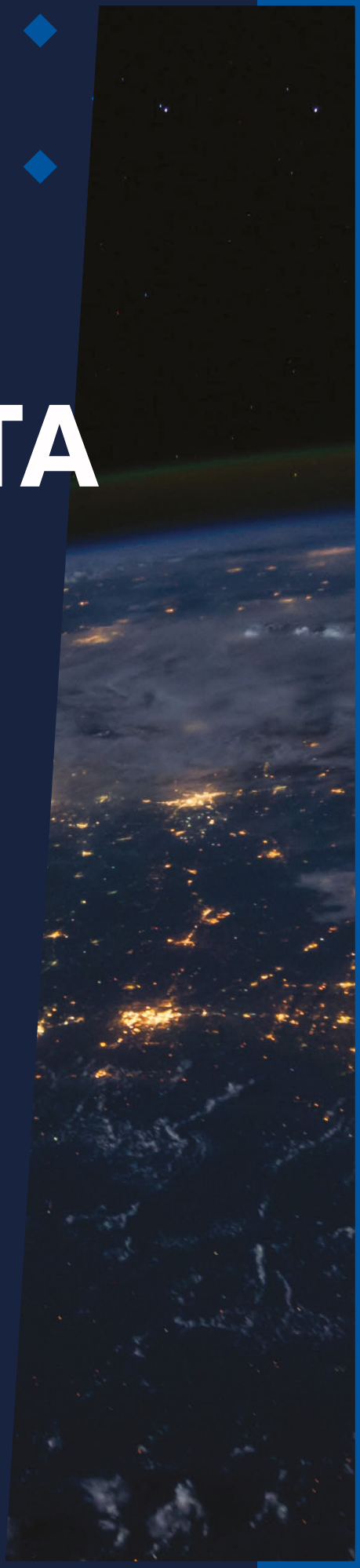
HOPE FOR JUSTICE

intel

PRIVATE DATA EXCHANGE

Leveraging Confidential Computing to Combat Human Trafficking



Hope for Justice, supported by Intel®, invite key anti-trafficking stakeholders into a collaborative partnership for the Private Data Exchange project, leveraging confidential computing as an innovative data collaboration tool in the fight against human trafficking.

AUTHOR: CALLUM F. HARVIE
callum.harvie@hopeforjustice.org

Private Data Exchange: Leveraging Confidential Computing to Combat Human Trafficking


POLICJA
POLICJA
Jinbaoma

BACKGROUND

Globally an estimated 49.6 million people are living and working in conditions that can be described as human trafficking. In the modern age, the digital world is increasingly a platform where such exploitation is initiated, solicited and facilitated – connecting huge numbers of potential victims with potential exploiters, often across country borders. Perpetrators now recruit victims behind anonymity, often developing online relationships, posting fake or deceptive job advertisements and exploiting victims via social media. While human traffickers have been able to operate in cyberspace and use technology successfully to their advantage, the same is not necessarily true of the actors responsible for combating this crime, and the counter-trafficking response has not leveraged technology at the same speed or scale. Nevertheless, those on the frontlines should embrace the use of technology positively, to enhance efforts to prevent exploitation, identify victims, support survivors, and effectively prosecute those responsible. Crucially, at the core of all technological development is the counter-trafficking sector's understanding and utilization of **data.**

Utilizing Data

Data is crucial tool in helping non-profit organizations, statutory actors and intergovernmental agencies in their work to end human trafficking. Many different organizations working with cases of human trafficking, hold and process existing pools of sensitive case-level data relating to victims, perpetrators, patterns and trends. This detailed information can often hold valuable intelligence for a variety of benefits, including the identification of victims of trafficking; the removal of individuals from situations of exploitation; the overcoming of obstacles faced by survivors along their journeys of recovery; the collection of evidence for the prosecution of human traffickers; and for the understanding of novel trends to support preventative intervention strategies. Similarly, data is also utilized to understand global trends of human trafficking. Led by large data initiatives and macro-level reporting mechanisms, data is collected both through the tracking of key indicators such as direct prevalence, the identification of proxy indicators such as poverty, the analysis of secondary data or indices such as inequality, as well as the undertaking of direct contextual analysis in target geographies. These analyses inform some of the most significant empirical reports on human trafficking that unequivocally guide the long-term strategic direction of the counter-trafficking sector.

Data-Sharing Challenges

The sharing of data between agencies is a recurring challenge across the counter-trafficking sector, for good reason. Human trafficking case data is complex, personal, and sensitive, relating to the personal experiences of those who have been subjected to some of the worst contemporary human rights abuses. It recounts details of a person's vulnerability, serious trauma and health conditions. It also contains evidence of criminal

perpetration that must be preserved to secure successful prosecution and convictions. Most importantly, it contains personally identifying information, locations, and legal statuses of victims and survivors, that could place an individual at further risk of harm should confidentiality be breached.

As such, this data must be handled with high levels of security and confidentiality, compliant with relevant data protection legislation such as the General Data Protection Regulation (GDRP) in the EU, the Health Insurance Portability and Accountability (HIPAA) Act in the USA, and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Beyond compliance, preserving trust and transparency between data controllers, data processors, and the victims or survivors to whom the data relates is of an even greater threshold, crucial to maintaining a survivor-centred approach.

Data Collaboration

Collaboration, cooperation and partnership are of paramount importance to the holistic global response to human trafficking. This simple principle extends deep into organizational strategies, political will, and global initiatives. However, this does not yet extend into arguably one of the most important elements of collaboration, the sharing of data. The burdens of data protection can seem so complex, litigious and sensitive, that organizations find it challenging to even consider the sharing of data with one another. However, failing to share data has several consequences.

- At the case level, data fragments and pieces of intelligence remain siloed within each organization, completely hidden from potential partners who may be able to support, share similarities in data or contribute to the wider intelligence picture. This severely limits the number of opportunities for collaboration, identification and intervention, to the ultimate detriment of victims and survivors.

- Similarly, big data initiatives often require a process of anonymization and sanitization by the contributing partner to ensure anything shared with global reports does not contain any personal or sensitive information. This process is resource-intensive, resources that many organizations simply do not have. Therefore, global datasets and indices on human trafficking can lack some of the most meaningful and timely insights as a result of reporting delays, absent submissions, and information redaction.

This presents a tension for the counter-trafficking sector. On one hand, data must be protected, confidential, and private. On the other hand, data must be collaborative, utilized in partnership and to generate real-time data and collective intelligence. Can these critical requirements be reconciled? By using technology, yes, they can.

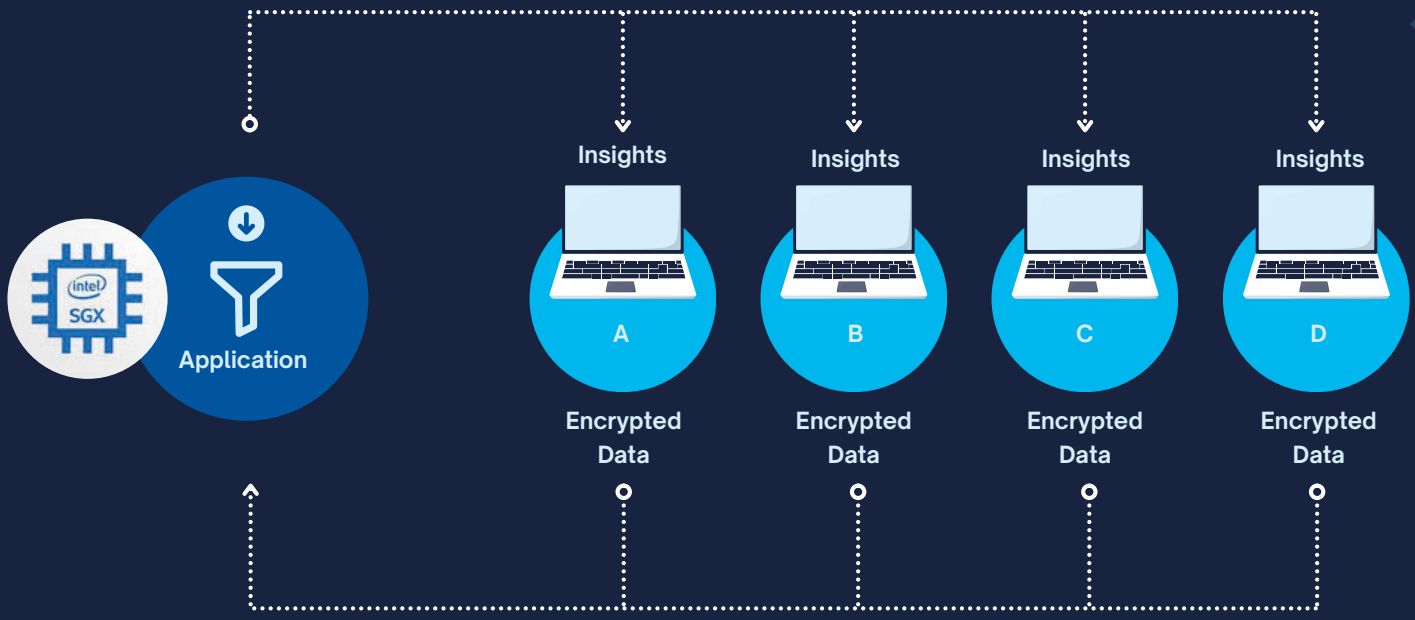
EXPLORING A TECHNOLOGICAL SOLUTION

Data sharing and collaboration are not challenges unique to the counter-trafficking sector. Many different sectors collect, process and share sensitive information to ensure crucial social and commercial services can continue to operate. For example: health services must share information securely to ensure a continuation of care; law enforcement frequently collaborate to ensure criminal investigations are joined up; and financial service institutions continue to share information to identify risk, fraud and financial security. In an increasingly digital world, data security technologies are advancing rapidly to ensure some of the world's most sensitive data remains secure. One of the most critical of these technologies is known as **Confidential Computing.**

What is Confidential Computing?

The field of Confidential Computing is an advanced technology that protects data through layers of encryption while it is being processed. Traditionally, data is encrypted at rest (for example in a database) and in transit (for example, when it is sent to another). Confidential computing however ensures that data remains encrypted throughout the entire process, even during computation. This is achieved through the use of secure enclaves, which are protected areas of a processor. These enclaves act as a secure safe room for sensitive data to be processed and analysed, shielding it from external threats, the view of other users and the processes of the operating system. It is also hidden from the manufacturers of the processor itself, thus allowing data to be analyzed while simultaneously preventing all unauthorized access. This makes confidential computing a key player in the future of cybersecurity.

Confidential Computing is a flexible technology that can be moulded to suit the requirements of an application design, however it is primarily used to enable sensitive data belonging to different users/organizations to be pooled, partitioned, processed and analyzed under encryption in a secure enclave. This enables different users to confidentially share data to a central source without any fear of compromise. In this environment, data can be securely cross-referenced, aggregated and analyzed, instantaneously notifying users of any insights, for example: when relevant data matches are uncovered, or key trends across the full collective dataset are identified.



What Does This Mean For Counter-Trafficking?

This technology is crucial for industries that handle sensitive information, such as finance, healthcare, and government, providing an additional layer of security and privacy in areas of low trust. These industries are already deploying Confidential Computing solutions, however, the technology is yet to be leveraged to support social and human rights issues such as human trafficking, that also involve the collection of highly sensitive data. This presents a huge opportunity for a partnership between the technology sector and the counter-trafficking sector to break new ground, and reinvent its approach to data collaboration.

PRIVATE DATA EXCHANGE

The **Private Data Exchange** is a research, development and innovation (RDI) initiative led by Hope for Justice, supported by Intel®, to demonstrate the potential impact of leveraging of Confidential Computing to combat human trafficking. Since conceptualization, trauma-informed practitioners have partnered with technological experts and computing engineers to understand the unique obstacles facing counter-trafficking data collaboration and explore prospective solutions this technology can provide.

Between 2022-2024, the Private Data Exchange project has identified significant challenges facing data collaboration across the counter-trafficking sector. It has also articulated the most innovative use cases provided by the encryption and logic of Confidential Computing, and has turned a thought-exercise into a tangible proof of concept with viable platform prototype built on **Intel® Software Guard Extensions (SGX).** The project utilises the sector-leading data framework of the Human Trafficking Case Data Standards (HTCDS), has been tested using dummy data.

The project now demonstrates three of the most tangible proven benefits of a Confidential Computing platform to counter-trafficking data collaboration:

- Firstly, all data is **encrypted** and secured with an encryption key. The information can only be viewed by the user who has uploaded it (the data owner). No other person or system can gain unauthorized access, preserving privacy and data sovereignty.

- Secondly, victim or survivor case records that hold **data matches** or similarities with that of another organization can be identified and flagged via a weighted match scoring algorithm, to mark cases for further action without compromising data privacy or security. This enables legitimate and secure collaboration on linked incidents when required.

- Finally, the encrypted data of all agencies can be aggregated across the entire dataset and analyzed to derive accurate live reporting via an **Insights Dashboard**. Reports are generated without revealing any of the sensitivities relating to the underlying data, negating the requirement for any manual anonymization.

Across all functions, each organization always remains in full control of its data. It can be altered, updated, or deleted without concern of loss or compromise. This unabated retention of data sovereignty therefore offers the capacity for organizations to collaborate on data both domestically *and* across borders.

Encryption

High levels of compliance, privacy and data sovereignty, with all data secured by an encryption key.

Data Matching

Identify agencies that hold similarities in their records and alert them of any potential matches.

Insights Dashboard

Aggregate sensitive encrypted data to derive live novel insights and reporting of trends.

Encryption

Encryption is the fundamental component of the Private Data Exchange, providing critical security guarantees against the compromise of privacy and data sovereignty. It also fully removes the requirement for the anonymization or sanitization of data, as raw data can be kept intact without fear of breach.

Within a secure enclave built on **Intel® Software Guard Extensions (SGX**) an organization's data is protected via unique application isolation technology. This protects data in transit, storage and use, ensuring that it remains fully secure even during processing. Once online, data can only be unencrypted by the data-owning organization. This ensures that sensitive information is completely inaccessible to unauthorized users *(i.e. other organizations, external threats, the system operators, and the manufacturer of processor).*

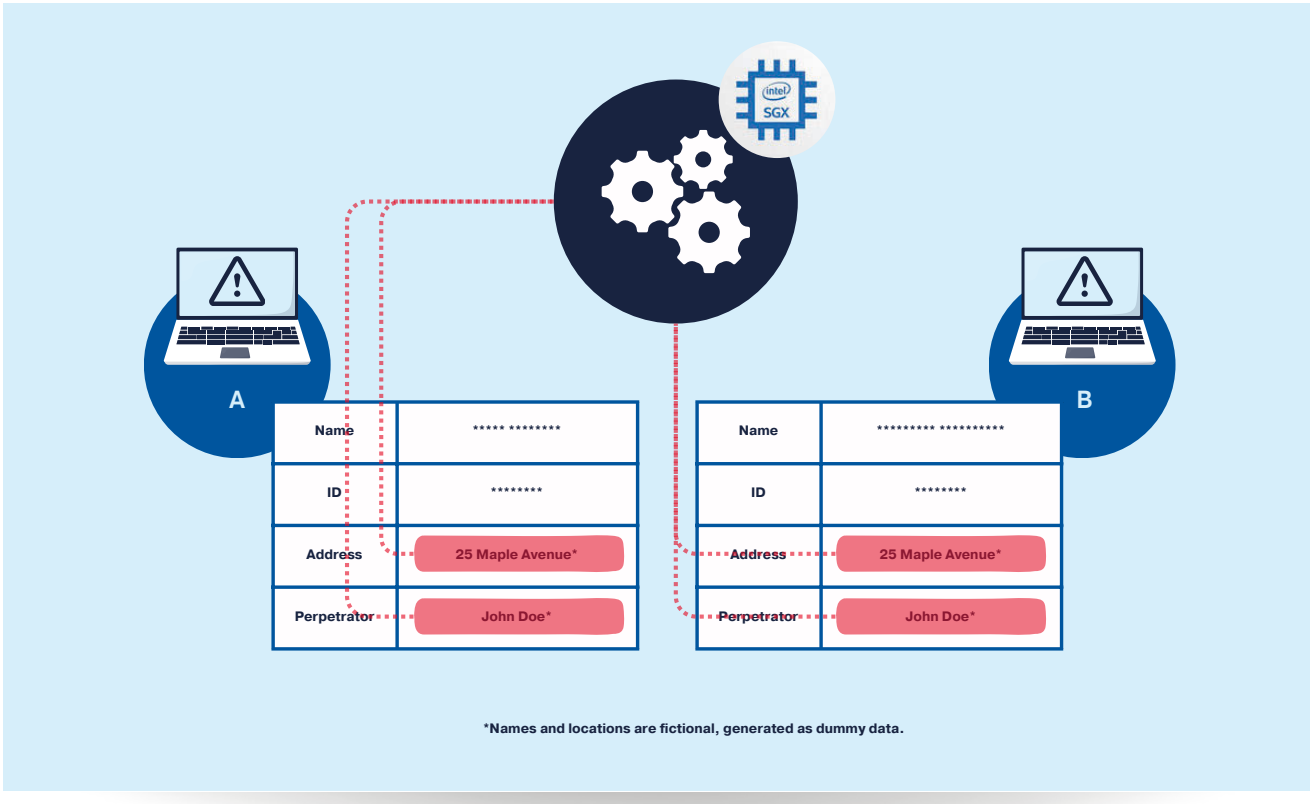
By utilizing encryption, data can be shared, pooled and processed in its encrypted format, allowing powerful algorithms to run Matching and Insights functions in a trusted execution environment, without ever needing to reveal the sensitive raw data beneath it.

Data Matching

Via a secure logic and scoring algorithm, the Private Data Exchange application allows the encrypted data of victim or survivor case records belonging to multiple parties to be securely analyzed, generating an alert to flag matches or similarities on variable data lines. This informs the case managers, or data operators of each organization, who then decide whether to collaborate with the linked agency.

Examples of data matches could include:

- *Identity Number* - This could provide insight that repeat fraudulent documents are being issued in the course of exploitation.
- *Name* - This may reveal that two people are related, either familial or spousal. This also includes a tolerance threshold for differing male/female suffixes.
- *Address* - This may reveal the existence of a multi-occupancy household regularly housing victims of human trafficking, owned or operated by a perpetrator.
- *Perpetrator Name* - This may reveal a pattern of exploitation with a repeat offender, crime operation or the name of an impacted business entity.



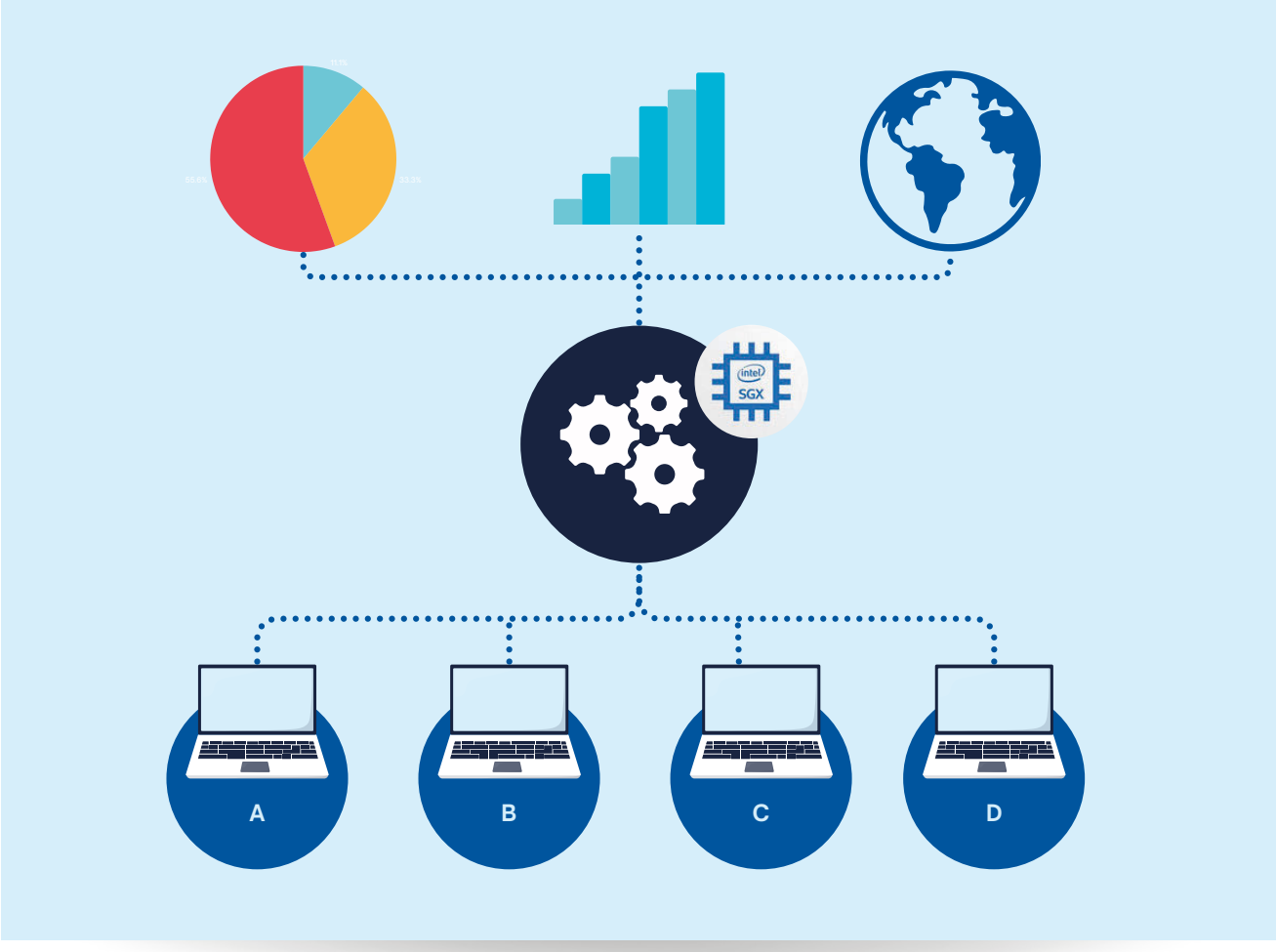
Insights Dashboard

The encrypted data of all contributing agencies is aggregated across the entire dataset and analyzed to derive accurate, live insights, reported on-demand via a dashboard reporting mechanism. This analyzes all data lines but is especially powerful when processing the more contextual data relating to macro-trends, and is filtered using commonly used data queries. For example:

- *Exploitation Type* - outlining the prevalence of each of the known types of human trafficking and exploitation.

- *Gender* - disaggregating gender within the dataset to support nuanced understanding and gender-sensitive approaches.

- *Locations, or Industries of Exploitation* - highlighting geographical or industrial hotspots where human trafficking is recurrent.



THE FUTURE OF COLLABORATION

The **Private Data Exchange** project demonstrates a critical opportunity for the counter-trafficking sector to re-examine and positively reform how sensitive information is handled, processed, shared and reported by utilizing confidential computing.

Stakeholders

Exploring confidential computing as a technological solution has several key impacts across a variety of stakeholders:

- Frontline civil society organizations, non-governmental agencies, hotlines, and others, can securely collaborate on live cases of human trafficking or related issues *(e.g. refugee support, gender-based violence etc.)*. By recognizing similarities, patterns or trends in their data, more holistic interventions can be coordinated, to the benefit of victims and survivors.

- National statutory agencies and reporting bodies can monitor prevalence, typologies and trends of exploitation occurring domestically, modernizing their approach to policy responses, *(e.g. National Referral Mechanisms)* reinforced by cutting-edge data analysis and cyber security.

- Multilateral organizations and intergovernmental agencies can co-ordinate greater collaboration across borders, facilitating a more globalized response to data-sharing, and undertake a more intelligence-rich method of reporting, informed by live case data.

- Business, industry and labour governance bodies can better monitor instances of exploitation and emerging trends occurring in supply chains, building resilience and ensuring greater social impact in sustainability goals and decent working practices.

OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings. Dec 2023.

Next Steps

Having been led by *Hope for Justice* in a Research, Development and Innovation (RDI) environment to date, the next chapter of the Private Data Exchange project will require a concerted effort from multiple agencies *(civil society, academia, multilateral agencies and governing institutions)* to contribute their unique expertise, time and resources to collaboratively develop a platform suitable for the agile, diverse and evolving needs of the contemporary counter-trafficking sector.

As such, Hope for Justice and Intel® are inviting key counter-trafficking stakeholders into a collaborative partnership and consortium for the next chapter of the Private Data Exchange project. This includes organizations who hold and collect data at the case level. It also includes governing or multilateral organizations who are considered stakeholders to high-level reporting and analysis. The Partnership invites data protection experts to support the ongoing alignment of technical development with emerging best practices in privacy regulation and compliance. Finally, the Partnership humbly invites investment from donors, foundations and corporate funds, to help build financial sustainability into the core of project impact and to support the active participation of frontline agencies.

Counter-trafficking practitioners should embrace the use of technology, including Confidential Computing, to positively enhance global efforts to prevent exploitation, identify victims, support survivors and effectively prosecute those responsible. This is a critical opportunity for the technology sector and the counter-trafficking sector to work together to make new strides in the fight against human trafficking.

"The Private Data Exchange project is an incredibly exciting opportunity for agencies in the space of anti-trafficking to work together to leverage confidential computing to the benefit of our sector. This shared endeavour is led by practitioners, supported by technological experts and informed by best practice, with victims and survivors remaining firmly at the centre of our innovation. We invite you to join with us."

Tim Nelson, Chief Executive Officer, Hope for Justice

"As security technology creators, we have both the responsibility and the opportunity to help protect every person's data and privacy. We're seeing this occur through confidential computing advancements – the innovations we are bringing forward today will help us facilitate change and soon become the standards for how we operate tomorrow."

Daniel Gutwein, Director of Education, Intel

Learn more.

Hope for Justice
P.O. Box 5527
Manchester, M61 0QU

(+44) 0300 008 8000 (local rate call)
info@hopeforjustice.org