

Using Technology to Improve International Criminal Law Investigations of Sexual and Gender-Based Crimes: Advances, Challenges, and Opportunities

It is increasingly common to see the use of digital photos, videos, audio files, satellite or drone imagery, maps, and 3D imaging presented as evidence in courts, tribunals, and investigative bodies addressing genocide, crimes against humanity, and war crimes. It is also common for artificial intelligence (AI) to be used to search this data within information management systems. However, relatively little attention has been paid to when and how such technology is being used – or should be used - in situations involving sexual and other forms of gender-based violence (SGBV), though many acknowledge that technology can be particularly useful in identifying linkage and corroborating data in SGBV crime cases.

In 2023-24, our Project Team undertook 39 semi-structured interviews with international and domestic SGBV crime investigators, professionals from international and civil society organizations who document such crimes, SGBV survivor advocacy organizations, archivists, and information technology specialists. Our interview data revealed that while technology improved the ability to document, in a digital and lasting manner, the experiences of SGBV crime victims in armed conflict and mass atrocity, there were also risks and challenges associated with doing so, related to five key themes:

Theme 1: Data confidentiality and security in the short and long term

- The use of technology adds data security concerns to survivors' confidentiality concerns.
- Standard practice in digital safety includes using encrypted apps to communicate via text, email, audio, or video call with survivors and to store the information using means that are as digitally-safe as possible.
- SGBV crime information may become 'locked up' when information is not shared with other organizations doing similar work, or when it is captured in civil society-created apps or databases for which funding is not long-term and adequate.
- Technology allows open-source documenters to collect and analyze information in real time, but crisis-response documentation needs to be planned to avoid *ad hoc* procedures.

Theme 2: Informed consent to provision and use of digital evidence

- Those who seek informed consent should use plain language suitable to the survivor's situation. This consent should include information on how the digital version of their SGBV crime information will be kept secure, stored, and used by that organization, and for how long.
- Separate informed consent must be sought for third-party sharing, the purpose of the sharing, and time or other limits on that sharing. Data security standards should be high at the third party.
- SGBV survivors portrayed in digital open source content should provide informed consent before those images can be used as SGBV crime evidence. However, before such consent is sought, investigators must consider the survivor's dignity, safety, and protection.

Theme 3: Access to digital SGBV crime evidence and to relevant technology

- Survivors of SGBV crimes may not have access to cell phones and internet or data, or a safe space in which to use it, or may not have the literacy required to use certain apps.
- Organizations must consider whether, when, and how a survivor can access the information they have provided.
- Interviewees would like to see software and hardware designers work with them to develop accessible technology that functions in a variety of challenging settings.

Theme 4: The promise and realities of technology

- Some of the most powerful technological tools that can assist SGBV crime investigations require expensive proprietary software. Not all organizations can afford to purchase or maintain this software. This causes problems for the long-term maintenance of databases and the SGBV crime evidence within those databases.

Project Team:

- **Dr. Valerie Oosterveld** (University of Western Ontario Faculty of Law), assisted by **Loyce Mrewa** (PhD Candidate) and **Alison Morrison** (JD Candidate)
- **Dr. Heather Flowe** (University of Birmingham School of Psychology), assisted by **Kirstin Wagner** (Research Fellow in Psychology)
- **Dr. Kateryna Busol** (National University of Kyiv-Mohyla Academy), assisted by **Polina Overchenko** (law graduate)
- **Natia Navrouzov**, LLM (Executive Director, Yazda), assisted by **Marie Lehmon**, LLM (Yazda and trainee lawyer to the Paris bar)

For more information about this project, please contact the Project Team Lead, Valerie Oosterveld, at vooster@uwo.ca.

- The use of proprietary AI within investigative software is not always sophisticated enough to identify SGBV crimes or to provide accurate translations. The use of open-access AI poses security risks.

Theme 5: The need for combined SGBV crime and technological training

- Siloed training is a problem. Technology experts need gender-competency *and* SGBV crime training, and SGBV crime experts need technology training (such as on the risks and benefits of using AI in SGBV crime investigations).
- Many interviewees called for more internal and external legal and ethical guidance and training on the ways technology can be usefully employed in SGBV crime investigations in gender- and culturally-sensitive, and contextualized ways.