www.interpol.int/Crime-areas/Crimes-against-children/Internet-crimes

8 International Federation Terre Des Hommes. (2013). Stop Webcam Child Sex Tourism. www.terredeshommes.org/webcam-child-sex-tourism

9 For example, the Electronic Frontier Foundation, ACLU, and seven other privacy advocacy organisations issued a joint statement in June 2015 expressing concern with governmental facial recognition and face databases. Lynch, J. (2015, 16 June). EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi>

10 United Nations Convention on the Rights of the Child. www.ohchr.org/en/professionalinterest/pages/crc.aspx

Sexuality rights

Concerns over privacy rights and surveillance have strong implications for the upholding of sexual rights. As many ethnographic studies have demonstrated, young people already constantly experiment with new internet platforms for expressing sexuality and desire and conducting relationships. To deny these cultural practices in internet safety education is to deny the reality of healthy youth sexuality and forces sexual practices to become more “invisible” and out of the oversight of guardian communities. Heather Horst¹¹ describes how both US youth in the Digital Youth Project,¹² for example, and Indonesian teenagers in Barendregt¹³ and Boellstorff’s¹⁴ research, experimented and played with their online profile photos and identities in ways that they deemed sexy for their intended audiences, but expressed surprise and bewilderment that these photos could be accessed by people outside their peer groups. Horst indicates that what would be needed in these contexts would be greater education around privacy settings and filters so that youth can better conceptualise that internet sites are potentially permanent and accessible by multiple publics.

Rather than filter and block all content related to sex, sexuality and sexual interactions, internet safety measures must encourage age-appropriate explorations of sexuality for teenaged youth. Especially in countries where state policies limit access to resources and public spaces for LGBT youth, it is imperative that young people have access to digital chat rooms, forums and sites that ensure their safety, community building, and interpersonal growth. Research studies by both Hasinoff¹⁵ and Gray¹⁶ illustrate the perils of sexually repressive policies seeping into moral panics that limit the networking and relationship-building of marginalised youth. A victimisation model furthers the policing of youth sexuality, as young people are literally

punished and criminalised for the distribution of sexually suggestive images. Panics over “sexting” stem from long-standing moral panics over youth sexuality – online or offline – and further the false narrative that young people are innocent, always already victims. A protective model is unsustainable, and ultimately furthers a culture of policing and repression.

Conclusion: Feminist technology design and resisting techno-panics

I am intrigued by the rapid and unprecedented rise in global alliances between law enforcement agencies and technology companies, as well as the forging of cross-border police partnerships, to design cyber crime detection software and to share data. But I am deeply concerned that the current model for anti-trafficking design centres technocratic expertise in the hands of wealthy states and multinational tech companies, at the exclusion of grassroots-level NGOs, activists and youth who have long been organising on issues of exploitation.

A feminist approach means moving toward youth-centric technologies that recognise different forms of expertise in producing sustainable models of safety. For example, Streetwise and Safe’s path-breaking research report¹⁷ on youth engaged in the sex trades provides deeply nuanced insight into young people’s own experiences with safety, consent, victimisation, empowerment and the police. The report is an exemplary resource for a feminist anti-trafficking technology able to recognise young people’s ongoing negotiations of risk and safety. The approach would use this knowledge to create technologies that can more sustainably and accurately – and powerfully – end abuse and exploitation.

A feminist design approach values all relevant forms of expertise and input in understanding what “sex trafficking” and “technology” mean in the lived experiences of young people; child protection services; sex workers aiming to end exploitation without punishing prostitution itself; survivors of trafficking, forced migration and human smuggling; and advocates for free speech and network neutrality and against censorship. A feminist design approach, emphasising harm reduction rather than policing, would be more effective because it takes into account the forms of structural violence

11 Horst, H. (n/d). Commentary on Bart Barendregt’s *Between m-governance and mobile anarchies: Pornoaksi and the fear of new media in present day Indonesia*. www.media-anthropology.net/horst_comment.pdf

12 Ito, M., et al. (2008). *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*. Chicago: MacArthur Foundation.

13 Barendregt, B. (2006). *Between m-governance and mobile anarchies: Pornoaksi and the fear of new media in present day Indonesia*. www.media-anthropology.net/barendregt_mgovernance.pdf.

14 Boellstorff, T. (2005). *The Gay Archipelago: Sexuality and Nation in Indonesia*. Princeton: Princeton University Press.

15 Hasinoff, A. A. (2014). *Sexting Panic: Rethinking Criminalisation, Privacy, and Consent*. Champagne, IL: University of Illinois Press.

16 Gray, M. (2009). *Out in the Country: Youth, Media, and Queer Visibility in Rural America*. New York: NYU Press.

17 Dank, M., et al. (2015). *Surviving the Streets of New York: Experiences of LGBTQ Youth, YMSM, and YSW Engaged in Survival Sex*. New York: Urban Institute, with Streetwise and Safe NYC.

– global poverty, rape culture, racism, labour exploitation, restrictive and dangerous immigration policies – that make online child exploitation and trafficking a reality in the first place.

The common narrative spun by many children’s advocacy organisations about child exploitation online frames the internet as a space of risk, vulnerability, harm and entrapment. The narrative usually goes like this: exploiters can use various digital platforms to locate, communicate with and groom victims; send text messages and email to conduct their affairs; use various financial transaction sites to conduct monetary exchanges; and trade and distribute photos and videos of trafficked or exploited victims. Such a narrative frames young people as the passive recipients of harm, rather than active agents who already engage in risk mitigation

and rely on each other for support networks online. I urge child safety specialists to think through online safety in a pragmatic manner that respects the vast benefits and opportunities of internet connectivity and to avoid “techno-panics” by focusing instead on harm-reduction approaches to youth safety. Many global feminist internet activists have organised against misogynistic, homophobic and racist harassment online; government interpretations of these issues could certainly take note from this legacy of grassroots organising in addressing sexual exploitation and violence in the digital space. In a sense, online sex trafficking and exploitation only magnify existing structural violence and social inequities. Sustainable problem solving therefore means resisting a “quick-fix” technological solution to a problem that is so much more than digital.

Sexual rights and the internet

The theme for this edition of Global Information Society Watch (GISWatch) is sexual rights and the online world. The eight thematic reports introduce the theme from different perspectives, including the global policy landscape for sexual rights and the internet, the privatisation of spaces for free expression and engagement, the need to create a feminist internet, how to think about children and their vulnerabilities online, and consent and pornography online.

These thematic reports frame the 57 country reports that follow. The topics of the country reports are diverse, ranging from the challenges and possibilities that the internet offers lesbian, gay, bisexual, transgender and queer (LGBTQ) communities, to the active role of religious, cultural and patriarchal establishments in suppressing sexual rights, such as same-sex marriage and the right to legal abortion, to the rights of sex workers, violence against women online, and sex education in schools. Each country report includes a list of action steps for future advocacy.

The timing of this publication is critical: many across the globe are denied their sexual rights, some facing direct persecution for their sexuality (in several countries, homosexuality is a crime). While these reports seem to indicate that the internet does help in the expression and defence of sexual rights, they also show that in some contexts this potential is under threat – whether through the active use of the internet by conservative and reactionary groups, or through threats of harassment and violence.

The reports suggest that a radical revisiting of policy, legislation and practice is needed in many contexts to protect and promote the possibilities of the internet for ensuring that sexual rights are realised all over the world.

GLOBAL INFORMATION SOCIETY WATCH

2015 Report

www.GISWatch.org



APC

Hivos