Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices:

Implementation Summary

March 2023

Creating a pathway along which tech, innovation and GBV/HP practitioners can meet

This is the short version of forthcoming guidance that will be comprehensive and refer to work at the intersection of gender-based violence (GBV) and harmful practices (HP), data and technology. This summary document is a brief overview of the opportunities, risks and insights relating to potential steps towards creating safe and ethical technology that supports existing GBV/HP programming. In recognition of the continuous advance of technology, the authors encourage use-case feedback that will allow the document to evolve. Both this document and the longer comprehensive guidance will be reviewed on an ongoing basis, in order that they remain applicable to emerging technologies and their associated risks.

Acknowledgements

This report was jointly produced by the UNFPA Technical Division, Gender and Human Rights Branch and Humanitarian Response Division, under the technical leadership of Alexandra Robinson and Kate Rougvie. The primary author is Stephanie Mikkelson, with support and review from Nora Piay-Fernandez.

The authors gratefully acknowledge the guidance and inputs provided by UNFPA Information Technology Solution Office as well as Mar Jubero, Emily Krasnor, Emily Springer and Sarah Katherine Baird.

The comprehensive guidance, which this report summarizes, was also developed with review and feedback from a number of key experts who volunteered their time in finalizing this important contribution to keeping women and girls safe in all spaces. Contributing experts and organizations include: Australia's eSafety Commissioner, the Gender-based Violence in Emergencies team at the United Nations Children's Fund (UNICEF), the International Rescue Committee (IRC), the International Telecommunication Union (ITU), the MediCapt team at Physicians for Human Rights, Oxfam, Pollicy, the United States Department of State Secretary's Office of Global Women's Issues, the United Nations High Commissioner for Refugees (UNHCR), Linda Raftree, Liz Dartnall and Revi Sterling.

Special thanks are extended to the editor of this report, Scriptoria, and to the graphic designer, Eneida Déchery at REC Design.

Cover photo: UNFPA

UNFPA, 2023. *Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary*. New York.

I. Introduction

We are at a turning point in time. The digital revolution is here and getting stronger by the minute. At the same time, movement restrictions of the COVID-19 pandemic, and its associated shadow pandemic, have prevented access to services and escape from violence. Since these pandemics, there has been an increased appetite for tech solutions designed to enhance access to information and services for survivors of gender-based violence (GBV) and harmful practices (HP).[1] Yet, this proliferation of technology is largely unregulated from a "do no harm" perspective. Therefore, despite its creators' good intentions, it can create additional spaces where women are at risk of harm.

There are enormous benefits in bringing technology to GBV/HP programming, but there can also be significant harms. Technology has the potential to create participatory interactions and reduce bias in decision-making processes, but it may also unintentionally do the opposite – by increasing bias and embedding intersectional forms of discrimination and oppression (e.g. inequality based on gender and/or ethnicity) into decision-making solutions for generations. Technology also has the potential to provide GBV/HP services to survivors who would not otherwise have had access, but it may also be a primary risk factor for increased violence within the home or virtually. Technology can therefore both decrease *and* increase risks of direct GBV simultaneously, if not implemented with caution.

Modern technology has been built on the infamous motto "move fast and break things". The idea of innovation, iteration, trying and testing, and building prototypes and minimum viable products as quickly as possible in order to see "what sticks" is viewed as an ideal environment for business, particularly where there is a heavy reliance on self-regulation. In such an environment, the consideration of ethics, safety and privacy slows things down, making it much more difficult to "move fast". It is not commonly understood that "moving fast" often comes at the cost of compromised ethics and safety.

The tech motto "move fast and break things" is in direct contradiction with the guiding principle of design in GBV/HP interventions, which is "do no harm". Despite this, one of today's leading social media companies, with about 3 billion users, held the former as their official company motto until 2014. Although the motto has since changed, this agile "lean startup" mentality lives on, particularly in innovation spaces.

There is nothing inherently wrong with the "move fast and break things" or "lean startup" concepts. But if they come at a social cost – such as compromising the safety of women and girls – alternative approaches must be incorporated. **Combining a "move fast and break things" mentality – iterative trial and error – with participatory methods or human-centred design provides a useful meeting point.** This combination provides the means for a community, frontline service provider or GBV survivor advocate, to quickly and safely discover new ideas and fresh approaches to problems.

Tech, innovation, GBV/HP practitioners cannot allow safety to be sidelined, especially when building digital interventions for GBV/HP programming. **It is essential that ethics, safety and privacy are baked into GBV/HP tech-based interventions from the outset, and are maintained throughout each intervention.** The goal of this guide is to create a pathway along which tech, innovation, GBV/HP practitioners can safely meet.

---

1 All references to gender-based violence (GBV) throughout this guidance include harmful practices (HP) and are together abbreviated as GBV/HP for ease of reading.

The three most important things to keep in mind when considering the intersection of GBV/HP data and technology are:

1. Understand the gaps

Gaps between tech and GBV/HP fields are wide.[2] Understanding these gaps is particularly important when considering models of cybersecurity threats utilized by the tech world. These models often do not incorporate intimate partners and oppressive groups or individuals; however, these actors are central to the principles of survivor-centred GBV/HP programming. In addition, anyone who collects GBV/HP data has a responsibility to protect it, and this is not understood equally among the fields of tech and GBV/HP response.

2. Data really matters!

Any data associated with GBV/HP is categorically "sensitive" because if an individual or group were identified, this could be life-threatening. Not knowing explicitly what data you are collecting, how it is being stored, for how long, or who has (intentional or unintentional) access to it puts everyone involved at risk of harm.

3. Security ≠ safety

No matter how strong the security system, no data is 100 per cent safe. GBV data, in particular, is highly sensitive and if accessed can be used to name, shame, blame and even harass or re-offend survivors. Therefore, all of us have a responsibility to understand risks, and to do everything possible to prevent and mitigate these risks – either by choosing not to go forward with a project or by moving forward cautiously.

A. Objectives

The four main objectives of this summary guidance are to:

- Increase awareness of the **potential benefits** and options that tech-based interventions could bring to GBV/HP programming.
- Increase understanding of potential **harm and misuse**, and reduce risks associated with GBV/HP tech-based interventions.
- Provide a **shared framework** for consistent standards and oversight.
- Outline a GBV/HP **digital intervention process** with considerations, steps and tools.

B. Intended audience

This guidance is intended for practitioners who are considering, building or adapting a tech-based intervention for GBV/HP programming. It was written with a particular focus on GBV programme practitioners in any setting, be it development, peace or humanitarian.

Additionally, this guidance is applicable for data science projects, donors or other stakeholders working at the intersection of gender, data and technology.

2 Women hold only 25 per cent of all computer occupations in the United States, as opposed to 72 per cent of counselling psychologists and 64 per cent of all social scientist occupations (United States 2019 Census). Women also make up less than 35 per cent of all employees in the five largest tech companies: Amazon, Facebook, Apple, Google, Microsoft – ordered by percentage of female employees (Statista study on women's representation in big tech).

II. Principles

This guidance has been written around six core GBV principles, with 10 additional data-specific principles.[3] Special attention has been given to all of these principles due to the categorically sensitive nature of data associated with GBV programming.

Data-specific principles should not be limited to personal data, but considered for all data related to GBV programming. Indeed, any association with GBV is categorically sensitive and demands the highest level of consideration.

GBV core principles include:

- **Do no harm**
- **Survivor-centred approach**[4]
- **Informed consent and transparency**
- **Participatory approaches**
- **Rights-based approach**
- **Advance gender equality**

Building upon this foundation, data-specific principles add another layer of ethical considerations for the collection, processing, and use of data for GBV/HP programming:

- **Safety by design**
- **Purpose limitation**
- **Data minimization**
- **Proper use of data**
- **Fairness**
- **Informed consent, transparency and ownership**
- **Accuracy and data quality**
- **Security: integrity, confidentiality and availability**
- **Accountability**
- **Unconditional service**

---

3 These principles are a combination of best practices and global minimum standards across GBV, gender-based violence in emergencies (GBViE), violence against women (VAW), health, data, and digital development. In particular, they are derived from United Nations Sustainable Development Group guidance on data privacy, ethics and protection, General Data Protection Regulation, GBViE minimum standards, VAW essential services package, Open Data Institute paper on data ethics, World Health Organization report on putting women first, World Medical Association Declaration of Helsinki, United States Violence Against Women Act, and International Committee of the Red Cross Professional Standards for Protection Work. The full description of each principle can be found in UNFPA's forthcoming comprehensive guidance on the safe and ethical use of technology to address gender-based violence and harmful practices.

4 Safety, confidentiality, respect and non-discrimination.

III. Potential benefits

Technology not only has the ability to increase access to and improve the quality of GBV/HP services and information, but also to facilitate more participatory decisions with less bias, as well as contribute to closing the "gender digital divide". For better or worse, technology and data science solutions can be robust tools to combat rapidly rising rates of technology-facilitated GBV (TF GBV), ultimately ensuring better and safer tech for tomorrow. That said, technology should never be seen as a stand-alone solution. Instead, it is a powerful tool that has the potential to support a programme intervention already grounded by, or supporting, a larger programme or GBV/HP prevention or responses initiative.

Technology has the potential to support and strengthen GBV/HP programming through:

Increasing access to services. Technology can be a tool which survivors of GBV/HP can use to access services and information when they are otherwise unable to physically reach services, or are hesitant about doing so. Examples include remote-service delivery interventions such as hotlines or self-help service delivery applications.

Amplifying positive social norms. Digital interventions can be used to positively influence and transform harmful social and gender norms to dismantle harmful practices such as female genital mutilation, child marriage and son preference/daughter aversion. Positive messaging can be shared with stand-alone digital interventions or can potentially be integrated into existing platforms that do not collect personal data.[5]

Facilitating service delivery and enhancing quality. Technology and digital solutions have the potential to improve remote or in-person service delivery and quality. This includes digital case management that enables rapid responses and real-time data; workflows that guide service providers through customer interactions; platforms that facilitate support groups; and simplified reporting to management or donors, among others.

5 Ensure that risks are well understood and mitigated particularly when working with any platform, including most mainstream social media platforms, which use personal data and user interactions for profit.

Streamlining research, and increasing robust evidence, findings and insights. Digital solutions have the ability to streamline data collection and research analysis, increase evidence at desired levels of disaggregation, and collect real-time data about GBV/HP while decreasing bias and allowing for even more participatory results.

Increasing gender equality and closing the gender digital divide. Creating digital interventions for GBV/HP programming results in tech products focused on women and girls' experiences, cultivating them as key users and closing the gender digital divide.

Increasing our future ability to create better tech for GBV/HP programming. As more GBV/HP tech-based solutions are built and deployed, our collective ability to understand how to create innovative tech solutions will grow, and we will then create better tech for GBV/HP programming in the future.

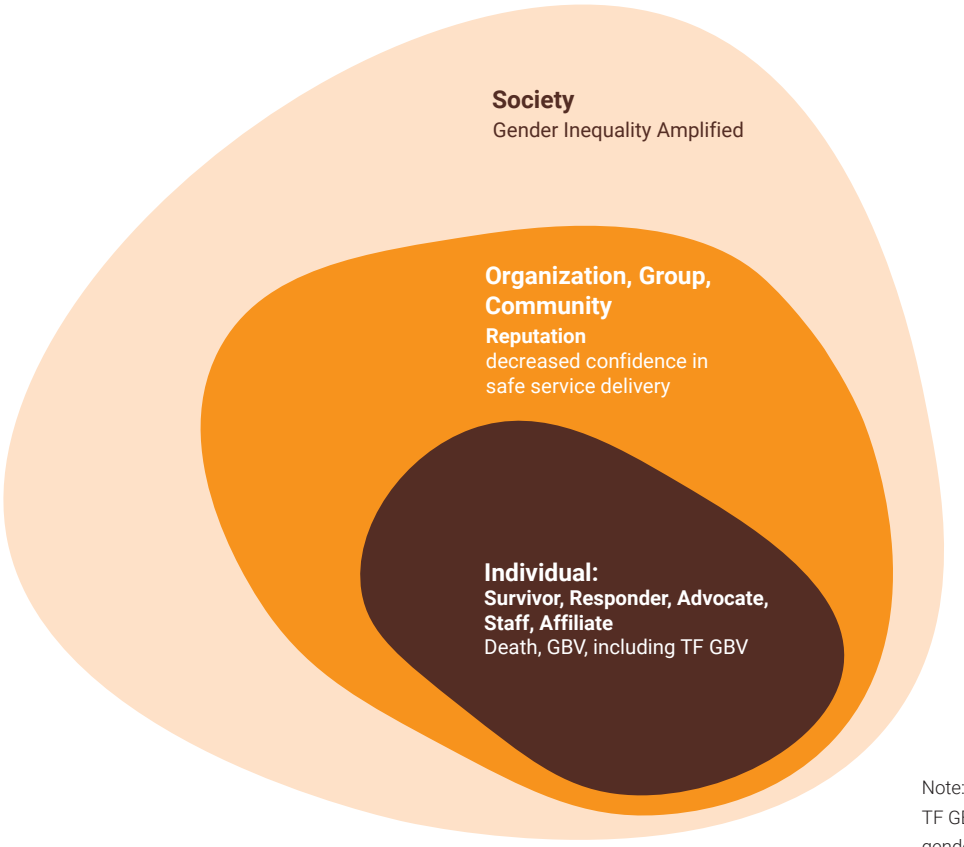
Combating technology-facilitated GBV. Technology will be a part of the solution to TF GBV. It will require a combination of better and safer technology from the start, survivor-centred mitigative digital solutions, and an increase in users' digital safety to combat TF GBV, in addition to supportive law and policies.

Finally, it is important to note that by creating more inclusive technology solutions and safe spaces for women, girls and others disproportionately affected by GBV/HP, we iteratively showcase how to create better and safer tech, even for those outside of GBV/HP programming.

IV.
Risks and harms

Technology has the potential to transform the effectiveness of GBV/HP programming, but as with any intervention, this does not come without risk. Once data is collected (digital or analogue), **there is no absolute safe solution for that data** – particularly if it is sensitive and/or GBV-related.

In order to build safe digital interventions, it is **crucial to understand the full spectrum of risks** for an individual, community and society, as well as to understand gaps in security and how these are created. In Figure 1 below, we encourage tech, innovation, and GBV/HP practitioners to consider the potential risks of digital interventions with a socio-ecological model.



Note: GBV = gender-based violence; TF GBV = technology-facilitated gender-based violence

Figure 1.
Framework of risk

It is **critical to understand threats from various actors – from high-risk malicious actors to mission-driven and "neutral" actors**. When assessing risk, especially with sensitive GBV-related data, we must consider how malicious, negligent and accidental actors may behave and also understand that no matter their intention, the same harmful outcome could result. All actors in Figure 2 below, whether consciously deciding to act inappropriately or not, motivated by harm or not, is irrelevant once privacy is breached and personal information is forever on the dark web, for example.

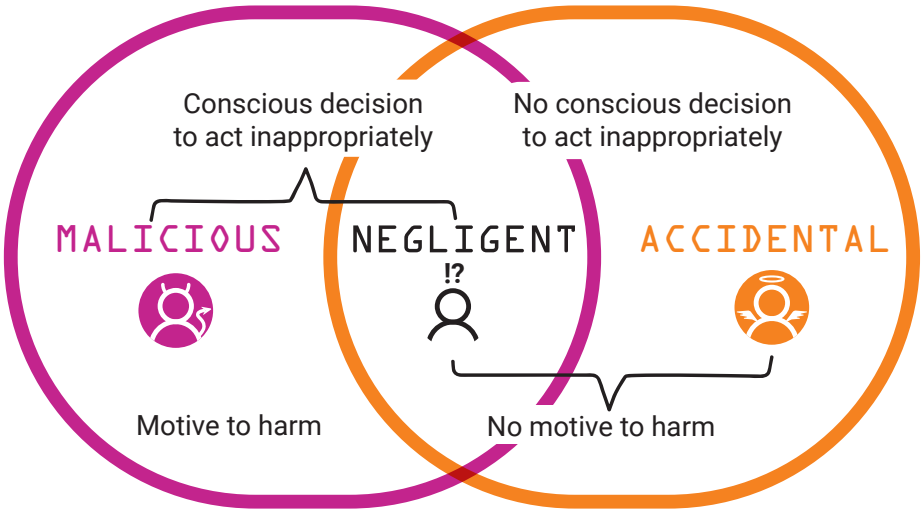


Figure 2.
Types of actors

There will always be a risk that if someone is determined enough, they will find a way to access data; remember **security ≠ safety**. It's our job to minimize this risk by safeguarding GBV/HP data, or eliminating risk by not collecting data at all. We need to work to **understand the gaps between GBV/HP and tech fields** so that we are better able to work collaboratively. For example, GBV/HP practitioners may want to focus on user consent and data privacy, while tech professionals may want to focus on criminal and justice system uses of data, if accessed in ways that may be extremely harmful, emotionally and physically, to survivors. In reference to Figure 3, the threat actor mapping, GBV/HP practitioners will likely be most comfortable focusing on intimate partners, whereas cybersecurity experts may be more accustomed to designing solutions that prevent hacking from financially motivated malicious actors.

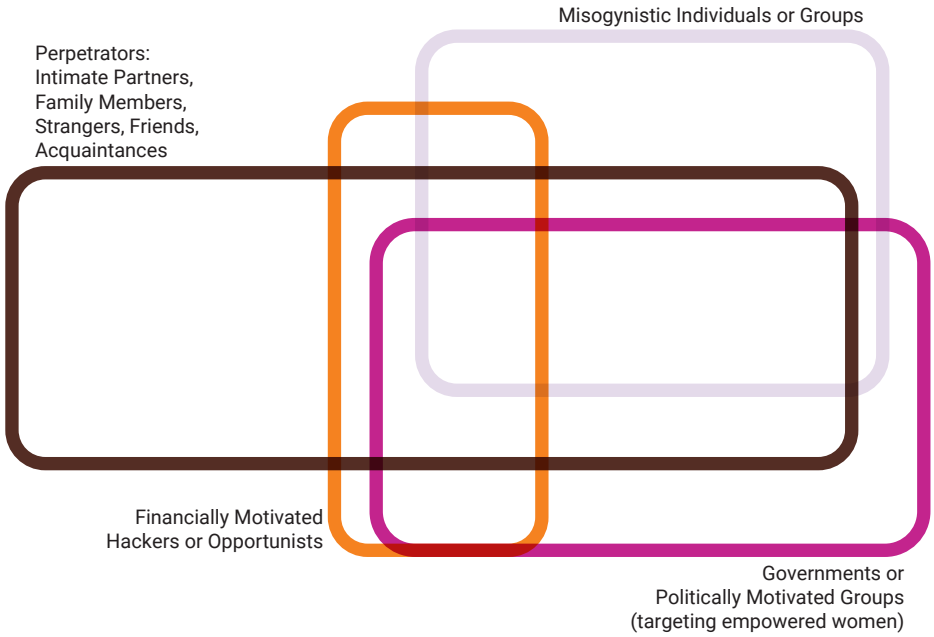


Figure 3.
Threat actor mapping: malicious actors

V.
Steps for practitioners working on GBV/ HP and tech

The framework shown in Figure 4 was developed to outline how GBV/HP and tech professionals can collaborate. It divides the GBV/HP digital intervention process into four phases (Scoping/Feasibility, Design, Implementation, Lifetime) consisting of 17 steps with suggested actions, outputs, reminders and key things to consider along the way.6

Scoping/Feasibility (Steps 1 and 2) ensures that a project has a solid and realistic foundation for successful impact. Design (Steps 3–16) consists of collecting user needs, and functional and technical specifications, and building the solution to spec. Implementation (Step 17) launches the solution, and Lifetime (the final phase) works through how to achieve long-term sustainability and ongoing maintenance.

In addition to the 17 steps outlined in Figure 4, there are six underlying considerations that must be integrated throughout the entire process in order to meet global ethical and safety standards. These considerations include:

Do no harm

User integration/participatory approaches

Use and accessibility

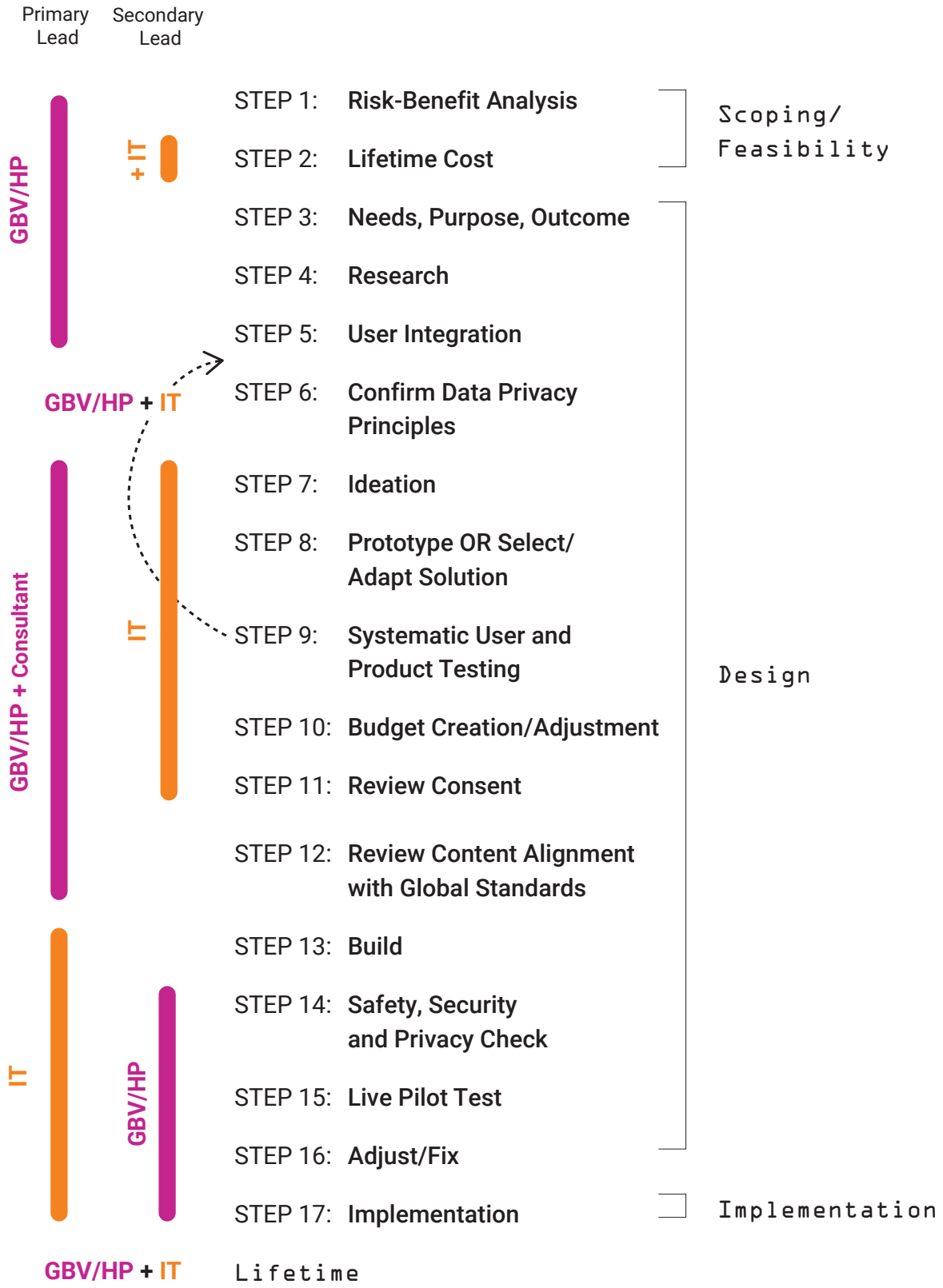
Safeguarding/ managing risk

Data analysis

Consent

For more details on each of the four phases and 17 steps, please see annex A: Checklist: essential considerations (Scoping/Design/Launch/Lifetime).

6 A detailed description of every step is included in the forthcoming comprehensive guidance.



Note: GBV = gender-based violence;
IT = information technology

Figure 4.
Steps for practitioners working on GBV/HP and tech

Annex A: Checklist: essential considerations (Scoping/Design/Launch/Lifetime)

CONSIDERATIONS

incorporated throughout the process:

- **Do no harm** – actively assess and decrease risk of harm.
- **User integration and participatory approaches.**
  - Solution idea originates from intended user.
  - Safety and security consultations carried out with users and community – community mapping, digital safety mapping, including technology-facilitated gender-based violence (TF GBV).
- **Use and accessibility** – consider differences in use and access based on: gender (social disapproval, fear of harassment etc.), literacy level (reading and writing), digital literacy (comfort and ability to use digital), connectivity (broadband access, cost of device and data), socioeconomic status, disability status, race and ethnicity, age.
- **Safeguarding/managing risk** – consider risks and ways of mitigating risks throughout the process (strongly consider intimate partner and oppressive group threats).
- **Data analysis** – create a data analysis plan based on sound methodology, with data storage and use planned from a project's onset and throughout its lifetime (including data destruction).
- **Consent** – consider the challenges involved in gaining informed and affirmative consent, and how an intervention can integrate consent throughout its design.

SCOPING/FEASIBILITY

1. **Risk–benefit assessment** – consider risks, mitigative strategies, harms and benefits.
2. **Lifetime cost** – consider the needs of a realistic timeline, budget and capacity.

DESIGN

3. **Clearly identify needs, purpose and outcome.**
4. **Complete research** with participatory and human-centred mixed methods (possible outputs: risk assessment, ICT assessment, digital ecosystem mapping, GBV/HP mapping, notes on possible user profiles/ personas, desk review report).
5. **User integration and participatory approaches** – create research-based user experience profiles including diverse digital preferences and behaviours (possible outputs: user profiles, user personas and experience profiles).

- **Use and accessibility** – design strategies, features and solutions to overcome context- and user-specific barriers to use and access (low literacy, poor connectivity, cost of data, cost of device, social disapproval of ICT, limited device functionality, non-email users etc.).
- **Safeguarding/managing risk** – create strategies and features to overcome and mitigate risks (e.g. multi-user login, discrete app icons, establish communication codes with users) .

6. **Data privacy principles** – review UNFPA/ United Nations Children's Fund (UNICEF) Data Protection Policy, United Nations Data Privacy Principles and country or regional data protection laws, and extend to meet context- or user-specific protections. Do not override consent (possible outputs: privacy principles that are specific to the intervention).

- **Data analysis** - Ensure that a data plan for analysis and use is in place.

7. **Ideation** – identify research-backed ideas with the collaboration of women and girls (possible outputs: draft user journey, workflow map, logic model, notes on functional requirements).

8. **Prototype** OR select/adapt product/platform – build a basic model of the idea and check against researched user profiles[7] (possible outputs: prototypes, user journeys, mock-up(s), wireframe, sketches/ drawings).

9. **Systematic user and product testing** – safely test an intervention early and often to ensure feedback is incorporated into the solution including safety feedback (possible outputs: user and product testing results and reports).

10. **Budget creation/adjustment** – create a full detailed budget based on an intervention, and adjust the initial lifetime cost as necessary.

11. **Consent** – check how the intervention has designed informed and affirmative consent: what is being shared, with whom and how?

12. **Content alignment with global standards** – check if content and process are aligned with globally endorsed standards for GBV/HP.

13. **Build** – build interventions based on user profiles, user journeys, workflow maps, mock-ups or interface designs, safeguarding features and consent specifications.

14. **Safety, security and privacy** – check that safety, security and privacy have been integrated throughout the digital development process, and reassess before piloting if not.

15. **Live pilot/test launch** – safely test an intervention with a limited number of real end users over an extended period of time.

16. **Adjust/fix** – make adjustments to an intervention based on pilot findings.

IMPLEMENTATION

17. **Implementation** – at this time, the product is ready for deployment and can go live. This is when end users begin using the product in real time, with many steps involved for a successful launch.

- Create **implementation team** – identify roles and responsibilities.
- Assess and create new or adjusted **policies and procedures**, if necessary.
- Conduct **trainings** – for staff and users (including on security, data privacy and TF GBV).
- **Sensitize the community**, if necessary.
- **Launch** a product and conduct **phased roll out.**
- Conduct **ongoing safeguarding** (especially against TF GBV).

LIFETIME

- Ensure **end user support** (feedback, complaints, system errors, 24/7 technical support, ongoing training, support for editing or deleting personal data).
- Ensure **product owner responsibilities** are planned (oversight and security, technical maintenance, ongoing content alignment).
- Ensure **monitoring and follow up** procedures are in place

7 "User profiles" are examples of different types of users, based on research conducted in the Scoping and Design phases. User profiles are outputs of Step 5 in the forthcoming comprehensive guidance.

Annex B: Digital intervention essentials to tackle GBV/HP: dos and don'ts

HARMS AND RISKS

- Do understand the **full range of harms and risks** before beginning to develop a digital intervention in partnership with programme partners and stakeholders (to determine whether tech is the right solution).
- Do consider and integrate **user safety throughout** the development of a digital intervention.
- **Don't assume that other people, including the tech designer, will consider user safety** (user data in particular). The issue is complex and requires that everyone apply the considerations described here in order for safety to be maximized.

UNDERSTANDING USERS/ PARTICIPATORY APPROACHES

- Do understand various user needs on the basis of gender and other forms of intersectional discrimination.
- Do consider different user profiles including preferences, accessibility challenges and backgrounds.
- Do use participatory and human-centred methods for collecting information and co-designing with the user throughout implementation.
- Do keep an intervention survivor-centred, whether or not the intended user is a survivor.
- Do base an intervention on actual user needs, research and evidence.
- Don't design for one user profile; instead map many profiles for different potential users.
- **Don't assume that you know best – listen to survivors and users in order to understand their needs.**

CONSENT

- Do create "opt-in" consent and creative ways of communicating data policies and terms.
- **Don't gain consent via bulk text with check boxes, or assume that consent is automatically given when information is accessed**.
- **Don't override consent**.

SAFETY

- **Do consult with potential users about their shared or monitored technology use**.
- Do add safeguarding features and processes that address data safety and security risks.

- Do monitor safety throughout the lifetime of an intervention.
- Don't assume that the use of technology is private and confidential.
- Don't assume that an intervention is safe and skip mitigative strategies.
- **Don't assume that safety remains the same throughout the lifetime of an intervention**.

SECURITY

- Do try to avoid collecting any personally identifiable information (name, location, ID, IP address etc.).
- Do set up security systems following the highest level of rigour and based on global security standards.
- **Do ensure that everyone involved in, or responsible for, the outcomes of an intervention is aware of security risks from intimate partners and oppressive groups, now and in the future.**[8]
- Don't assume that current security threat models address risks from intimate partners and oppressive groups.
- **Don't collect any identifying information without informed consent, safeguarding strategies, and mitigative security measures regularly practised and assessed**.

DIGITAL ECOSYSTEM

- Do research the current digital ecosystem, including infrastructure and other digital interventions, before beginning to develop a digital intervention.
- Do explore whether a previously developed digital intervention can be adapted for your context and users.
- Don't build a digital intervention that will not work with current infrastructure, or overlaps or replicates other interventions that can be adapted.

COLLABORATION

- **Do bring together diverse teams with various technical skill sets and expertise (ICT, digital, GBV, HP etc.).**
- Do build in processes for ongoing participation and monitoring of technology in partnership with cyber security, technologists, GBV/HP practitioners, and end users.

LIFETIME

- Do plan for the lifetime of an intervention.
- Do build in processes for closing out tech when and if needed, and for protecting data and privacy during the lifetime of an intervention.
- Do consider how an intervention will integrate or work with existing structures and systems.
- **Do consider that any data connected to a user belongs to that user and not to an organization or tech company**.
- **Don't sell or share any data about users to external parties without informed consent**.
- Don't consider a product launch as the end of a project.

8 Unstable environments, particularly those that are susceptible to a rapid deterioration in governance, must consider all possible future risks.

Annex C: Risk-benefit analysis tool

RISK FACTORS

Data security

Are you planning on collecting or asking for *any* identifiable information? (Name, date of birth, ID number, address or location, email, phone number, IP address etc.) *This includes any information that could be potentially tied back to an individual (either on its own or if triangulated with other data).* If yes, then you are using data at the **highest level of sensitivity and must consider additional security and mitigation measures**.

Assessing the likelihood of risks:

- **Leakage** – what is the likelihood of unintentional leakage or disclosure of either the raw data or the information/ knowledge resulting from your data analysis?
- **Intentional unauthorized disclosure** – what is the likelihood of intentional unauthorized disclosure by a member of your project?
- **Destruction** – what is the likelihood that data is physically destroyed, due to different technical/mechanical problems?
- **Misuse risk** – what is the likelihood of the raw data or information/knowledge resulting from your data analysis being misused or reused for a purpose notdauthorized by yournorganization?
- **Re-identification risk** – what is the likelihood that any non-personal, de-identified, aggregated or pseudonymized data will be used to identify an individual?
- **Legal risk** – what is the likelihood of your collection, analysis or other use of the data being non-compliant with the law (including privacy laws) or with contractual obligations?
- **Data quality** – what is the likelihood of your data being inaccurate, not up to date or irrelevant to the project's purpose?
- **Creation of new data** – what is the likelihood that your project will create new data sets which may be potentially sensitive?
- **Loss of control** – what is the risk that an organization will lose control over raw data or the information/knowledge resulting from your analysis based on legal/ policy rights asserted by governments, ministries or other government officials?

Mitigative measures – systemic
(in place and regularly practised):

- **Clear policies and procedures** that outline privacy practices for handling data (including but not limited to information-sharing protocols).
- **Data minimization** (collection of only minimum required, time-limited storage, proper disposal).
- Regular **data privacy impact assessments** or other data risk assessments.
- Limited access levels with regular assessment ("need to know" restrictions).

- Regular **security audits** to test security.
- Firewalls, up-to-date anti-virus software, strong passwords changed frequently.
- Use of **encryption** (data stored and in transit).
- **Data breach management** policies and procedures.
- **Staff training** on IT security, data privacy, what/who/how to notify in case of a data breach.
- **Monitoring** of access and identification of potential threats.
- Strong **application security** that follows the highest level of rigour in global standards.
- **ICT governance** structure to manage, monitor and advise on security.

Indicators of heightened risk
(*affecting data security, but also general safety*):

- Individual or group coming from, or currently within, a context where there is a history of human rights violations, oppressive behaviour, known surveillance, no data protection or privacy laws properly enforced, patriarchal laws, or an otherwise risky political or legal setting.
- A humanitarian context or otherwise unstable setting.
- Concerning or unequal power dynamics within relationships.
- Commonly practised device sharing or monitoring.

ASSESSING HARM

- **Physical** – are there any potential physical harms (e.g. death, serious bodily injury, forced movement)?
- **Infringement of rights** – are there any potential legal harms (e.g. loss of privacy or other fundamental rights, profiling, active persecution, violence, forced movement, repression)?
- **Economic** – are there any potential economic harms (e.g. loss of livelihood, loss of home, loss of other property, financial loss)?
- **Psychological and emotional** – are there any potential psychological or emotional harms (e.g. distress, depression, emotional instability)?
- **Social** – are there any potential social harms to known or identifiable individuals (e.g. reputational damage)?

BENEFITS

- What is the intended positive impact on the lives of women and girls? What is the likelihood of this impact occurring? What is the magnitude of the expected positive impact? What is the relative significance of the positive impact?
- Are there direct positive outcomes for survivors (e.g. access to services, livelihood advancement, financial support)? Is this addressing a gap in access to services?
- Is there a problem or unexplored issue that this project serves to address or explore?

FACTORING IN PROMISING TRAITS

- **Participatory approaches** – was the solution or idea identified by the community in which it is intended to support? Will the project be actively driven by women and girls from that same community?
- **Valid methodology** – is the project methodologically sound? Has analysis and data use been planned from the onset with a clear data architecture?
- **Realistic mission** – is the project grounded in a solid achievable mission?

Adapted from: National Network to End Domestic Violence: Data Security Checklist; United Nations Global Pulse: Risks, Harms and Benefits Assessment Tool; Girl Effect: Digital Safeguarding Tips and Guidance.

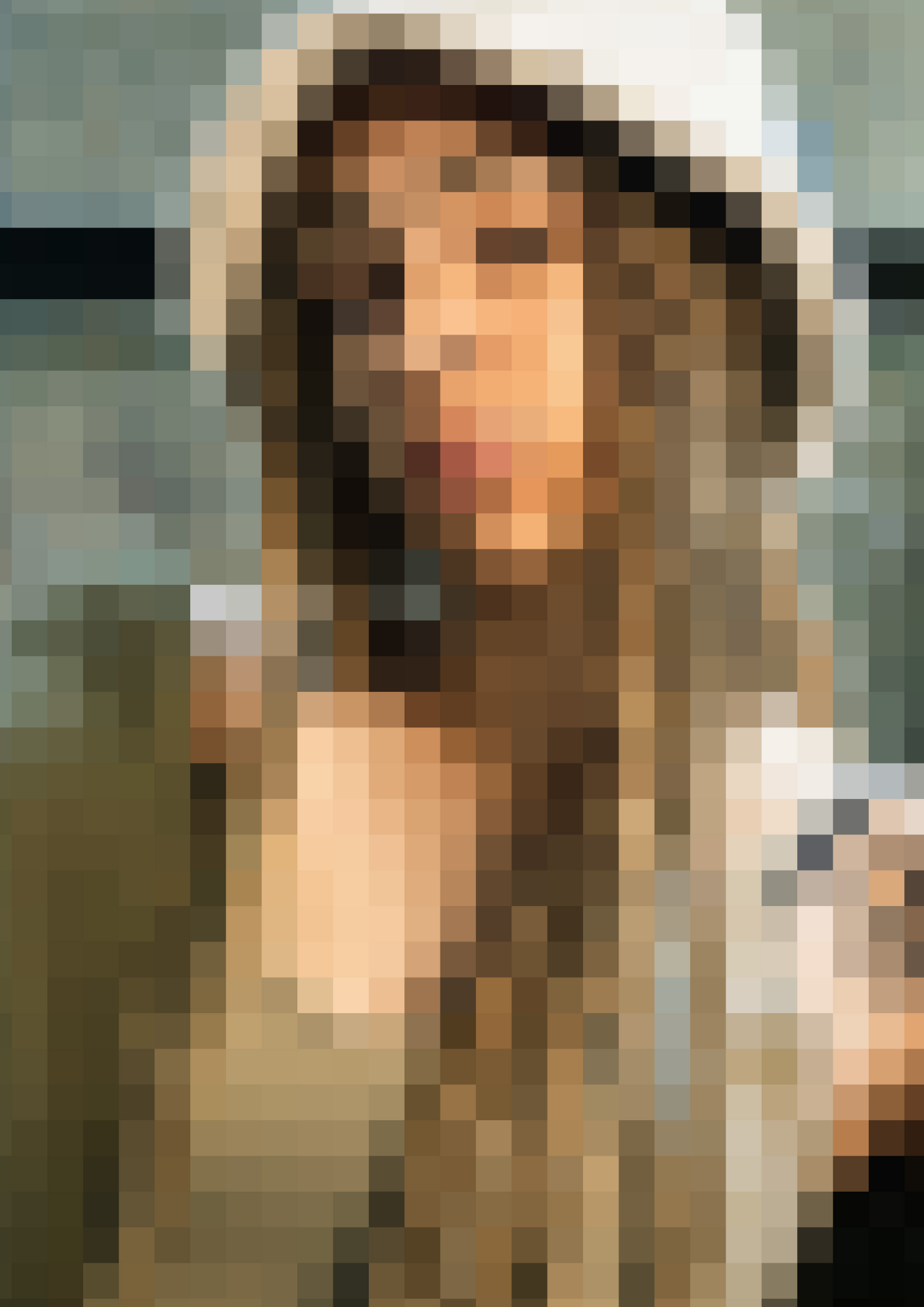


Photo credit for previous page and on the right: UNFPA