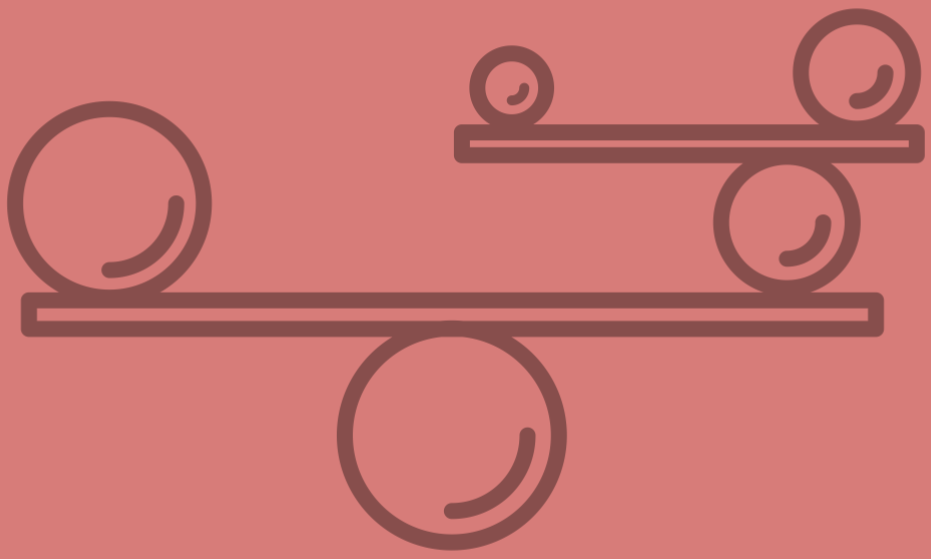

Legal and Ethical Issues in Data Collection on Trafficking in Persons

NEXUS Institute

2019

This research and publication were made possible through support provided by the United States Department of State Office to Monitor and Combat Trafficking in Persons (J/TIP), under the terms of Grant No. S-SJTIP-14-GR-1036. The opinions expressed herein are those of the authors and do not necessarily reflect the views of the U.S. Department of State.

Authors: Marika McAdam, Rebecca Surtees and Laura S. Johnson
Project Director: Stephen Warnath
Layout and design: Laura S. Johnson

Publisher: NEXUS Institute
1440 G Street NW
Washington, D.C. 20005

Citation: McAdam, Marika, Rebecca Surtees and Laura S. Johnson (2019) *Legal and Ethical Issues in Data Collection on Trafficking in Persons*. Washington, D.C., United States: NEXUS Institute.

The NEXUS Institute® is an independent international human rights research and policy center. NEXUS is dedicated to ending contemporary forms of slavery and human trafficking, as well as other abuses and offenses that intersect human rights and international criminal law and policy. NEXUS is a leader in research, analysis, evaluation and technical assistance and in developing innovative approaches to combating human trafficking and related issues.

www.NEXUSInstitute.net @NEXUSInstitute

Photographs in this report illustrate various aspects of data collection. Unless stated otherwise, individuals in these photographs are not trafficking victims.

Foreword

Discussions about human trafficking data sometimes seem surprisingly abstract, as if research is most centrally about counting things from some distance: approximating "head counts" of global prevalence, formulating statistics, calculating metrics or constructing maps to illustrate geographic "hot-spots", "routes" or "hubs". All of these exercises, done well, can play a role in contributing to our understanding of human trafficking. But, even at their best, they are only a partial path to improved understanding and, moreover, sometimes seem to obscure the fact that human trafficking is, first and foremost, about human beings. The essence of human trafficking violations involves human beings severely exploiting and inflicting harm and suffering upon – often with the aim and result of subjugating – fellow human beings. It is from the human stories of those who have experienced what is unimaginable for the rest of us that we learn the most important lessons. It is from their courageous and generous sharing that we are provided the critical context that is essential for a fuller and more encompassing understanding of the phenomenon and, if we are fortunate, the possibility of embracing elusive insights that shed light on more effective and appropriate ways to prevent and combat it.

TIP data collection and research necessarily involve human engagement. This engagement and interaction create responsibilities and obligations. Those who collect data about the lives of others – including about some very sensitive, personal and painful aspects of their lives – must recognize the broad swath of harm that can potentially occur in the collection and/or use of this data (inadvertent or not) and avoid being a source of further harm.

There are many ways that anti-trafficking professionals can make mistakes or take actions with unintended negative consequences. Almost anyone who has worked in the anti-trafficking field is aware of situations where survivors' interests have been compromised or placed at elevated risk or danger because of treatment of an individual's data or how the data was obtained. This includes, but is not limited to, researchers not recognizing how their questions or approach can potentially re-traumatize TIP survivors; failure to obtain informed consent for participation in research; risking stigmatization and ostracism of trafficking victims when conducting research in ways that make TIP victims visible to others; or compromising victims' personal and sensitive data. Working with children – defined by international law as anyone under 18 in human trafficking cases – raises additional layers of requirements and considerations to recognize, protect and advance the best interest of each child.

The question arises: how can we acquire and use data to accelerate understanding and progress to combat human trafficking both most effectively and most appropriately? We hope that this paper helps to introduce and illuminate for readers at least the first steps toward finding answers to this complex issue.

As elaborated in this paper, the starting point is the cardinal principle that must guide all who work on human trafficking issues, including data collection: "Do No Harm". While being mindful of the fundamental principle to "do no harm", the next critical touchstones involve working within the guardrails provided by legal requirements and ethical standards. This paper discusses in detail this protection framework of laws and ethics. These requirements, standards and principles exist to protect individuals, especially those who have survived human trafficking, from being subjected to harm from those who interact with them, including in collecting and using their data. As a result, to acquire the data needed to advance anti-trafficking objectives in appropriate ways, the full range of normative standards must be understood and addressed satisfactorily at every step along the way.

This paper, *Legal and Ethical Issues in Data Collection on Trafficking in Persons,* focuses a lens on the range of legal and ethical considerations that arise in the collection of TIP data. Our intention is to encourage thoughtful discussion about these critical issues. We do not attempt to answer for readers all of the questions and issues they will face, but rather to constructively contribute to thinking on the issues that the anti-trafficking field is now grappling with as data collection on TIP continues to emerge and evolve. We hope that next steps include all stakeholders engaging in thoughtful reflection, analysis and conversation to determine how these considerations can be practically addressed in the most appropriate ways.

The vision that inspired the creation of the NEXUS Institute included addressing the need for independent in-depth research and analysis on human trafficking to support the development and implementation of more effective laws, policies and practices to combat human trafficking and to support victims of trafficking to recover and rebuild their lives. While research and data collection on human trafficking around the world have grown and improved since NEXUS was founded nearly twenty years ago, there remain substantial gaps in data available to professionals and practitioners to inform anti-trafficking efforts. Before these gaps can be addressed effectively and appropriately, there is an urgent need to better understand how anti-trafficking data can be ethically and legally collected and used.

This paper is part of a series of studies produced in the context of the NEXUS Institute's research project *Good Practice in Global Data Collection on Trafficking in Persons: The Science (and Art) of Understanding Trafficking in Persons*. Over the course of three years, our team, led by NEXUS Senior Researcher Rebecca Surtees, conducted interviews with anti-trafficking actors engaged with TIP data collection both in and out of government from countries around the world who shared their thoughts and experiences about the complex legal and ethical issues that they have faced. This study benefits from their knowledge and experiences. The study also benefits from issues raised by trafficking victims who have participated in NEXUS research projects over many years. I am profoundly grateful to be able to work with my wonderful colleagues who comprise the NEXUS research team for this paper: Rebecca Surtees, Marika McAdam and Laura S. Johnson. These pre-eminent research professionals have decades of collective experience dedicated to analyzing human trafficking issues and sharing the insights and new knowledge that they discover with the rest of us. With this paper they have, once again, addressed important issues that are integral to well-considered research with thoughtfulness and sensitivity.

NEXUS conducted this research and produced this paper as part of our work on a multi-year project supported by the United States Department of State Office to Monitor and Combat Trafficking in Persons. This office is filled with individuals who have dedicated themselves and their professional lives to initiatives intended to help move our world closer to eradicating human trafficking and to providing meaningful support to its survivors around the world. NEXUS is grateful for the opportunity and support that this office has provided to conduct in-depth research to contribute to this objective.

Finally, in our over twenty years working on these issues we have been fortunate to work with many prominent leaders and superb colleagues in the field of combatting human trafficking around the world. I am grateful that the following individuals generously contributed their time and expertise as peer reviewers of this report. These include: Sarah Craggs (IOM Afghanistan); Mike Dottridge (Independent Consultant on human rights and human trafficking issues); Jordan Greenbaum (International Centre for Missing and Exploited Children); Benjamin Harkins (International Labour Organization); Duncan Jepson (Liberty Shared); Matthew Mullen (Institute of Human Rights and Peace Studies, Mahidol University); and Fabrizio Sarrica (UNODC Research on Trafficking in Persons and Smuggling of Migrants).

As always, I invite those who care about human trafficking and related issues and are interested in being part of seeking solutions to follow our work at www.NEXUSInstitute.net

and on Twitter @NEXUSInstitute and to sign up for material that we send out periodically to share our most recent work. If you are interested in our training and advisory services for professionals and officials based, in part, on the findings of NEXUS research, including the topics and issues addressed in this paper, please see what we offer at www.WarnathGroup.com.

Stephen Charles Warnath
Founder, President & CEO
NEXUS Institute

Acronyms and abbreviations

ACFID	Australia Council for International Development
ACTIP	ASEAN Convention against Trafficking in Persons, Especially Women and Children
ADLS	Administrative Data Liaison Service
AFAPDP	Association Francophone des Autorités de Protection des Données Personnelles
AI	artificial intelligence
AoIR	Association of Internet Researchers
APEC	Asia-Pacific Economic Cooperation
app	application
ASEAN	Association of South-East Asian Nations
AU	African Union
CIOMS	Council for International Organizations of Medical Sciences
CoE	Council of Europe
CTDC	Counter-Trafficking Data Collaborative
DFID	UK Department for International Development
DPA	Data Privacy Act
EC	European Commission
ECOWAS	Economic Community of West African States
EIGE	European Institute for Gender Equality
ERB	Ethical Review Board
EDPS	European Data Protection Supervisor
EU	European Union
FCRA	Fair Credit Reporting Act
FRA	European Union Agency for Fundamental Rights
GAATW	Global Alliance Against Traffic in Women
GCC	Gulf Cooperation Council
GDPR	General Data Protection Regulation
GO	government organization
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTD	Human Trafficking Database
ICMPD	International Centre for Migration Policy Development
ICO	UK Information Commissioner's Office
ICT	information communications technology
IEC	independent ethics committee
IFCR	International Federation of Red Cross and Red Crescent Societies
ILO	International Labour Organization
IO	international organization
IOM	International Organization for Migration
IP	intellectual property
IP (address)	internet protocol
IRB	institutional review board
ISI	International Statistical Institute
J/TIP	United States Department of State Office to Monitor and Combat Trafficking
MSF	Médecins Sans Frontières

MSI	Marie Stopes International
NGO	non-governmental organization
NSF	National Science Foundation
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
RCUK	Research Councils UK
REB	research ethics board
THB	trafficking in human beings
TIP	trafficking in persons
UK	United Kingdom
UKRIO	UK Research Integrity Office
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNGP	United Nations Guiding Principles on Business and Human Rights
UNIAP	United Nations Inter-Agency Project on Human Trafficking
UNICEF	United Nations Children's Fund
UNHCR	United Nations High Commissioner for Refugees
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention on Transnational Organized Crime
U.S.	United States
VAWA	Violence Against Women Act
WANGO	World Association of Non-Governmental Organizations
WHO	World Health Organization
WMA	World Medical Association

Executive summary

1. Introduction

Data collection on trafficking in persons (TIP) is an important part of anti-trafficking efforts, including for protection, prosecution and prevention purposes. There has been increased emphasis on gathering TIP data in recent years and, commensurately, growing awareness of the legal and ethical considerations associated with doing so. There are many legal and ethical complexities at play in how anti-trafficking researchers and professionals undertake TIP data collection. These challenges and complexities are not unique to this field of work but also remain unresolved in many professional fields and are part of on-going discussion and debate.

The legal and ethical frameworks relevant to data collection on trafficking in persons differ by country, context and project and may also be informed by a raft of other factors, including the type of data being collected, who is collecting data, where data collection takes place, who is funding data collection, whether data collection involves a group requiring special consideration, whether there are emerging issues affecting the existing legal and ethical framework and so on. This paper explores the legal and ethical issues that arise when conducting TIP data collection, including the intersections and, at times, the tensions between the two. This paper draws on concrete examples and experiences of those working in the field of TIP data collection from different countries globally to identify what issues and problems may arise, how these may be addressed, as well as complex on-going discussion and debate around these issues, which remain largely unresolved. This exploration also aims to identify areas of agreement and consensus toward arriving at fundamental principles of good practice on legal and ethical issues. This paper is intended for anti-trafficking actors engaged in TIP data collection across its varying forms and from different approaches, particularly prosecution and protection.

This paper is part of a series of studies produced in the context of the NEXUS Institute's research project *Good Practice in Global Data Collection on Trafficking in Persons: The Science (and Art) of Understanding TIP*, which aims to identify good practice in the field of TIP data collection to support the enactment of more effective evidence-based anti-trafficking policy and practice. This project was generously funded by the United States Department of State Office to Monitor and Combat Trafficking in Persons (J/TIP).

2. Research Methodology

This publication is based on a review of laws, policies, guidance and resources on data protection and research ethics, as well as interviews with key informants including TIP researchers, TIP experts, staff from TIP data collection projects and National Rapporteurs or equivalent mechanisms.

2.1 Desk research – literature and document review

This study is based on an extensive review of literature and resources on TIP research and data collection. Some was specific to trafficking in persons, while some was broader in scope and included data protection and research ethics more broadly. This included a review of: national and international legislation on data collection and data protection issues; handbooks, guidelines and manuals about TIP data collection including data protection and ethics; ethical guidelines and protocols for research and data collection (for TIP and more generally); papers and articles on different research methodologies and data collection approaches, including ethical and legal issues; project documents about TIP data collection efforts, including methods, procedures and data protection requirements; media reports or op-eds on TIP data collection including reviews and critiques of research methodology or

data collection approaches, including the use of technology in TIP data collection; and websites about specific TIP data collection projects or research projects.

2.2 Interviews with key informants

We conducted a total of 163 interviews with 128 respondents representing non-governmental organizations (NGOs), research projects, academic institutions, international organizations (IOs), private sector actors and government. This included 95 interviews with TIP researchers and TIP experts (67 first interviews and 28 follow-up interviews); 55 interviews with staff of TIP data collection projects (49 first interviews and six follow-up interviews); and interviews with twelve staff representing ten National Rapporteurs or equivalent mechanisms. While criteria differed somewhat by category of respondent, a central aspect was diversity in sampling with regards to: 1) the types of TIP data collection being considered (for example, on protection or prosecution); 2) the approaches and methods used; 3) geographic scope or coverage; and 4) professional specialty or discipline.

2.3 Review process

This paper was reviewed by seven external peer reviewers, each of whom has extensive knowledge and experience in TIP research and/or data collection, as well as the TIP field more broadly. Peer reviewers included researchers, data collection staff and TIP experts from universities, international organizations, UN agencies, civil society and an independent expert from the field of human rights. In addition, staff at the United States Department of State Office to Combat and Monitor Trafficking in Persons (J/TIP) reviewed and provided helpful feedback on the paper. This paper was reviewed internally within NEXUS Institute at various stages of drafting including after the external peer review process.

3. What is TIP Data and TIP Data Collection?

Data collection is a broad concept, referring to a wide range of different practices related to the process of gathering and measuring information on variables of interest. It includes but is broader than just research, as it also includes a wide range of administrative data collection by various organizations and institutions as well as other types of data collected about TIP by governments, international organizations, NGOs, businesses and private sector actors. For the purposes of this paper, TIP data collection is understood to be the overarching practice of gathering data on various aspects of trafficking in persons and includes a wide range of data collection initiatives by various organizations and institutions, including governments, international organizations, NGOs and businesses. For this study, we are primarily concerned with what we perceive to be two distinct categories of data collected about trafficking in persons: 1) *Data collected for administrative purposes*. This refers to information collected primarily for administrative (not research) purposes. It is collected by government departments and other organizations (for example NGOs and IOs) for the purposes of registration, transaction and record keeping, usually during service delivery (for example healthcare, social work, legal assistance); and 2) *Data collected for research purposes*. This refers to the deliberate and discrete collection of data on a specific issue for the purpose of research. This may be collected by researchers, governments, NGOs, international organizations and private sector actors and may be collected by a range of methods (for example through interviews, questionnaires, focus group discussions, surveys) whether in person or remotely (for example, by telephone, online). There are also *emerging types of TIP data* that we consider in this paper, as TIP data collection may also increasingly include less traditional types of data, including data from supply chains, Open Data and Big Data. Regardless of the type of data or the stakeholder collecting it, TIP data collection involves a raft of complex legal and ethical questions to be identified and parsed.

4. Legal and Ethical Considerations in TIP Data Collection

4.1 Determining applicable law and relevant ethical issues

The human trafficking field is fairly new and so too are discussions around legal and ethical frameworks for TIP data collection. The development, further articulation and implementation of such frameworks are important in order to move forward to ethically and legally collect the information that is needed on trafficking in persons to prevent and prosecute this crime and to ensure victims' enjoyment of rights and access to protections. There is increasing emphasis on the need to ensure that any data collected is responsible data. How to collect responsible data in the trafficking context raises unique considerations and challenges for how to apply and adapt existing legal and ethical frameworks. While legal and ethical frameworks are different, although interrelated, the implications of responsible data collection apply to both.

In some countries and across some regions, legal and ethical frameworks surrounding TIP data collection (or even data collection generally) are more developed than in others. However, even where frameworks are well advanced, important questions remain about whether relevant stakeholders are fully informed about, comprehend and can implement these frameworks. Data collectors may lack awareness about the rules and risks involved in collecting data and may not always be in a position to engage in critical discussions about how to legally and ethically collect, use and manage data.

Determining what legal or ethical frameworks are relevant may not always be simple or direct. Different types of data collection will involve different legal and ethical considerations. For example, a specific framework for data collection and protection may apply for administrative data that is collected in the course of on-going work and is not specific to trafficking (for example, in criminal justice administration or provision of health care services, or in record keeping about welfare and housing). However, in the case of data that is collected specifically for a TIP data collection project, initiative or study there are important distinctions to be made with regard to legal and ethical issues depending on the type of data being collected and from whom. Some particular categories of data that merit particular care and caution include: data collection with vulnerable persons, including children and trafficking victims; data collection that includes personal and/or sensitive data, particularly when this data is collected about trafficking victims; data collection involving suspects and/or convicted criminals, including human traffickers; and data collection with anti-trafficking professionals and stakeholders.

While these categories of data have legal implications that a data collector *must* respond to (in order to be in compliance with the relevant laws), they also have ethical implications that a data collector *should* respond to, even in cases where there are not enforceable codes of conduct or minimum standards required by law. Our aim in presenting legal and ethical considerations alongside one another in this paper is to encourage the development of an ethical framework to accompany and strengthen the implementation of relevant legal and ethical frameworks for data collection.

4.1.1 Data collection with vulnerable persons, including children and victims of trafficking

Vulnerability can be understood as the diminished capacity of an individual to anticipate, cope with, resist and/or recover from the impact of trafficking or it can relate to the status or situation of a particular group (for instance, ethnic minorities or populations in particular situations such as prisons). The concept of vulnerability is relative and dynamic. While some countries recognize vulnerable statuses and offer certain protections in law, in other countries there is no legal framework to recognize and protect vulnerable persons.

Some laws require special measures to be taken where vulnerability factors are present in data collection. And when a potential subject of data collection is considered vulnerable or data collection involves vulnerable groups, specific ethical considerations arise. Data collectors must ensure that the information provided to data subjects about the data collection is adapted to the needs of any vulnerable persons and takes into account how best to approach informed consent.

To the extent possible, it is important to approach vulnerable persons about participating in data collection when they are at their least vulnerable. That is, a trafficking victim who is currently being actively exploited may be more vulnerable than one who is well into the process of recovery and has developed adequate social support and a sense of stability. When including a vulnerable group in data collection, attention is needed to the principle of "do no harm", including careful consideration of what data is actually needed (and what is not needed). In some situations, it will be appropriate to exclude a possible respondent because the heightened risk to the individual is not outweighed by the benefits of their inclusion (for example, if free and informed consent processes are jeopardized by circumstances, if the data collected is compromised or if the individual has no access to support services). On the other hand, it may be unfair to exclude a person from participation on the basis of their vulnerability.

Children are considered to be a vulnerable group and, in addition to the overarching vulnerability of being under age 18, many children have their own additional vulnerabilities. There are specific and complex legal and ethical issues that must be considered when engaging children in research or data collection. Application of the principle of "do no harm" in TIP data collection involving children means ensuring the "best interests of the child", a primary consideration to guard against emotional or physical harms and protect a child's rights and interests.

Ethical considerations regarding research on vulnerable populations need to also address the skills of the data collector. Consistent with the principle of "do no harm", those gathering information from vulnerable persons (including trafficking victims) should use a trauma-informed, culturally sensitive, rights-based approach.

4.1.2 Data collection that includes personal and/or sensitive data, notably data collected about trafficking victims

Personal data refers to any information that can be used on its own or with other information to identify an individual (data subject). An identifiable person is one who can be identified, directly or indirectly, by information, in particular by reference to an identification number or to one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity. An individual can be considered identifiable from the use of full names or a combination of identifying aspects such as physical characteristics, pseudonyms, occupation, address and so on. In TIP data collection, personal data is most frequently about trafficking victims.

Some personal data is considered sensitive data, presenting a greater risk to a person's private life than "regular" personal data if breached and, therefore, requires extra protection. Because certain categories of personal information could be used in a discriminatory way against an individual or even lead to the targeting of certain individuals, these categories are considered to be sensitive data and should be treated with greater care and be subject to more stringent restrictions.

When personal data is collected and stored for administrative purposes, breaches of confidentiality can have serious consequences. Breaches of confidentiality related to trafficking in persons constitute egregious violations of ethics and law. Such examples do not necessarily mean that personal data should not be collected – indeed, it may be necessary to

collect in order to effectively respond to TIP – but rather highlight the importance of ensuring that any data that is collected is also protected.

These are not uncontested issues and there are competing discussions around the collection of personal data within the TIP field. Researchers have noted that there is no longer an easy consensus on the social, academic or regulatory delineations of public/private in everyday life and practice. There are also questions to be asked about the sharing of personal data through emerging forms of data (such as biometric data) and technological tools such as smart phone applications (apps), particularly in light of recent enthusiasm in the anti-trafficking field to produce apps, which, in many cases, collect information about migrant workers and trafficked persons.

In some cases, ensuring the security of sensitive data requires the same level of protection be applied to de-identified data as explicit personal data. It is advised that those engaged in data collection should work to determine whether an individual or group of individuals is identifiable by considering all of the means reasonably likely to be used to single out an individual or group(s) of individuals.

4.1.3 Data collection involving suspects and convicted criminals, including human traffickers

Collecting data about persons suspected or accused of crimes (prior to a conviction) involves specific legal considerations, including privacy and confidentiality. Legal and ethical issues in data collection with and about traffickers will be informed by the stage of the investigation or prosecution process at which data is being collected. Suspects of the crime of trafficking must be afforded the same rights and protections in terms of data collection as victim of trafficking until the stage at which they are convicted of a crime definitively (that is have no further right of appeal).

Data collection with or about suspected or alleged criminals may test the legal limits of confidentiality. There are, for example, legal requirements in some countries for researchers and data collectors to report illegal or criminal activities of research subjects to authorities or risk legal consequences where they fail to do so. It is possible that the application of such laws may not necessarily be in the best interests of the data subjects or others who stand to gain or lose from data being divulged. In countries where legal requirements are not as onerous, the risks involved in sharing information – or of not sharing it – in the particular country context will require balancing the interests of data subjects against any decisions about data sharing.

Further, data collected about a suspected victim or trafficker while a court case is on-going may have evidentiary value to either a prosecutor or defense lawyer and, in some cases, a data collector could be subpoenaed to provide it and face legal issues for failing to provide such information. In some cases, risk of retaliation against a data collection subject or data collector is present whether or not a person on trial is convicted. These considerations raise concerns about providing evidentiary information and whether it should be collected in cases where its collection or use may raise serious risks to human subjects or data collectors.

It is possible that what is legal may conflict with what is ethical, placing data collectors in complex situations that can have profound bearing on the safety of a data collection subject and/or others, including data collectors themselves. There are no standard approaches as to how such risks can best be managed. In some cases, exemptions may be sought from requirements to report illegal activities. In other situations, the data collection project may be designed in such a way as to reduce the risk that data collectors will discover information that places them in difficult situations. In all cases, the interests of persons who are potentially placed at risk must be carefully and ethically balanced.

4.1.4 Data collection involving anti-trafficking professionals and stakeholders

Typically, questions around legal and ethical issues in TIP data collection focus on interactions with trafficking victims as respondents. However, there are also questions to be asked about issues that may arise with data collection with others in the trafficking field (for example, suspected or convicted traffickers, as discussed above, as well as anti-trafficking stakeholders, discussed herein). Some professionals (for instance under certain jurisdictions) may not be allowed to share information about their anti-trafficking work.

Part of addressing such challenges requires anonymizing information from key informants, so as not to identify individuals or even organizations or institutions. This is a particularly pressing issue in smaller countries or locations where there are only a handful of organizations or institutions working on the issue of TIP. Those working in more constrained political contexts may not be able to safely participate in data collection that may yield negative findings. Anti-trafficking actors must navigate various legal and ethical considerations as data providers (that is, individuals, organizations or institutions who provide data to the data collection effort) or data sources and may face risks when involved in data collection.

Risks to potential data subjects need to be carefully considered and communicated, consistent with voluntary and informed consent. At the same time, a disproportionate focus on protection measures may curtail reasonable approaches to enhance the TIP knowledge base. The response to risk should not be to set extreme limits on data collection. Rather, it is important to ensure that the ethical conundrums recognized and addressed are inclusive of the wide range of people who are involved in this field. Further, there should be continued thought and dialogue on the boundaries that are set around different types of data collection and subjects involving policymakers, practitioners and researchers.

4.2 Intersections between law and ethics in TIP data collection

Data collection on trafficking in persons requires looking to both law and ethics to realize the highest possible standard. Ideally legal and ethical requirements should align and be mutually reinforcing. However, this is not always the case. In some cases what is ethical and what is legal may conflict. In some countries, the laws that are in place fall short of what is ethical or may not align with the relevant ethical framework. For instance, while robust legislation allowing for significant regulations and oversight may, at first glance, seem to accord with a high standard of protection for the rights of data subjects, the legislation may, in practice, serve to undermine the protection of these rights. In some countries, data protection laws are not comprehensive or may not even exist. In these jurisdictions, personal data that is collected, stored and shared as part of TIP data collection or anti-trafficking responses may be technically legal, but nonetheless raise significant ethical issues. For example, harm may be caused by data collection that is carried out without fully informed consent, even if protocols and tools are in line with the legal requirements of the country where TIP data collection is occurring.

There are also external factors that influence whether legal data collection is indeed ethical. What is legal and what is ethical may come into particular tension in the case of less open political systems where data collectors may not have legal freedom to conduct data collection due to state controls. Equally in such political systems, the civil society and state actors involved in the anti-trafficking field may not have space or opportunity to speak freely (and safely). While carrying out data collection in such situations may be technically legal as far as the laws of that country are concerned, there are ethical considerations to be borne in mind, not least in terms of the well-being of respondents and key informants.

Conversely, what is considered ethical may not be legal. Conflict between ethical standards and legal requirements may arise in situations where data collection is conducted that may divulge information about an illegal activity. In some situations, data collectors or

researchers may themselves become liable to prosecution if they don't comply with the legal requirements of data collection, such as reporting crime. In some jurisdictions, the law requires confidential information to be released to relevant authorities, such as that relating to instances of child abuse. Compliance with such laws may raise risks to trafficking victims, particularly where their implementation does not adhere to ethical consent procedures and results in security breaches. In some cases, this can lead to important and otherwise ethical research and data collection not being undertaken. However, from an ethical point of view, it may be justified to undertake data collection and research that are intended to better the lives and safety of a vulnerable population and it may even be unethical to not conduct such data collection/research.

It is important to acknowledge the complexity around the ethics of TIP data collection, which requires predicting outcomes and consequences of action in complex social and political landscapes. This complexity must not discourage discussion about and reflection on these issues but rather encourage and facilitate the conversations that can deepen understanding. The risk of being too rigid is that researchers and data collectors will stop doing ethically complicated research/data collection, not least with vulnerable persons. And this may have negative consequences for our ability to respond effectively (and ethically) to the issue of TIP, including in the aid of vulnerable persons. Moreover, the possibility that vulnerable persons like trafficking victims would not be represented in TIP research and data collection is in and of itself an ethical concern.

Questions about what constitutes legal *and* ethical data collection are pressing in light of the global push for more data on trafficking in persons. The relationship between what is legal and what is ethical can be complex and varies from country to country or context to context. Indeed, each data collection project will raise its own specific legal and ethical issues. Although blanket generalizations cannot be made as to what the most appropriate approach is in ensuring that legality is assured and ethical concerns are properly addressed, it is clear that good practice is to act in a way that does not exploit lower standards of protections in a given country or context to serve data collection goals or alleviate burdens of carrying out data collection activities.

The reality is that good practice is highly contextual. A course of action or good faith attempt at ethical data collection in one country may have entirely different and negative consequences in another. For instance, in some cases, seeking government permission to collect data may be absolutely imperative to protect data subjects and other stakeholders involved, while in other cases, that exact same course of action may expose stakeholders and data subjects to significant risks. In short, while law and ethics can work in harmony, in practice, the line between what is ethical and what is legal is often not clear and the two may intersect (and conflict) in complex ways. Case-by-case assessments are required to take into account the specific legal, ethical and social contexts in which the data is to be collected.

5. Legal Frameworks in TIP Data Collection

Laws that are relevant to data protection have become increasingly prevalent globally, particularly with the emergence of technological means of collecting data. Government agencies, businesses, international organizations, non-governmental organizations and other actors have been using information technology to collect and store personal information in databases since the 1960s. Such databases can be searched, edited, cross-referenced and the data within them shared and disseminated rapidly throughout the world, raising significant questions about how this data – and more specifically, the right of data subjects – is to be protected. In response to questions concerning who owns data when it is collected and who has the right to access, change, delete and disseminate such data, data protection principles began to emerge that were eventually articulated and codified in data protection laws and regulations.

Considerations of legal issues and relevant legal frameworks for data collection in the anti-trafficking field are relatively new and quickly changing, particularly as new challenges emerge in light of increased cross-border data processing, rapidly advancing information communications technology (ICT) and the cyber-security risks posed as a result. Numerous and varying laws may apply when TIP-related data is collected. These are discussed in the following sub-sections.

5.1 Identifying relevant legal frameworks for TIP data collection

Data collection activities should comply with any applicable national legislation and, to the extent where the latter are more robust and protective, take into account relevant regional and international legal standards. These are unlikely to be TIP-specific, but instead will relate to data collection in general.

Relevant laws often are found in the context of data protection laws (privacy laws) and standards that uphold the right of all persons to privacy. These may also be found in the context of criminal justice data protections where data is collected about presumed victims or suspected traffickers. However, other laws may come into play and data collectors should consider all of the relevant legal issues that may emerge in TIP data collection. Laws and standards that may be relevant to TIP data collection and which, therefore, should be examined as part of developing the legal framework for data collection include:

- Data protection and privacy laws, for instance, concerning online and cloud-based data collection;
- Human subjects protection laws, in the context of research;
- Criminal justice laws, that may be relevant to the protection of suspected perpetrators and presumed or identified victims of crime; and
- Laws relating to anonymity (online and offline), that may either protect anonymity or compromise it (contrary to human rights concerning freedom of information and expression).

In determining the relevant legal framework for TIP data collection, what data ownership means for individuals (for example, trafficking victims) merits some discussion. Data first belongs to the individual to whom that data relates, who has a corresponding right to withhold consent or retract it in a given data collection process. However, in real terms an individual may have little or no control over how their data is used, and little or no power to stop its subsequent sharing or to require its destruction. The individual may be unaware of how the data is analyzed and not be informed of any changes to its use, let alone given an opportunity to consent or refuse. Furthermore, there may be no practical means of enforcing accountability to that individual. In short, while an individual has the right of ownership, they may not be able to effectively exercise that right. More generally there is a disconnect between what protections laws afford and how these protections work in practice.

Issues of ownership also arise for organizations and institutions engaged in TIP data collection. Activities may be subject to laws in the country which funds data collection or where the organization collecting data is established, as well as to the laws in the country/countries in which data collection activities take place. Given that several different legal frameworks may be simultaneously relevant, it may be unclear how conflicting laws can be reconciled and followed or, if they cannot be reconciled, which should prevail. Ethical principles are relevant in addressing and resolving these complex legal questions.

Data collection partnerships (and partners) may span several jurisdictions, making issues of data collection (and data ownership) increasingly complex and subject to different legal and regulatory frameworks. Multi-jurisdictional contexts are an increasing reality as cooperation in the anti-trafficking field becomes increasingly inter-agency and trans-border and as new

technologies emerge to support such work. When TIP data collection involves several jurisdictions, there is often a lack of legislative certainty on data ownership and responsibilities. This is further complicated by online activities such as the use of social networking sites and cloud computing and the fact that collecting personal data has become increasingly sophisticated and less easily detectable. Even in jurisdictions where there are more detailed laws and regulations concerning who owns data, frameworks may be inadequate to keep up with the emergence of new technology-based data tools and data collection capacity that raise additional ownership questions.

Determining the relevant jurisdiction for data collection activities can be undertaken by first reviewing the national legal framework for the country/countries where data collection takes place. If there are not relevant national laws or if data collectors want to uphold higher standards than required by the national legal framework, it is good practice to look to regional and international instruments in understanding the legal framework for TIP data collection. The following sections outline that framework.

5.2 National legal frameworks

Individuals have the right to have their personal data protected by national legislation and, indeed, states have an obligation to protect the privacy rights of their citizens. Data protection (privacy) legislation varies widely across countries. Many countries in North and South America, Europe and Asia have explicit laws on data protection and privacy. Where there is legislation in place, there is notable overlap between the principles captured therein, largely because much legislation is based on common frameworks. In general, the legislative frameworks that result are conceptualized as privacy law, meaning the broad category of laws that regulate the collection of personal information as well as the storage and use of personal information by governments, public organizations or private organizations. Specific subsets of privacy law are designed to regulate specific types of data collected. These include: financial privacy laws; health privacy laws; information privacy laws and online privacy laws.

Whether data protection laws constitute a subset of privacy law or involve different legislative instruments varies from country to country. In some countries, privacy protections are contained in constitutional law. In other countries, telecommunications or other laws may include privacy provisions. Data protection laws generally concern how personal information about individuals is used (collected, processed, shared, stored, destroyed, and so on) and in some cases, this may concern a person's privacy. Privacy laws may go beyond data issues, for instance, to include privacy in one's own home and a person's right to a private life. Some privacy laws touch on issues such as what the state or the media or others can and cannot do. Data protection laws and principles can, therefore, be seen as a subset of broader privacy laws and principles.

As data is increasingly collected across multiple jurisdictions, lack of legislative harmonization may result in gaps in protection for data subjects. While it is impossible to accurately generalize the range of different approaches taken by national legislation on data protection, the following succinct (and necessarily incomplete) overview is offered by way of a brief illustration as to what domestic data protection laws may look like.

Scope and applicability. Privacy/data protection laws apply to private and or public entities and explicitly exclude personal data collected or used for personal/domestic purposes. Privacy/data protection law provisions generally relate to data collection, recording, storage, maintenance, adaptation or alteration, use, disclosure, transmission, erasure or destruction (often broadly termed processing) and dissemination (often termed transfer). Dissemination provisions relate to transfer between countries, although in some instances, requirements are specified with respect to media use of data and publication of personal data.

Definitions. National laws generally offer a definition of both personal data (also called personal information) and sensitive personal data (sensitive data). Definitions significantly overlap across laws. Personal data generally relates to information of any kind about an individual that is directly or indirectly identifiable, whether by reference to an identification number or to factors such as physical, physiological, mental, economic or social identity. Increasingly, personal data is being construed to apply to that existing in cyberspaces, such as email and IP addresses. Sensitive data generally relates to information about an individual's physical or mental health, race or ethnicity, religion or belief, political or other opinion, labor union membership, sexual life, criminal record, habits, behavior or sexuality, among other characteristics.

Rights and obligations (or guiding principles). The rights of data owners or subjects are commonly set out in explicit principles in legislation. Such rights include the right to information, the right to access data, to correct data, to rectify data, erase, block data and to object and complain. Sometimes these rights are limited to citizens or permanent residents, potentially raising gaps for trafficked persons in irregular situations. The obligations of data controllers include the obligation to seek consent, to inform data subjects and regulatory bodies or government ministers of key events, to process data anonymously and maintain confidentiality even after the relationship between the controller and their employer or with the data subject has ended.

Regulating bodies and compliance. There are two categories of security measures to protect data: 1) technical measures, which refer to measures designed to keep data secure when electronic devices and equipment are involved (for example firewalls, anti-virus software, authentication and authorization systems); and 2) organizational measures, which refer to instructions, policies, and internal procedures governing how personal data are handled by the data controller. Privacy and data protection laws often establish regulatory bodies (called commissions, boards or supervisory authorities) and specify their key functions and powers. These regulating bodies are typically imbued with oversight, monitoring and mediating responsibilities, can request information and take measures to suspend or stop processing of personal data, issue complaints or receive and consider complaints and impose sanctions on data controllers who have contravened laws. Many laws also specify that Codes of Conduct should be drawn up to support implementation of the law.

5.3 Regional legal frameworks

Different regions are at different stages in the development of legislative and policy infrastructures for data protection. Some regional legislative frameworks are comprehensive; others are lacking. Moreover, even when regional frameworks do exist, they are not always implemented in practice. The most comprehensive approach – and one that has significant impact on the development of data protection regimes in other regions – is the European Union's framework.

European Union. The European Union has developed a robust framework for data protection, comprised of dedicated and mandatory data protection legislation that is currently being further strengthened in response to new technological challenges. The EU approach has far-reaching impact beyond Europe in setting standards of protection. In recent years, data protection in the EU has been reformed by two key instruments, the *General Data Protection Regulation* (GDPR) and a Directive specific to the criminal justice sector, to update and broaden the EU data protection framework that was adopted over twenty years ago. Additionally, the European Union legal framework includes human rights law protecting privacy as a fundamental right, as well as human trafficking laws that address aspects of TIP data collection. The regional legal framework relevant to TIP data collection in the European Union includes:

- European Union Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("General Data Protection Regulation") (2016)
- European Union Directive 2016/680 on data protection in the area of police and justice (2016)
- European Union Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims ("EU Trafficking Directive") (2011)
- Council of Europe Convention on Action against Trafficking in Human Beings (2005)
- European Union Charter of Fundamental Rights (2000)
- European Union Data Protection Directive 95/46/EC (1995)
- Council of Europe Committee of Ministers Recommendation Rec(87)15 regulating the automated processing of personal data in the police sector ("COE Police Recommendation") (1987)
- Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Data (1981)
- Council of Europe European Convention on Human Rights (1950)

Africa. Data protection initiatives are uneven across Africa. Where frameworks are in place, there are often disparities between the approaches taken with requirements in some sub-regions of Africa more robust than others (for instance, in relation to whether there are any restrictions in place for cross-border transfer of data and concerning notification of any data breaches). The regional legal framework relevant to TIP data collection in Africa includes:

- African Union Convention on Cyber-security and Personal Data Protection (2014)
- Supplementary Act A/SA.1/01/10 on Personal Data Protection within Economic Community of West African States (ECOWAS) (2010)
- East African Community (EAC) Framework for Cyber Laws (2009)

Asia-Pacific. In the Asia-Pacific region, there has been a surge in data protection frameworks enacted into national law, with stronger compliance demanded from governments. Particularly as data technology advances across the region, legislative frameworks have evolved to stay abreast of the privacy risks posed, resulting in a range of emerging cyber-security regulatory regimes. The regional legal framework relevant to TIP data collection in the Asia-Pacific includes:

- Association of Southeast Asian Nations (ASEAN) Framework on Personal Data Protection (2016)
- Association of Southeast Asian Nations (ASEAN) Convention against Trafficking in Persons (2015)
- Association of Southeast Asian Nations (ASEAN) Plan of Action against Trafficking in Persons, Especially Women and Girls (2015)
- Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (2011)
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005)

Organization of American States. The Organization of American States (OAS) does not yet provide a regional legal framework for data protection. However, it has undertaken significant work to understand the legal frameworks that are in place at the national level in the Latin American region and elsewhere, towards strengthening the approach of the OAS. The resolutions and recommendations related to the development of a regional legal framework that could be relevant to TIP data collection in the OAS include:

- OAS General Assembly Resolutions 2514, 2661 (2011)
- Draft Principles and Recommendations on Data Protection (2011)

5.4 International law

International law that may apply to TIP data collection ranges from laws specific to trafficking in persons to laws specific to data collection, particularly those protecting the human right to privacy. States parties to international legal instruments must implement those instruments at the national level. Notably when it comes to data protection, legislative frameworks at the domestic level more frequently draw from regional than international instruments. Nonetheless, as TIP is addressed by a growing body of international law on transnational organized crime, it is important for data collectors to consider the international legal framework for anti-trafficking work and how that framework may apply to data collection. This refers primarily to the United Nations *Convention on Transnational Organized Crime* (UNTOC) and the *Trafficking in Persons Protocol* (UN *Trafficking Protocol*) supplementing it, the key international legal instruments relevant to trafficking in persons.

5.5 Guidelines, manuals and procedures

How all of these legal frameworks operate in practice (at the institutional or organizational level) varies quite substantially, with differences in the practical implementation of various rules and requirements. Several legal tools exist to support states in the implementation of data protection legislation. In addition, it is necessary to consider the laws that may apply to trafficking-related administrative data, including data about victims being assisted by the state or an NGO (for example, medical files, case files of social workers, psychologists) or data about the criminal justice sphere (for example, investigations, prosecutions, convictions). Administrative rules, regulations, procedures will operationalize such legislation, which can provide practical guidance on how to adhere to and operationalize the relevant laws and regulations in day-to-day operations.

The collection and protection of data will be also guided by the institutional rules and procedures of the relevant institution or organization collecting the data, which may be introduced to comply with existing legislation or may be implemented irrespective of any legislation. Such internal requirements on how data is collected and managed are not likely to be trafficking-specific but most often will be incorporated into general rules and procedures.

5.6 Summary

While most countries have some privacy laws in place, the extent to which they are comprehensive and effectively implemented varies significantly around the world. Many countries in North and South America, Europe, Africa and Asia have explicit laws on data protection and privacy, with more and more countries introducing such laws and revising existing laws to address emerging challenges. Notwithstanding the differences in how data protection is captured in domestic legislation, there is notable overlap between the principles captured therein, largely because much legislation is based on common frameworks.

At the regional level, the most comprehensive approach (and one that has significant impact on how other regions develop their data protection regimes) is the European Union's framework and the recent GDPR. The impact of this rigorous framework is manifesting not only in national legislation of EU countries but also in countries elsewhere that will amend their legislation in accordance with the practices and principles that are set out therein.

TIP data collection may trigger the applicability of different types of law, such as transnational criminal law relating to the crime of trafficking in persons or international human rights law. In the last few years, several states have taken steps to introduce stronger data protection legislation to respond to demands for new data and the challenges posed by new technology to collect it.

Which categories of law (and within them, which provisions) are relevant to TIP data collection and protection will vary significantly depending on the specifics of the data collection initiative. The multiplicity of data collection partners, the role of technology and the multiple jurisdictions that data owners may be operating in raise questions about data ownership and may present the actors involved (whether NGO, state institutions others or a combination thereof) with significant challenges in understanding and applying their protection obligations. Given that several different legal frameworks may be relevant simultaneously, complex questions arise when the laws of the relevant countries conflict in terms of how they can be reconciled, or which should prevail in the event that reconciliation is not possible.

The effectiveness of any legal instrument depends on the extent to which it is implemented in practice. As TIP data is collected using increasingly advanced methods by an ever-diversifying range of actors, the legislation governing its protection will need to continually evolve to keep abreast of emerging protection risks. Furthermore, as data is increasingly collected in ways that traverse international borders, legislation will become increasingly extra-territorial in scope and application, highlighting the benefit of harmonizing legislation in accordance with the most rigorous standards. The implications that new and ever-evolving legal frameworks may have on TIP-related data and the rights of data subjects involve emerging issues that bear consideration and on-going, multi-sectorial discussion.

6. Ethical Frameworks in TIP Data Collection

Ethical principles should underpin all TIP data collection activities, whether data collection involves research data or administrative data. Each data collection project will require attention to how to specifically attend to ethical issues at each of the stages of data collection, from design and planning, through data collection, storage, maintenance and management, analysis, use, presentation and dissemination, including as issues change and arise over time. As the field of data collection ethics evolves, this is a critical time for anti-trafficking actors to consider how to ensure TIP data collection activities are ethical.

There is no universally accepted definition of ethics. Ethical principles are understood as referring to those general judgments that serve to justify decisions about and evaluations of human actions. The genesis of research ethics was in the field of medical research and born of the grossly abusive practices that took place in the context of Nazi biomedical experimentation in concentration camps during World War II. While the origin of research ethics principles is anchored in medical research, it is a continually evolving field with its scope broadening over time.

There is no all-purpose model for an ethical framework for TIP data collection, not least given the diverse group of stakeholders involved in TIP research and data collection. Much TIP data collection involves administrative data, such as data about victims who are being assisted (including by medical staff, social workers and psychologists in state-run institutions or NGOs and so on) and data about suspects and criminals (including investigations, prosecutions, convictions and so on). It also includes data that may be collected by businesses (for instance about workers in supply chains). Such data may be proprietary data and, thus, not the subject of traditional ethical frameworks but rather the subject of legal requirements, including confidentiality agreements. Much TIP data collection involves human subjects, which raises specific ethical implications. Other TIP data collection does not involve human subjects research but still requires an ethical framework.

In the trafficking field, more trafficking-related research is being conducted under the umbrella of health research, highlighting the potential applicability of ethics in medical and health-related research contexts to other areas of research and data collection, including TIP. The most current challenge is how to adapt this model to data sciences (including Big Data

and Open Data analytics) that are often undertaken by actors who have no experience of applying ethical principles or subjecting their work to ethical review.

Different approaches have been taken to ensure ethical data collection in the field of trafficking in persons. While the appetite for data on TIP has increased in recent years, awareness of the ethical requirements for different types of data collection has not increased commensurately. Globally there is an increased impetus to strengthen ethical capacity in research and data collection across a range of fields including trafficking in persons. Different approaches may be used to ensure the adherence to ethical standards in TIP data collection including: ethics review; research and data collection partnerships; self-administration of ethical standards and guidelines; peer review procedures; and informal third-party engagement in protection. In some cases, a combination of approaches may be used.

6.1 Ethics review

Ethics review is the review and approval (or rejection) of research proposals and oversight of research activities. The most common form is through Institutional Review Boards (IRBs), established at specific institutions to carry out reviews of research conducted by that institution. Some IRBs have been specifically established to provide ethical oversight to research and data collection work in international or multi-country contexts. While not yet the case in the field of trafficking, this offers one possible way forward as attention to ethics and the demand for ethics review gains traction in the anti-trafficking field, for research as well as other types of TIP data collection. There are also private, independent IRBs that provide ethics review services, although none specialized in the field of trafficking in persons.

IRB membership is generally governed by a set of standards guiding the number and composition of its members. In the case of TIP-related research, IRBs would be strengthened if membership included individuals with a trafficking-related background and/or included former trafficking victims, migrant workers or other representatives of the community relevant to the study. In the absence of a standing member that fits such criteria, IRBs often have a mechanism for consulting with subject experts on a case-by-case basis. While common for universities, IRBs are not generally used for research and data collection being conducted by NGOs, international organizations and the United Nations.

While there are many arguments for the strength of the IRB model, there have also been questions about the quality and rigor of ethics review. Even within universities, some types of TIP data collection (for example, Big Data and Open Data) are often not subject to ethics review, in spite of generally being based on human subjects research and high levels of personal data. Others have critiqued IRBs for affording no significant advantage in terms of either the research outcome or the ethics, with IRB members having little research experience themselves or inadequate understanding of the subject matter to determine what are or are not ethical procedures.

To benefit TIP research, such processes must be adapted to the reality of how TIP research is conducted and by whom, including how to accommodate short funding timelines and emergency responses that are the reality of much TIP data collection work. It is also important that donors take into account the cost of ethics review as well as the time involved to seek and obtain ethics approval.

6.2 Research and data collection partnerships

Research and data collection partnerships may include various constellations including between an NGO and university or research institute; the UN and an NGO; a government ministry and a university or research institute; and a combination of the above in multiple

stakeholder partnerships. In some instances, partnerships between data collectors (or between researchers) can import ethical standards and provide oversight to data collection activities. When an entity with no formal ethics review process in place partners with an organization that does undertake ethics review, there may be an explicit policy to rely on the formal ethics review process.

In some cases, partnerships serve to augment ethics oversight through the adoption and application of one partner's ethical principles or guidelines within the data collection partnership. Engaging researchers with experience in ethical principles and approaches to TIP data collection can also introduce ethical oversight to a research study or data collection effort, even without formal ethics review. Increasingly, service-providing NGOs are partnering with researchers or research institutes, resulting in the marriage of relevant expertise and data and bringing research ethics to situations where they may otherwise be lacking.

Some partnerships may involve multiple stakeholders. Partnerships can offer significant benefits, primarily by linking, on the one hand, research and ethics expertise with, on the other hand, subject-matter expertise and access to various types of data. Another possible model for partnerships involves working with vulnerable persons or communities to determine how data is collected.

That being said, partnerships in their various forms may serve to facilitate research or data collection, but not necessary strengthen ethics. It is the specific nature of the partnership and the mechanisms and tools used that will determine good practice and address the range of ethical issues to be faced in the specific TIP data collection effort.

Some partnership arrangements between anti-trafficking actors risk diluting ethical standards when responsibilities are allocated to the partner that has least capacity to fulfill them. Such arrangements can result in the lowest standards of data collection being defaulted to. On the other hand, partnership arrangements can also serve to raise standards (for instance, while there may be no legal requirement to obtain informed consent in a given study, the partnership agreement may require it, and the more able partners may work to build capacity of others).

6.3 Self-administered ethical standards and guidelines

Another approach is the adaptation and application of ethical principles to the design and conduct of data collection activities. This approach is largely self-administered and *ad hoc* in nature. It may involve individuals involved in a given activity looking to principles and guidelines that have been developed externally by other actors in developing their own activities. Alternatively, internal guidelines that include ethical guidance may be developed by an organization. Sometimes a combination of approaches is applied (for instance, where internal policy guidelines will specify which external ethics guidelines are to be complied with in the context of the research or data collection initiative). Indeed, there are several tools that have been developed that are applicable both to data collection in general and to trafficking-related data collection specifically.

The ethical standards and guidelines that have been developed may represent strong expertise and international good practice. However, there is some disagreement between practitioners as to whether there is adequate written ethical guidance available. Some practitioners maintain that existing guidance is available but that it is deficient with respect to real-world application. For example, the common requirement that research respondents should sign a written consent form as part of the informed consent process may be out of step with the reality of research and data collection on the ground (for example, where some respondents may not be literate or may be suspicious of signing such a consent form). Others maintain there is adequate material available but that it needs to be better operationalized,

as the tools that are available are not always well-suited for application in the field (for example, guidance and tools being too difficult for practitioners to apply or not available in a relevant language).

There are some self-administered tools and guidance that are currently used by frontline data collectors and researchers in the TIP data collection field. In addition, there are professional and research codes of ethics and guidance that are not specific to trafficking but that offer relevant guidance that can be applied to TIP data collection. Relying on existing, publicly available policies and guidelines avoids unnecessary duplication of efforts.

However, self-administered ethical standards may not always amount to sufficient ethical oversight. The largely voluntary nature of this approach may mean that guidelines are inconsistently adapted and applied. Often, there is no monitoring mechanism in place to check that data collection has complied with the principles and guidelines and there may be no system in place to identify and address ethical issues that arise as a result of deviations from them. The development of internal ethical research and data collection policies and mechanisms of oversight can be instrumental in addressing those risks.

6.4 Peer review processes

Generally, peer review processes are employed by academic journals and books to ensure that published research is of an adequate standard. However, it is also an approach used by some organizations to bring a critical lens to a study or data collection project and could be used to a greater extent in the field of TIP data collection. Peer review mechanisms may include informal review by a group of relevant peers or may involve a mechanism of internal review within an organization. Peer review can be used to offer ethical oversight to the design and implementation of data collection projects as well as how data is presented for use and dissemination. One variation of peer review is an external reference group, also sometimes called a research advisory group. An external reference group is comprised of individuals who provide expert advice and guidance throughout the data collection process. A reference group may also include persons with direct experience of the issue being studied, which, for TIP data collection, might include former victims of trafficking.

Some organizations voluntarily subject their research and data collection to peer review to augment and ensure research quality, even when not publishing in an academic journal. While generally not required by an organization or donor, and often in fact not budgeted for by donors, it is advantageous to the overall outcome. Another variation of peer review involves including data collectors in reviewing and validating the research results. Yet another approach might involve respondents from a particular project reviewing the study, whether victims of trafficking, their family members, community representatives or anti-trafficking stakeholders. Such an approach would need to address various issues, including how results are shared (for example, for a less literate population versus a more literate one), recognizing language barriers, allowing for adequate time to review and provide feedback as well as giving some consideration to compensation.

While traditional peer review contributes to ethical rigor, it is generally associated with academic publication (generally for purchase and often only available in English) which means that results are not generally accessible to NGOs and governments at the frontline of the anti-trafficking response. The relatively slow pace of publication of formal peer review research also impacts the timeliness of research results in the fast-moving field of trafficking in persons.

6.5 Informal third-party engagement in protection

In some cases, ensuring ethical data collection can occur through other channels or due to the involvement of third-parties. Such involvement may be incidental to the data collection

activity or it may be done intentionally to guard ethics (for example, to mitigate risks to data collection subjects). Examples of third-party engagement in data protection include: third-party guardians appointed in child protection cases; consultation with community leaders; and service providers as gatekeepers.

An example of third-party involvement that is incidental to data collection is where children are enrolled in state child protection systems and have an appointed guardian safeguarding their best interests. In such cases, that appointed person has a responsibility to vet the engagement of the child in data collection activities. In other cases, researchers and data collectors may take active steps to engage third-parties in the design and implementation of research activities with the express purpose of mitigating any risks to subjects. This approach can take many forms, depending on the context.

This approach (informal third-party engagement in protection) raises ethical risks itself, notwithstanding that there may be no direct contact with potential research participants. For instance, consultation with parents of potential research participants can raise particular risks for the children, when, for instance, the impression is given to parents (rightly or wrongly) that their child falls into a particular category of interest to the study that the parent was not previously aware of or does not clearly understand. Or the involvement of government officials, law enforcement or private sector actors as gatekeepers may result in coercion, when, for instance, children are given no meaningful choice to participate in data collection or alter the information that they share due to pressure from the gatekeeper. Such risks are not unique to children; care must be taken with all trafficked persons that research or data collection does not out them to those in their family or community.

6.6 Summary

While research ethics principles have their origin in medical research, they are evolving to apply also to the social sciences and other fields. The wide range of actors and types of research and data collection being conducted in the human trafficking field raises complex questions as to how ethical principles and good practice standards can be adapted to ensure ethical data collection in the field of human trafficking.

Much TIP data collection involves administrative data, such as data about victims who are being assisted (including by medical staff, social workers and psychologists in state-run institutions or NGOs and so on) and data about suspects and criminals (including investigations, prosecutions, convictions and so on). It also includes data that may be collected by businesses, for instance about workers in supply chains. Such data may be proprietary data and, thus, not the subject of traditional ethical frameworks but rather the subject of legal requirements, including confidentiality agreements. Some TIP data collection involves human subjects, which raises specific ethical considerations as to how that data is collected and processed. At the same time, a significant proportion of TIP data collection does not involve human subjects research and yet still requires ethical oversight. The ethical implications of these variations of TIP data collection must be carefully considered and addressed.

Different approaches have been taken to ensure ethical data collection in the field of human trafficking. Ethics review by an Institutional Review Board (IRB) or ethics committee offers a valuable safeguard for research subjects. However, there are also limitations to ethics review for some trafficking research and data collection and, accordingly, practitioners have applied other informal mechanisms and *ad hoc* approaches to apply ethical principles and standards to their data collection activities.

In some instances, partnerships between different entities carrying out data collection or research can import ethical standards and some degree of oversight. This might include when research and data collection are carried out in partnership with government ministries

involved in the anti-trafficking response or with academic institutions that have in place mechanisms for ethical oversight. Partnerships can offer significant benefits, primarily by linking research and ethics expertise with trafficking expertise. That being said, partnerships do not necessarily ensure a satisfactory standard of ethics.

Another common approach is to apply pre-existing general ethical principles to the design and conduct of trafficking-related data collection activities. This approach is largely self-administered and *ad hoc* in nature. It may involve adapting and applying external guidelines or elaborating internal ethical guidelines. Relying on already-developed policies and guidelines offers the distinct advantage of benefiting from existing and tested tools. Many organizations adhere to Codes of Conduct that are either specific to their organization or more generally apply to a field or profession.

Peer review is also an approach used by some organizations to bring a critical lens to a TIP study or data collection project. Peer review mechanisms (including the use of a reference group) may include informal review by a group of relevant external peers or internal review within an organization. Peer review can be used to offer ethical oversight in the design and implementation of data collection projects and the use and dissemination of data. Yet another version of peer review might involve data subjects being part of the peer review process.

Finally, in some cases, the involvement of third-parties can offer a measure of ethical oversight in data collection. Such involvement may not be a matter of policy but incidental to the data collection activity, or it may be intentionally sought with ethics-specific goals such as mitigating risks to data collection subjects. An example of the former is when children are enrolled in state child protection systems and have an appointed guardian safeguarding their best interests who acts as a gatekeeper to any data collection involving their charge.

Ethical principles should underpin all TIP data collection activities, whether involving research data or administrative data. Ethical issues arise at each of the stages of data collection and may change over time. As the need and desire for data on trafficking in persons increase and data collection activities are carried out by an ever-widening range of state, non-state and private actors, it is critical that those involved in this work take stock of the ethics of their data collection activities and explore options for strengthening the standards and principles that govern them.

7. Emerging Issues in TIP Data Collection

The principles of legal and ethical data collection that have been developed, and the legal and ethical frameworks that have evolved on the basis of those principles, must be adapted to the emerging issues that advancements in data collection present. The following sections address some of these issues, with respect to: information communications technology (ICT) and third-party technology providers; Big Data; Open Data; and private sector engagement in anti-trafficking.

These sub-sections are not mutually exclusive but rather overlap and intersect with one another. For example, many issues identified in terms of ICT will be relevant to the work being done by private sector actors and to the accountability of supply chains. Similarly, ICT and third-party technology providers intersect in clear ways with the collection and use of Big Data and Open Data. Moreover, many of the legal and ethical considerations are cross-cutting, running through each of the sections below.

7.1 Information communications technology and third-party technology providers

Increasingly, data collectors and anti-trafficking actors are paying attention to how to leverage ICT to enhance TIP data collection. Many forms of TIP data collection are increasingly being supported by new technologies as well as the engagement of third-party technology providers. Third-party technology providers are increasingly reliant on ICT to provide the machinery that collects and/or stores data – for instance, when smartphones and other devices collect data and feed it into a storage platform for processing. In this example, ethical and legal questions arise, including questions about data ownership; such questions are further exacerbated in the context of Big Data. In short, ICT raises many and varying legal and ethical issues with respect to discussions around TIP data collection. These relate to data ownership, data sharing, reliance on technology partners and ownership and responsibility.

7.1.1 Data ownership in the context of ICT

Issues surrounding ownership of data are extremely challenging in the context of ICT. This is due, in large part, to the many actors – both government and non-governmental – engaged in anti-trafficking work utilizing ICT. Indeed, the diversity of stakeholders can complicate and blur lines of data ownership. While states are primarily responsible for implementing measures to address trafficking in persons under international law, non-state actors – including NGOs and international organizations and, increasingly, third-party providers from the private sector – provide fundamental support to states' efforts to fulfill their obligations. In some countries, responsibilities (notably, to protect and assist trafficking victims) have been outsourced to local or foreign NGOs. When data is collected by those organizations in the context of their daily work or as part of discrete research and data collection, it may be unclear who owns that data. Which laws and regulations apply to determine data ownership, responsibility for protecting data, rights of access and who can or should bear the costs of using data (and the implications thereof), are questions not easily answered and have been the subject of complex litigation.

7.1.2 Data sharing with third-party technology providers

Ambiguity of data ownership can pose a barrier to free flow of information, resulting in stakeholders not sharing data. Alternatively, lack of clarity can also result in over-sharing, whereby data is shared with third-parties that need not – and perhaps should not – have access to it. Firewalls may need to be put in place to ensure that data collected for one purpose, for instance to protect victims of trafficking, is not used for other purposes, such as immigration management or law enforcement. ICT has a significant impact on the way that data is shared and the control that can be exercised. Whether and how data is shared may be mandatory or optional, depending on the source of funding, the nature of the organization, legal limitations and other factors that must be weighed against both the benefits of sharing and the potential risks of doing so, particularly for data subjects. Explicit agreements or contracts that govern data sharing may introduce some control, but these are not always in place or well understood, or may have questionable grounds across several jurisdictions. In practical terms, it is ultimately the actor that has the *capacity* to share data who makes such decisions about whether and how to do so. Here again, the fact that different actors are involved in data collection (individual researchers, NGOs, IOs, government, private sector actors), becomes relevant.

7.1.3 Reliance on third-party technology providers

In a landscape of growing technological resources available for data collection and storage, issues arise concerning capacity of users to protect data. For instance, when a technology company develops a technology-based method of data collection and provides (or even sells) that method to data collectors, it must be considered whether the user (potentially a victim service provider, police officer, social scientist) has capacity to use that technology in a way that adequately protects privacy. When actors are dependent on technology provided by

third-parties, they may not have full control over the data that is collected by them and may even have to pay to receive or have access to their own data. There are also questions to be asked about how data is stored. The pros and cons of storing the data locally or with a third-party must be weighed against questions of ownership. While local storage (for example, on a personal computer) may offer greater clarity in terms of ownership, it may be less physically secure from theft, damage or loss. On the other hand, storing data remotely (for example, on a network or in the cloud) may result in greater physical security of the data but require more reliance on third-party providers, less clarity as to its ownership and less control over who can access it and for what purpose.

7.1.4 Anti-trafficking responsibilities of ICT providers

Issues and questions about ownership and responsibility also arise when human traffickers use ICT or when ICT is utilized in committing human trafficking crimes. Whether data subjects (for instance, people with Facebook profiles) own their data or whether their data is owned by the relevant ICT platform is not necessarily clear to those users.

7.2 Using Big Data in anti-trafficking work

There is increasing discussion in the anti-trafficking community around the ways in which Big Data can be leveraged to address human trafficking issues, including building a better understanding of the issue. Such efforts have taken a variety of forms, whether by new actors who have developed particular interest in combating trafficking and related forms of exploitation or by existing anti-trafficking actors partnering to pool their datasets. Actors involved in Big Data activities may have different agendas that may impact how they plan to use the data and be guided by different understandings of the phenomenon. In the anti-trafficking context in particular, emerging concepts such as “modern slavery” that lack agreed, legal definitions may result in divergent understandings of distinct but overlapping phenomena, that impact what data is collected and how it is captured and analyzed. TIP data collection that involves Big Data raises complicated legal and ethical questions.

7.2.1 Risks posed by Big Data

Depending on how Big Data is used, by whom and for what purposes, the risks posed to the persons about whom the data is collected may be minimal or significant. This human element is crucially important in understanding the implications of Big Data. That is, what is collected, how it is analyzed and what is done with it ultimately depends on the humans involved and the judgments they make. In Big Data contexts, the links of responsibility and accountability that exist between the research subject and the data collector are severed by the distance between the initial data collection and its reuse. This raises risks both for individuals and communities that can be difficult to predict and mitigate. Tensions between protection and Big Data are on-going and many scholars and technologists are grappling with how to protect individuals when analyzing and working with Big Data.

7.2.2 The need for oversight of Big Data

Against this backdrop and a growing catalogue of potential or actual harms caused by Big Data, there is a recognized need for robust and flexible legal and ethical frameworks that can adapt to emerging issues across all spheres of inquiry, not just concerning trafficking. A rising body of literature reveals there is a growing divide between established laws, regulations and ethical frameworks surrounding data protection and Big Data. Earlier ethical frameworks were not drafted in anticipation of large-scale, high-tech research methodologies, leaving uncertain whether or not they apply. This is not dissimilar to another long-standing tension between social sciences research and the research regulatory framework that is primarily designed for biomedical research. Efforts to build an ethical framework for TIP data collection should be cognizant of the on-going challenges involved in adapting biomedical science approaches to social sciences. They should build on lessons learned from that experience in adapting those approaches again to emerging data and computer sciences. The various tools and guidelines that have been and are being developed

in relation to Big Data echo the principles offered in relation to data protection more generally, underlining their importance not only in traditional forms of research and data collection but also in emerging methods.

7.3 Using Open Data in anti-trafficking work

Open Data is data that has been collected by an organization or institution and is subsequently made publically available, subject to the necessary data protections. Open Data may come from the government or from other organizations like NGOs or international organizations (for example in the form of administrative data or case management data). Open Data might include de-identified, anonymized information about trafficking victims who have been assisted by a service provider; persons considered at risk of trafficking from high sending areas; perpetrators from criminal justice actors and so on. Open Data can be used, re-used and shared by anyone – subject only, at most, to the requirement to attribute and share-alike.

7.3.1 Opportunities of Open Data

There are myriad potential benefits of Open Data on TIP. It offers information to a wide range of professionals who can then analyze that information in the design of anti-trafficking programs and policies. The opening up and sharing of some datasets can be a cost effective and efficient way to conduct TIP research and analysis. This points to the high order question of the potential for harm when Open Data is *not* made available and used.

7.3.2 Risks and issues with Open Data

Open Data raises complicated legal and ethical questions, including around data protection issues, issues of consent, potential misuse of Open Data and lack of ethical oversight. All governments have limitations as to what data can be released publicly; governments have a duty to protect privacy and secrets, as prescribed by laws. Most common limitations are protection of privacy, commercial or state secrecy. Certainly, care is needed in terms of data protection, to protect the privacy of all data subjects and adhere to legal requirements. And this is a challenging process, not least in terms of de-identification of personal and/or identifying data. One central concern necessarily must be as to whether Open Data could, in anyway, be identifying. This is something that needs careful thought given the evidence in the field of Big Data that even the most seemingly anonymized and removed datasets can potentially be de-anonymized and reconstructed.

7.4 Private sector engagement in anti-trafficking

Increased emphasis on corporate social responsibility and the pursuit by NGO and international organizations of alternative funding sources has led to an increased role of actors from the private sector in anti-trafficking work. Private sector actors may have a fundamentally different culture of information gathering, use and ownership than traditional anti-trafficking actors. There may also be differences of approach within and between private sector actors. Issues arise in all business environments including: the traps in non-disclosure; the potential to manipulate data and findings; the possibility that concerning findings do not translate to change; the possibility that auditing becomes an end in itself; the notion that supply chain change comes in response to consumers and is thus dependent on the market; the potential for private actors to deflect blame onto the state or other actors; attempts to separate TIP in supply chains from exploitation and other labor rights violations; and the idea that structural and systemic flaws may remain.

7.4.1 Supply chain accountability

Perhaps the most common form of private sector engagement relates to supply chain accountability. Recent attention to keeping supply chains “free” from human trafficking and exploitation has led to increased private sector and business engagement in the anti-trafficking field. Large corporations whose supply chains have been scrutinized are now also

anti-trafficking stakeholders. Even when private sector or business actors are acting in good faith to rid their supply chains of exploited labor, questions arise about the data that is collected to do so. Issues with this form of data collection relate to the conditions under which data is collected, who collects it, who owns it, who it is shared with, how it is used and how these processes and outcomes may impinge on rights of workers and employers.

7.4.2 Public-private partnerships

Some NGOs that conduct audits and otherwise engage in supply chain accountability also work on other elements of anti-trafficking efforts, including victim protection and advocacy. An NGO service provider that assists victims will collect data about its work and, thus, data collection may serve the primary purpose of providing assistance to trafficking victims. But when this organization takes on the additional role of engaging with private sector partners, there may be a secondary purpose of the data gathered (that is, to know about businesses that are potentially exploiting their employees). The donors for such an initiative may be public (the state that hosts the assistance program, other states from where victims derive or third states that are funding anti-trafficking activities) or they may come from the private sector, or be a combination of both.

7.4.3 Defamation and other risks of collecting private sector data

Data collection about private sector actors, including but not limited to supply chains, may also pose a risk to those collecting the data, whether as researchers, NGOs, governments auditors or private actors. There is a legal framework to be considered when collecting data about TIP in the business sector including the risk of retaliation by the company, defamation charges, among others.

7.5 Summary

As capacity to collect and process data expands and accelerates, new opportunities emerge to harness this capacity towards strengthening anti-trafficking efforts. However, alongside opportunities are emerging challenges in protecting data and the rights of data subjects.

On the one hand, the use of ICT for TIP data collection may result in increased protection of data and data subjects' rights and a greater evidence base for mounting responses. On the other hand, the use of ICT can pose unpredictable risks, raising questions about who owns the data and how and with whom it is shared. Related challenges emerge with increased collection of Big Data. While trafficking-specific Big Data is currently lacking, increased attention has been paid to exploring the possibilities of its use. As the link between data subjects and Big Data owners/processors becomes more distant, researchers risk losing sight of how rights can be affected.

Similarly, increased attention is being paid to how Open Data can be harnessed to strengthen understanding of trafficking and inform responses. At the same time, the risks are yet to be fully explored, including the risks – as with Big Data – that the data has not been ethically obtained and is not adequately anonymized to protect sources and others. Another concern is whether Open Data can be misused by well-meaning actors who lack the capacity to effectively analyze it or even by traffickers who may gain some advantage from this information.

As anti-trafficking becomes an increasingly multi-disciplinary field, with ICT providers engaged in responses and businesses being encouraged to prevent exploitation in their supply chains, stakeholders with different agendas are increasingly engaging with each other. The intersection of these different perspectives has enormous potential to strengthen data collection. But there may also be some deficits, particularly as public and private sector interests conflict. These risks need to be mitigated in a complex and often multi-jurisdictional landscape of overlapping legal and ethical responsibilities.

Many of these challenges are not necessarily unique to anti-trafficking work. The far-reaching scope of new forms of technology and its potential for positive and negative impact are being discussed in many fields. And there is value in anti-trafficking actors engaging in and learning from discussions taking place about emerging challenges, particularly in ICT, Big Data and Open Data. The lessons learned in that general context need to be carefully considered in light of the specific risks involved in addressing the serious crime of trafficking.

In working towards stronger protection of data and the rights of data subjects, it is crucial to recall that the principles underpinning data collection remain unchanged by emerging and evolving issues. Anti-trafficking actors are not required to develop new ethical and legal principles to guide their collection of data. Rather, they are called upon to creatively adapt ways to uphold these principles, in the complex and ever-changing landscape of global TIP data collection.

8. Conclusion

This paper is intended as a starting point in what we hope will be an inclusive, dynamic, challenging and reflective discussion of legal and ethical considerations in TIP data collection, toward determining how these considerations can be practically implemented. Our aim is to contribute to thinking and discussion on data collection issues that the anti-trafficking field is now grappling with. Certainly, it continues to be of critical importance to reflect and debate on ethics and law in the collection of more traditional forms of data (that is, research data and administrative data). But as important – and possibly more so given its emerging and less-developed nature – is the need for a robust and nuanced discussion around what constitute ethical and legal ways to collect TIP data in the era of ICT and third-party technology providers, Big Data, Open Data and data collected by, for and about the private sector.

We consider this to be an opportune time for those collecting data about TIP and related phenomena (including modern and contemporary forms of slavery, forced labor and child sexual exploitation), as well as funders of TIP data collection and research to engage in this important, sometimes difficult and always challenging discussion in order to move forward in the best possible way to collect the information that is needed to prevent and combat human trafficking globally, in ways that are ethically and legally sound.

The following principles are based on those that frequently occur in both ethical guidance documents and legal frameworks. In formulating the principles below, particular consideration has been given to key sources of ethical guidance and key legal frameworks. These principles offer a strong foundation and common ground for raising standards in collecting data, protecting its sources and effectively applying that data to strengthen responses to human trafficking.

Lawfulness and fairness, including the notion of “do no harm” and maximizing benefits;

Ensuring that data collection is **time-bound and for specific and legitimate purposes**, meaning that data can only be collected for limited purposes and kept for no longer than is necessary to fulfill those purposes;

Integrity, meaning that collected personal data is accurate, kept up to date and deleted when no longer necessary to fulfill the purpose for which it was collected (or according to the terms of data collection);

Voluntary and participatory, ensuring free and meaningful consent is given to participation and that that participation is voluntary; data subjects should be engaged as partners in the design and implementation of the research or data collection initiative, as well as in the use and distribution of any outputs;

Transparency and accountability, so that participants are given accurate information about any data collection and have recourse for any harms caused by data collection or its use;

Privacy, anonymity and confidentiality, so that the data collection is anonymous and personal information is kept confidential;

Safety and wellbeing, so that the design and implementation of any data collection activity ensures the safety of persons involved, including data subjects, data collectors, interpreters and community members; and

Security, meaning that data is stored and shared in a way that protects it from unauthorized access or use.

Consideration about how these principles apply to TIP data collection specifically is a fairly new discussion in the relatively young, emerging field of human trafficking. The evolving and divergent nature of what constitutes TIP data collection and by which organizations, institutions and companies it is undertaken, adds another layer of complexity to be explored and addressed.