Author

Hera Hussain, [illegible]

[illegible] 30 [illegible] 30, [illegible] 35 [illegible] 2020 [illegible]

B [illegible] : F [illegible] D

Overview: This document presents the summaries of ten seminal resources related to business and technology’s interaction with technology-facilis7 /P /Lang (en-US)/MCID 22 BDC

Lack of diversity of product teams and leadership, as well as a lack of prioritisation of the increased harm faced by women and marginalised genders, and those that find themselves at the intersections of multiple oppressions, has resulted in products, policies, and services that are unsafe and put survivors of gender-based violence (GBV) at risk. In many cases, the technology itself is a cause of trauma or re-traumatisation despite repeated claims that “technology is neutral and it’s how people use it” which dismisses the issue as a sociological or user based problem. One clear example, included in this review, of how harms to women have been ignored is shown in Slupska’s research on IoT “smart” home security devices. Her research shows that out of 40 cybersecurity papers reviewed, only one article mentions domestic violence, a harm that largely affects women. This absence of women or feminist approaches to cybersecurity cuts across all technology and is highly problematic for the safety of women and marginalised groups.

Despite the increasing coverage of technology-facilitated gender-based violence (TF GBV) in media, public policy and academia, the market prioritisation and business incentives have changed little. There is however, a growing resd m0growing

B P

T a a-i f ed de ig ackle ech l g -facili a ed ge de -ba ed i le ce, 2022 Chayn

Summary: The trauma-informed design principles were created by Chayn based on their work on gender-based violence, especially tech abuse. These were applied and further crafted through the Orbits project where Chayn and End Cyber Abuse, consulted technologists, activists, survivors, academics and designers globally on the principles and how they can be applied to technology-facilitated abuse.

Design principle	Application
Safety Making brave and bold choices that prioritise the physical and emotional safety of people.	• 2 Factor Authentication • Sharing last known logins and locations • Permitting third party reporting (with informed consent from survivor) • Reporting to platforms for offline behaviour of users • Safety exit button on websites. To support emotional safety, consider redirecting to something comforting instead • Allowing users to opt for disguised emails with fake subject lines, like Chayn's mini-course platform Soul Medicine • Blocking and filtering content and users
Agency Honouring the survivor's wishes to create affirming experiences. This requires seeking informed consent at every step and providing information, community, and material support to survivors.	• Allowing people to access essential information without having to create accounts • Giving an option of what information is kept public and private, such as full names and location • Actively asking survivors for their consent in sharing information with other agencies and individuals within the organisation, and being clear with survivors about how and why their information is being shared.
Equity Designing for inclusion must consider how position, identity, vulnerabilities, experiences, knowledge, and skills shape trauma and recovery. Survivors are not a homogenous group.	•

Privacy Securing a survivor's personal information, such as data, images, videos, statements, and their trauma story must be kept secure and undisclosed, unless the survivor decides otherwise. Also ensuring frictionless access to help and information.	• Clearly indicating what data is publicly accessible and what isn't • Automatic disabling of cookies and tracking when survivors report abuse on platforms • Using end-to-end encrypted technology and exploring the use of privacy-enhancing technologies (PET) such as encryption and data masking • Withholding survivors' details with the perpetrator during any punitive actions taken • Providing survivors with a digital file of evidence that can support civil and criminal cases, if they want to pursue those routes
Accountability Maintaining a relationship of trust includes being open and consistent about what is being done, how, and why; we must create and nourish constructive feedback loops that trigger change	• Providing clear ways to help survivors identify in-platform reporting mechanisms such as quick access bars for reporting abuse • Acknowledging gaps in knowledge or foresight which can contribute to harmful features • Being consistent and predictable in product design - by providing structure and routine • Committing to long-term systemic change, rather than reacting to scandals and infrequent public outrage
Plurality Actively leaving space for complexity and recognising harm manifests in different and disproportionate ways for people living at the intersection of multiple oppression.	• Training moderators to understand cultural context • Refraining from assuming which language is spoken based on location • Offering ways for people to customise their journey on product • Training staff on the impact of additional vulnerabilities, such as caste, race, religion, sexual orientation, and disabilities • In complaint processes, it should be possible for survivors to identify multiple offences, including offline ones
Power sharing Distributing and sharing power by co-designing interventions with survivors.	• Giving survivors decision-making power in tech companies through compensated board or committee positions (only with survivors informed consent and respect for their confidentiality) • For global firms, using local teams and networks to gather ideas for ways to improve services across the globe • Creating community-owned models and practices for governance and evaluation • Translating and localising content and policies
Hope Creating validating, empathetic, warm, and soothing experiences, motivating people to seek and embrace the help on offer. We should seek collaborative solutions	

The full report can be seen ____.

Da a hee f Da a e

The following table covers some applications of the principles of trauma-informed care.

Area	Topic	Example Good Practice
UX Research & Design	User Research User Interface Design Usability Assessment	• Carefully consider how user research can be retraumatizing and work to minimize potential harm. ["seek ways to avoid retraumatization"] • Conduct user studies in a place where participant feel safe and familiar [safety, trust] • Consider involving survivors in the research process [collaboration, enablement] • Draw inspiration inspiration from trauma-informed design principles in other environments such as physical spaces [saftey, trust] • Create, publish, and encourage reuse of trauma-informed design patterns

Th ea M deli g I i a e Pa e Vi le ce: Tech Ab e a a C be eo i Challe ge i he I e e f Thi g , 2021Julia Slupska and Leonie Maria Tanczer

Summary: Current cybersecurity literature is almost entirely blind to intimate partner violence (IPV). This paper

By using a smart lock system as a case study, they present a model for technology companies to identify IPV threats and create design changes that reduce the likelihood of harm based on the threat model. The following is a table of mitigative strategies.

Ownership-based compromise	**Restricting ownership:** Company having a protocol which allows them to remove owner access when abused (e.g domestic abuse)
	Equalising account holder rights: Multiple account owners, allowing distribution of power.
	Consent changes: Shared devices should require all associated users to consent to fundamental changes.
	Customer-facing staff guidance: Supporting staff to identify how to assist users in instances of disputes around who is a legitimate account holder.
Smartphone compromise	**Automatic logouts:** Periodic logging out of users from accounts, prompting re-authentication when using a smartphone to lock/unlock smart locks.
	Report-theft feature: A web-based feature to report theft or takeover of devices.
Account compromise	**Register of login details:** Vague, innocuous-looking regular notifications of login locations and timestamps.
	New login prompts: Notifications to an account whenever an IoT device login is attempted.
	Change of password prompts: Requirement of new login across all devices if a user changes password.
	Reinstate account ownership: Reinstate access to compromised accounts through time-stamped backups so survivors can access and control their data.
	Multi-factor authentication: Multi-authentication methods so accounts are less vulnerable to password coercion.
	Transparency around privileges: Users on lower authorization levels should receive frequent reminders of the different access & power other Accounts have.
	Access trials: Notification to all users of account holders checking critical settings such as access logs.
Smart lock compromise	**Factory reset:** Simple activation from inside home Wi-Fi network to reset a IoT device to its original state, enabling survivors to restrict access after a threat.
	Logs: Access logs (who, when, where) should not be subject to changes and edits.
	Disable functionalities: Users should be able to disable functionalities e.g remote closing/ unlocking of a door.
System compromise	**Connection reminders:** Regular reminders of which IoT devices are connected and which user accounts have access to them.
	Opt-out: Allowing opt-out of certain data collection which aren't essential to the functionality.
	Actionable advice: Tailored company guidance for survivors on steps to follow if they are facing domestic abuse or harassment.

Read more ____.

No Excuse for Abuse, PEN America

Summary: PEN America’s report presents a mix of proactive, reactive and accountability measures to tackle online abuse. Recommendations are from the experiences and needs of writers and journalists who identify as women, BIPOC, LGBTQIA+, and as members of religious or ethnic minorities.

Empowering Targeted Users And Their Allies	
Proactive Measures: Reducing Risk And Exposure	• Allowing proactive filtering of content by users and their allies • Enhanced safety modes and visibility snapshots • Delegate account access to trusted allies
Reactive Measures: Facilitating Response And Alleviating Harm	• Access to emergency support from the platform • Features to automate quick documentation of abuse • Improve blocking, muting and restricting engagement and content from abusers • Make reporting user-friendly and trauma-informed by ensuring clarity, consistency and allow bulk reporting • Support third-party tools designed to counter online abuse—especially those built by and for women, BIPOC, and LGBTQIA+ technologists

Disarming Abusive Users	
Accountability Measure	• Make rules and repercussions clear and easily accessible in real time from directly within the main website • Establish a transparent system of escalating penalties for abuse including warnings, strikes, temporary functionality limitations, suspensions, content takedowns and account bans. • Proactive nudges to encourage users to rethink abusive content before they post it. • Improve the appeals process for users subjected to content or accounts taken downs, restriction, or suspensions.

F

Da a Fe i i, by Catherine D’Ignazio and Lauren Klein

Summary: Data feminism presents 7 principles for how data science, and data scientists can be used for good and not participate and perpetuate systems of oppression.

Examine power. Data feminism begins by analyzing how power operates in the world.

Challenge power. Data feminism commits to challenging unequal power structures and working toward justice.

Elevate emotion and embodiment. Data feminism teaches us to value multiple forms of knowledge, including the knowledge that comes from people as living, feeling bodies in the world.

Rethink binaries and hierarchies. Data feminism requires us to challenge the gender binary, along with other systems of counting and classification that perpetuate oppression.

Embrace pluralism. Data feminism insists that the most complete knowledge comes from synthesizing multiple perspectives, with priority given to local, Indigenous, and experiential ways of knowing.

Consider context. Data feminism asserts that data are not neutral or objective. They are the products of unequal social relations, and this context is essential for conducting accurate, ethical analysis.

Make labor visible.

C e f l Tech

Summary: The FRIES (Freely given; Reversible; Informed; Enthusiastic; Specific) model became an accessible way to talk to young people about bodily autonomy and consent. It goes beyond “No means no” which, while powerful, doesn’t offer an alternative to what consent can look like. The Consentful tech project proposes we use this framework and apply it to technology design as well.

T a d Ab abili T lki, Angelika Strohmayer, Julia Slupska, Rosanna Bellini, Gina Neff, Lynne Coventry, Tara Hairston, Adam Dodge

Summary:
This toolkit is a collection of resources which includes the following:

- Recommendations for gender-based violence advocates in supporting survivors of technology-mediated abuse and for engaging with technology companies to improve their services
- Advice for technology companies and researchers wanting to implement safety features that better support survivors and proactively engaging with perpetrators
- Abusability and the secure systems development life cycle provides an outline for a development life cycle that takes peoples’ safety into consideration
- A self-evaluation tool for technology companies of how mature their features are in relation to the safety

Where scholarship diverges

There are very few points of divergence in these papers which could signal that the feminist technology sector is both small, and arising as a response to issues identified from grassroots movements. The differences arise out of the expertise of the authors and the “lens” they employ in examining tech abuse.

- Most papers depict domestic and sexual violence within family or intimate settings. With the growing concern around incel communities, there is a critical need to also consider how to address the risks of coordinated group attacks that are gender or identity motivated.
- While the literature does highlight different approaches to tech between Majority and Minority worlds, content moderation and policies focus on the experiences of wealthy nations. This means survivors in the Global South are at a greater disadvantage as often the support options available to them are in the form of therapeutic and law enforcement support and are limited.
- Law enforcement and criminal justice systems appear in many papers but there was a lack of in-depth acknowledgement considering the complex factors such as lack of awareness amongst legal systems and enforcement, systemic injustice, and cross-national crimes which means presenting this as the only way of getting justice for survivors misses out on all the reasons why survivors may not choose to do that. In many jurisdictions where trust in policing is low, survivors may prefer to get support and accountability from the technology companies themselves or other civic actors.
- Design discussions often focus on harm reduction and accountability but a more holistic approach must also include healing justice.
- Some papers mention the need for end-to-end encryption and PETs, while others don’t. There seems to be a lack of consensus around this and it should be further explored.