

## Tackling exploitation through ‘technology for freedom’

Christa Foster Crawford and Ashley Kafton

**Examples from Southeast Asia show both the promise and the pitfalls of emerging technologies and platforms that are being used to tackle forms of exploitation.**

Factors that make migrants vulnerable to exploitation – while on the move or at their place of destination – include displacement and insecurity, lack of legal status, insufficient awareness of rights and potential risks, and inability to understand the language or how to access help. In Southeast Asia, two of the forms of exploitation to which migrants are vulnerable are online child sexual exploitation and forced labour.

Online child sexual exploitation involves the making of sexually explicit images or videos of children under the age of 18. Unlike in-person exploitation, the harm continues so long as the images exist. Although physical movement is not a prerequisite for a crime of this nature to be defined as trafficking, some children have been moved to places where the online exploitation takes place, including to major hubs in the Philippines and Thailand. Others are vulnerable to such exploitation because they are already on the move.

Another form of exploitation takes place in the fishing industry, when people who are fleeing harm or lack of economic opportunity in their home country are lured into forced labour. Job brokers who offer hope instead trap people on boats where they can be out at sea for months or years at a time, working in inhumane conditions for long hours with little or no pay. Those who try to escape are punished and sometimes killed.

Technology companies, NGOs and governments are harnessing the power of technology to prevent and prosecute these and other forms of harm. However, although these emerging technologies promise freedom for many, in the wrong hands they can also be used to facilitate exploitation.

### Technology for prevention

One of the most effective ways of preventing exploitation is to reduce demand for products which involve labour exploitation. When

forced labour is no longer hidden in the supply chain, companies are incentivised to ensure that the entire production process is free of exploitation. Blockchain, which creates an immutable record of transactions, helps to promote greater transparency and accountability. It can be used, for instance, to track a product through the entire production process to verify that it was not made using forced labour, or to document labour contracts and wage payments.<sup>1</sup> However, technology cannot guarantee exploitation-free products, and may therefore give consumers what may be a false sense of security and shield producers from scrutiny.

First, supply chain accountability may not cover all inputs. For instance, there is current political will to address exploitation at sea (in the fishing industry) but exploitation in the sorting and packing process continues unchecked. Second, the reality is that the complex, inter-related global supply chain means that most end products will contain some inputs which have involved exploitation. Developers must ensure that technology accurately tracks constituent inputs and fungible goods, and governments and industry must ensure that accountability is built into all stages of the production process.

Prevention efforts must also address the supply side. Chatbots like Facebook’s Miss Migration,<sup>2</sup> and apps that can be accessed through mobile phones and devices as well as through online platforms, help prevent harm by educating migrants about their rights and providing resources for safer migration, access to ethical job brokers, and warnings about unscrupulous job brokers and transportation agents. Such tools also generate data about the users and so inform an evidence-based understanding of the problem and effective responses. However, the high cost of devices, lack of access to the internet (due to limitations on infrastructure

June 2020

www.fmreview.org/Issue64

and freedom) and lack of resources in local languages are common barriers to information being shared widely and effectively. QR codes and radio-frequency identification (RFID) tags, which can transmit data without the use of mobile devices or computers, are one response to this, although they still require data readers, which are not available in every community. And cultural relevance and issues of literacy, numeracy and other potential barriers must also be taken into account when developing and presenting such information.

Prevention must be focused at the community level, including through economic empowerment. People in poor communities are more vulnerable to exploitation, which is often compounded by crisis migration. Technology can be used to indirectly mitigate risk, in part by creating new economic opportunities. For example, many communities that are at risk of trafficking lack access to banks or other traditional means of finance, making them vulnerable to predatory lenders or even unable to receive non-cash payments. The primary barrier is their lack of documentation to confirm their identity, finances or credit-worthiness. By providing an online identity, blockchain makes possible access to bank accounts, the ability to receive verified wage payments, and even access to credit. This in turn reduces their vulnerability to trafficking, especially in the context of crises such as fires or floods that may force them to move if they are unable to rebuild.

Technology can also be used to raise awareness of rights abuses. For instance, Rohingya people in Myanmar have faced internal displacement and exploitation in the international fishing industry for decades. Now monitoring groups can use drone and satellite imagery as well as geodata and data visualisations in order to document the destruction of villages in real time, with the goal of ending rights abuses through raising awareness. However, the same technology can equally be used by governments and individuals to commit abuses. Technology designers, in collaboration with governments, NGOs and the international community, must decide how to mitigate the potential damage the use of such technology can bring.

### Technology for protection

Emerging technologies help law enforcement to identify and assist victims, whether they are online, out at sea, or elsewhere. For instance, not only does artificial intelligence permit law enforcement to locate and remove from circulation some of the hundreds of millions of exploitative images of children, but facial recognition software, metadata embedded in images and geolocation technology also enable them to identify and assist victims, regardless of their remote locations. Mobile apps and RFID tags help ensure that vulnerable migrants can be found at sea even if they lack documentation, making them even harder to trace, or are hidden through corrupt practices such as ships sailing under 'false flags'. In fact, geolocation records can be combined with blockchain to document how often workers are allowed off fishing vessels and then to alert law enforcement and NGOs to potential cases of labour exploitation and slave-like conditions. Furthermore, a digital identity can be created using blockchain technology and optional biometric identifiers to provide independent identity documents as an alternative to government-issued documentation. Digital identities help to protect against exploitation, including by enabling individuals to prove their eligibility for services, and by providing information about where they live if they do not know how to find their way home. However, the same technology can also give traffickers and unethical employers efficient unbreakable ways of tagging and tracking individuals in order to monitor and control them. This is particularly the case when biometric data are involved.

Also essential to protection is having the awareness of and ability to enjoy one's legal and human rights. Apps, QR codes and other tools can inform migrants about their labour and migration rights and where to get help if needed.<sup>3</sup> Blockchain and e-payment services<sup>4</sup> can help ensure that migrants are paid fair and legal wages, providing transparency and accountability, preventing employers from illegally withholding payment, and making it safer and easier to send home remittances. And other apps

and services make it easier to document and monitor working conditions and employment terms, empowering the worker.<sup>5</sup>

However, such technological tools are only as good as the information they use and the extent to which they are accessible. As with tools focused on prevention, there are real accessibility concerns, which are compounded by the very real risk that the exploiter will confiscate the technology, or even use it to track and control those whom they exploit.

### Technology for prosecution

Finally, technology is being used both to identify and locate perpetrators, and to provide evidence for criminal prosecution and other forms of enforcement. Just as they can be used to identify victims of online child sexual exploitation, the metadata, geolocation data and other unique identifiers embedded in exploitative images can reveal the identity and location of perpetrators, leading to their arrest and prosecution. Once convicted, technological restrictions (preventing computer use or blocking certain kinds of content) can help prevent future harm. However, the trend within the technology sector is towards greater privacy, anonymity and encryption which, although core rights and values that should be protected, make it harder to identify perpetrators and hold them accountable.

Similarly, blockchain technology gives banks and financial institutions an immutable record of transactions, providing clear evidence against traffickers with large-scale operations, who need to make use of the international banking system to profit from their crimes. Governments can use that evidence to hold perpetrators financially and criminally liable, and industries, investors and other stakeholders can more easily recognise exploitative transactions and create a culture of freedom.<sup>6</sup> However, the issues around privacy that arise with perpetrator identification also apply to digital evidence. Furthermore, the vast number of lower-level perpetrators who do not operate through formal banking systems may escape this type of detection.

The answer to these pitfalls is not to hinder the role of technology, for it will continue to advance, with those advances often led by exploiters. Instead, the power of technology must be harnessed for the greatest good and must mitigate the most avoidable harms. In doing so, several key principles should be considered.<sup>7</sup> The first is to scale better, not just bigger. Increased anonymity, privacy and encryption are essential elements of technology for freedom, but developers and policymakers must take into account how they can be used for harm. The second principle is to focus on people. While tracking the identity and location of products has few ethical implications, there are many implications for human rights, dignity and safety in tracking the identity and location of human beings, especially when this involves biometric data. Finally, technology must be informed by communities. Communities should be asked what they need and solutions should be designed to meet those needs and to adapt in the face of rapidly evolving forms of harm.

**Christa Foster Crawford**

*christa@FreedomResource.org*

Founder, Freedom Resource International

*www.FreedomResource.org*;

Associate Director, Center for Human Rights Law, Payap University, Thailand

**Ashley Kafton *ak469117@ohio.edu***

Graduate student, International Development

and Southeast Asian Studies, Ohio University

*www.ohio.edu/cis*

1. The Mekong Club (2018) 'Using Blockchain to Combat Modern Slavery' [bit.ly/MekongClub-blockchain-2018](https://bit.ly/MekongClub-blockchain-2018)

2. [www.facebook.com/MissMigration](https://www.facebook.com/MissMigration)

3. For example, in Thailand apps are being developed by a number of partnerships between technology companies, NGOs and governments, relating to rights and resources in the fishing industry (for three examples, see [www.MASThuman.org](http://www.MASThuman.org), the Apprise pilot study being conducted by the UNU Institute in Macau, and work by Winrock International) and to rights and resources during detention (see the Association for the Prevention of Torture and the Payap Center for Human Rights Law).

4. For example, SaverAsia [www.saverasia.com](http://www.saverasia.com)

5. For example, the eMin project [bit.ly/Diginex-Verifik8-eMin](https://bit.ly/Diginex-Verifik8-eMin)

6. For example, Liberty Shared Operational Research and Analysis Programme <https://libertyshared.org/operational-research>

7. These recommendations and the framework for this article were first included in Crawford C F (2019) 'Sex and Shrimp: Blockchain Use Cases for Ending Child Sex Trafficking and Modern Slavery' presented at the Blockchain for Social Impact Conference 2019, New York City, 10 June 2019.